AC – 11 July, 2022
Item No. – 6.25 (R)

University of Mumbai

Revised Syllabus for

B.E. Third Year- Cyber Security

Semester – (Sem. - V to VI)

(REV- 2019 'C' Scheme)

Under

FACULTY OF SCIENCE & TECHNOLOGY

(With effect from the academic year 2022-23)

University of Mumbai

Syllabus for Approval

Sr. No.	Heading	Particulars
1	Title of the Course	**Third Year Engineering Cyber Security**
2	Eligibility for Admission	**After Passing Second Year Engineering as per the Ordinance 0.6243**
3	Passing Marks	**40%**
4	Ordinances / Regulations (if any)	**Ordinance 0.6243**
5	No. of Years / Semesters	**4 Years/ 8 semesters**
6	Level	**Under Graduation**
7	Pattern	**Semester**
8	Status	**Revised 2019**
9	To be implemented from Academic Year	**With effect from Academic Year: 2022-2023**

Dr. S. K. Ukarande
Associate Dean
Faculty of Science and Technology
University of Mumbai

Dr Anuradha Muzumdar
Dean
Faculty of Science and Technology
University of Mumbai

Preamble

To meet the challenge of ensuring excellence in engineering education, the issue of quality needs to be addressed, debated and taken forward in a systematic manner. Accreditation is the principal means of quality assurance in higher education. The major emphasis of accreditation process is to measure the outcomes of the program that is being accredited. In line with this Faculty of Science and Technology (in particular Engineering) of University of Mumbai has taken a lead in incorporating philosophy of outcome based education in the process of curriculum development.

Faculty resolved that course objectives and course outcomes are to be clearly defined for each course, so that all faculty members in affiliated institutes understand the depth and approach of course to be taught, which will enhance learner's learning process. Choice based Credit and grading system enables a much-required shift in focus from teacher-centric to learner-centric education since the workload estimated is based on the investment of time in learning and not in teaching. It also focuses on continuous evaluation which will enhance the quality of education. Credit assignment for courses is based on 15 weeks teaching learning process, however content of courses is to be taught in 13 weeks and remaining 2 weeks to be utilized for revision, guest lectures, coverage of content beyond syllabus etc.

There was a concern that the earlier revised curriculum more focused on providing information and knowledge across various domains of the said program, which led to heavily loading of students in terms of direct contact hours. In this regard, faculty of science and technology resolved that to minimize the burden of contact hours, total credits of entire program will be of 170, wherein focus is not only on providing knowledge but also on building skills, attitude and self learning. Therefore in the present curriculum skill based laboratories and mini projects are made mandatory across all disciplines of engineering in second and third year of programs, which will definitely facilitate self learning of students. The overall credits and approach of curriculum proposed in the present revision is in line with AICTE model curriculum.

The present curriculum will be implemented for Second Year of Engineering from the academic year 2021-22. Subsequently this will be carried forward for Third Year and Final Year Engineering in the academic years 2022-23, 2023-24, respectively.

Dr. S. K. Ukarande
Associate Dean
Faculty of Science and Technology
University of Mumbai

Dr Anuradha Muzumdar
Dean
Faculty of Science and Technology
University of Mumbai

Incorporation and Implementation of Online Contents from NPTEL/ Swayam Platform

The curriculum revision is mainly focused on knowledge component, skill based activities and project based activities. Self-learning opportunities are provided to learners. In the revision process this time in particular Revised syllabus of 'C' scheme wherever possible additional resource links of platforms such as NPTEL, Swayam are appropriately provided. In an earlier revision of curriculum in the year 2012 and 2016 in Revised scheme 'A' and 'B' respectively, efforts were made to use online contents more appropriately as additional learning materials to enhance learning of students.

In the current revision based on the recommendation of AICTE model curriculum overall credits are reduced to 171, to provide opportunity of self-learning to learner. Learners are now getting sufficient time for self-learning either through online courses or additional projects for enhancing their knowledge and skill sets.

The Principals/ HoD's/ Faculties of all the institute are required to motivate and encourage learners to use additional online resources available on platforms such as NPTEL/ Swayam. Learners can be advised to take up online courses, on successful completion they are required to submit certification for the same. This will definitely help learners to facilitate their enhanced learning based on their interest.

Dr. S. K. Ukarande
Associate Dean
Faculty of Science and Technology
University of Mumbai

Dr Anuradha Muzumdar
Dean
Faculty of Science and Technology
University of Mumbai

Preface by Board of Studies Team

It is our honor and a privilege to present the Rev-2019 'C' scheme syllabus of the Bachelor of Engineering in the Cyber Security -- CS (effective from the year 2021-22). AICTE has introduced Cyber Security as one of the nine emerging technology and hence many colleges affiliated with the University of Mumbai has started four years UG program for Cyber Security. As part of the policy decision from the University end, the Board of IT got an opportunity to work on designing the syllabus for this new branch. As the Cyber Security is comparatively a young branch among other emerging engineering disciplines in the University of Mumbai, and hence while designing the syllabus promotion of an interdisciplinary approach has been considered.

The branch also provides multi-faceted scope like better placement and promotion of entrepreneurship culture among students and increased Industry Institute Interactions. Industries' views are considered as stakeholders while the design of the syllabus. As per Industry views only 16 % of graduates are directly employable. One of the reasons is a syllabus that is not in line with the latest emerging technologies. Our team of faculties has tried to include all the latest emerging technologies in the Cyber Security syllabus. Also the first time we are giving skill-based labs and Mini-project to students from the third semester onwards, which will help students to work on the latest Cyber Security technologies. Also the first time we are giving the choice of elective from fifth semester such that students will be mastered in one of the Cyber Security domain. The syllabus is peer-reviewed by experts from reputed industries and as per their suggestions, it covers future emerging trends in Cyber Security technology and research opportunities available due to these trends. .

We would like to thank senior faculties of IT and Computer Department, of all colleges affiliated to University of Mumbai for significant contribution in framing the syllabus. Also on behalf of all faculties we thank all the industry experts for their valuable feedback and suggestions. We sincerely hope that the revised syllabus will help all graduate engineers to face the future challenges in the field of Emerging Areas of Cyber Security.

Program Specific Outcome for graduate Program in Cyber Security

1. Apply Core of Cyber Security knowledge to develop stable and secure Cyber Security Application.
2. Identify the issues of Cyber Security in real time application and in area of cyber security domain.
3. Ability to apply and develop Cyber Security multidisciplinary projects and make it Cyber Security enabled Applications.

Board of Studies in Information Technology - Team
Dr. Deven Shah (Chairman)
Dr. Lata Ragha (Member)
Dr. Vaishali D. Khairnar (Member)
Dr. Sharvari Govilkar (Member)
Dr. Sunil B. Wankhade (Member)
Dr. Anil Kale (Member)
Dr. Vaibhav Narwade (Member)
Dr. GV Choudhary (Member)

Ad-hoc Board Information Technology
University of Mumbai

Program Structure for Third Year Cyber Security

UNIVERSITY OF MUMBAI (With Effect from 2022-2023)

Semester V

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned			
		Theory	Pract.	Theory	Tut	Pract.	Total
CSC501	Theoretical Computer Science	3	--	3	1	--	4
CSC502	Software Engineering	3	--	3	--	--	3
CSC503	Computer Network	3	--	3	--	--	3
CSC504	Data Warehousing & Mining	3	--	3	--	--	3
CSDLO501x	**Department Level Optional Course- 1**	3	--	3	--	--	3
CSL501	Software Engineering Lab	--	2	--	--	1	1
CSL502	Computer Network Lab	--	2	--	--	1	1
CSL503	Data Warehousing & Mining Lab	--	2	--	--	1	1
CSL504	Professional Comm. & Ethics II	--	2*+2	--	--	2	2
CSM501	Mini Project: 2 A	--	4$	--	--	2	2
Total		**15**	**14**	**15**	**01**	**07**	**23**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract &oral	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test 2	Avg					
CSC501	Theoretical Computer Science	20	20	20	80	3	25	--	125
CSC502	Software Engineering	20	20	20	80	3	--	--	100
CSC503	Computer Network	20	20	20	80	3	--	--	100
CSC504	Data Warehousing & Mining	20	20	20	80	3	--	--	100
CSDLO501x	**Department Level Optional Course -1**	20	20	20	80	3	--	--	100
CSL501	Software Engineering Lab	--	--	--	--	--	25	25	50
CSL502	Computer Network Lab	--	--	--	--	--	25	25	50

CSL503	Data Warehousing & Mining Lab	--	--	--	--	--	25	25	50
CSL504	Professional Comm. & Ethics II	--	--	--	--	--	25	25	50
CSM501	Mini Project : 2A	--	--	--	--	--	25	25	50
Total		**--**	**--**	**100**	**400**	--	**150**	**125**	**775**

* Theory class to be conducted for full class and $ indicates workload of Learner (Not Faculty), students can form groups with minimum 2(Two) and not more than 4(Four). Faculty Load: 1hour per week per four groups.

CSDO501X	**Department Optional Course – 1**
CSDLO5011	Probabilistic Graphical Models
CSDLO5012	Internet Programming
CSDLO5013	Advance Database Management System

Program Structure for Third Year Cyber Security
UNIVERSITY OF MUMBAI (With Effect from 2022-2023)

Semester VI

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned		
		Theory	Pract. Tut.	Theory	Pract.	Total
CSC601	Cryptography and Network Security	3	--	3	--	3
CSC602	Application Security and Secure Coding Principles	3	--	3		3
CSC603	Ethical Hacking & Digital Forensic	3	--	3	--	3
CSC604	Web X.0	3	--	3	--	3
CSDLO601x	**Department Level Optional Course -2**	3	--	3	--	3
CSL601	CNS Lab	--	2	--	1	1
CSL602	AS and SC Lab	--	2	--	1	1
CSL603	EH and DF Lab	--	2	--	1	1
CSL604	Web Lab	--	2	--	1	1
CSL605	ICT Security Lab (SBL)	--	4	--	2	2
CSM601	Mini Project Lab: 2B Application Security	--	4[$]	--	2	2
Total		**15**	**16**	**15**	**08**	**23**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract. &oral	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test 2	Avg					
CSC601	Cryptography and Network Security	20	20	20	80	3	--	--	100
CSC602	Application Security and Secure Coding Principles	20	20	20	80	3	--	--	100
CSC603	Ethical Hacking & Digital Forensic	20	20	20	80	3	--	--	100
CSC604	Web X.0	20	20	20	80	3	--	--	100
CSDLO601x	**Department Level Optional Course -2**	20	20	20	80	3	--	--	100
CSL601	CNS Lab	--	--	--	--	--	25	25	50
CSL602	AS and SC Lab	--	--	--	--	--	25	--	25
CSL603	EH and DF Lab	--	--	--	--	--	25	-	25
CSL604	Web Lab						25	25	50
CSL605	ICT Security Lab (SBL)	--	--	--	--	--	50	25	75
CSM601	Mini Project Lab: 2B Application Security	--	--	--	--	--	25	25	50
Total		**--**	**--**	**100**	**400**	**--**	**175**	**100**	**775**

$ indicates work load of Learner (Not Faculty), for Mini-Project. Students can form groups with minimum 2(Two) and not more than 4(Four). Faculty Load: 1hour per week per four groups.

CSDLO601X	**Department Optional Course – 2**
CSDLO6011	Enterprise Network Design
CSDLO6012	Blockchain Technology
CSDLO6013	Virtualization and cloud security
CSDLO6014	Cyber Security and Ransom ware incident response system

Program Structure for Third Year Cyber Security

UNIVERSITY OF MUMBAI (With Effect from 2022-2023)

Semester V

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned			
		Theory	Pract.	Theory	Tut	Pract.	Total
CSC501	Theoretical Computer Science	3	--	3	1	--	4
CSC502	Software Engineering	3	--	3	--	--	3
CSC503	Computer Network	3	--	3	--	--	3
CSC504	Data Warehousing & Mining	3	--	3	--	--	3
CSDLO501x	**Department Level Optional Course- 1**	3	--	3	--	--	3
CSL501	Software Engineering Lab	--	2	--	--	1	1
CSL502	Computer Network Lab	--	2	--	--	1	1
CSL503	Data Warehousing & Mining Lab	--	2	--	--	1	1
CSL504	Professional Comm. & Ethics II	--	2*+2	--	--	2	2
CSM501	Mini Project: 2 A	--	4$	--	--	2	2
Total		**15**	**14**	**15**	**01**	**07**	**23**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract &oral	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test 2	Avg					
CSC501	Theoretical Computer Science	20	20	20	80	3	25	--	125
CSC502	Software Engineering	20	20	20	80	3	--	--	100
CSC503	Computer Network	20	20	20	80	3	--	--	100
CSC504	Data Warehousing & Mining	20	20	20	80	3	--	--	100
CSDLO501x	**Department Level Optional Course -1**	20	20	20	80	3	--	--	100
CSL501	Software Engineering Lab	--	--	--	--	--	25	25	50
CSL502	Computer Network Lab	--	--	--	--	--	25	25	50

CSL503	Data Warehousing & Mining Lab	--	--	--	--	--	25	25	50
CSL504	Professional Comm. & Ethics II	--	--	--	--	--	25	25	50
CSM501	Mini Project : 2A	--	--	--	--	--	25	25	50
Total		**--**	**--**	**100**	**400**	--	**150**	**125**	**775**

* Theory class to be conducted for full class and $ indicates workload of Learner (Not Faculty), students can form groups with minimum 2(Two) and not more than 4(Four). Faculty Load: 1hour per week per four groups.

CSDO501X	**Department Optional Course – 1**
CSDLO5011	Probabilistic Graphical Models
CSDLO5012	Internet Programming
CSDLO5013	Advance Database Management System

Course Code	Course Name	Credits
CSC501	Theoretical Computer Science	4

Prerequisite: Discrete Structures	
Course Objectives:	
1.	Acquire conceptual understanding of fundamentals of grammars and languages.
2.	Build concepts of theoretical design of deterministic and non-deterministic finite automata and push down automata.
3.	Develop understanding of different types of Turing machines and applications.
4.	Understand the concept of Undecidability.
Course Outcomes: At the end of the course, the students will be able to	
1.	Understand concepts of Theoretical Computer Science, difference and equivalence of DFA and NFA , languages described by finite automata and regular expressions.
2.	Design Context free grammer, pushdown automata to recognize the language.
3.	Develop an understanding of computation through Turing Machine.
4.	Acquire fundamental understanding of decidability and undecidability.

Module No.	Unit No.	Topics	Theory Hrs.
1.0		**Basic Concepts and Finite Automata**	**09**
	1.1	Importance of TCS, Alphabets, Strings, Languages, Closure properties, Finite Automata (FA) and Finite State machine (FSM).	
	1.2	Deterministic Finite Automata (DFA) and Nondeterministic Finite Automata (NFA): Definitions, transition diagrams and Language recognizers, Equivalence between NFA with and without ε- transitions, NFA to DFA Conversion, Minimization of DFA, FSM with output: Moore and Mealy machines, Applications and limitations of FA.	
2.0		**Regular Expressions and Languages**	**07**
	2.1	Regular Expression (RE),Equivalence of RE and FA, Arden's Theorem, RE Applications	
	2.2	Regular Language (RL), Closure properties of RLs, Decision properties of RLs, Pumping lemma for RLs.	
3.0		**Grammars**	**08**
	3.1	Grammars and Chomsky hierarchy	
	3.2	Regular Grammar (RG), Equivalence of Left and Right linear grammar, Equivalence of RG and FA.	

	3.3	**Context Free Grammars (CFG)** Definition, Sentential forms, Leftmost and Rightmost derivations, Parse tree, Ambiguity, Simplification and Applications, Normal Forms: Chomsky Normal Forms (CNF) and Greibach Normal Forms (GNF), Context Free language (CFL) - Pumping lemma, Closure properties.	
4.0		**Pushdown Automata(PDA)**	**04**
	4.1	Definition, Language of PDA,PDA as generator, decider and acceptor of CFG, Deterministic PDA , Non-Deterministic PDA, Application of PDA.	
5.0		**Turing Machine (TM)**	**09**
	5.1	Definition, Design of TM as generator, decider and acceptor, Variants of TM: Multitrack, Multitape, Universal TM, Applications, Power and Limitations of TMs.	
6.0		**Undecidability**	**02**
	6.1	Decidability and Undecidability, Recursive and Recursively Enumerable Languages, Halting Problem, Rice's Theorem, Post Correspondence Problem.	
		Total	**39**

Text Books:	
1.	John E. Hopcroft, Rajeev Motwani, Jeffery D. Ullman, ***"Introduction to Automata Theory, Languages and Computation"***, 3rd Edition, Pearson Education, 2008.
2.	Michael Sipser, **"Theory of Computation"**, 3rd Edition, Cengage learning. 2013.
3.	Vivek Kulkarni, ***"Theory of Computation",*** Illustrated Edition, Oxford University Press, (12 April 2013) India.
Reference Books:	
1.	J. C. Martin, ***"Introduction to Languages and the Theory of Computation"*****,** 4th Edition, Tata McGraw Hill Publication, 2013.
2.	Kavi Mahesh, ***"Theory of Computation: A Problem Solving Approach"***, Kindle Edition, Wiley-India, 2011.

Assessment:	
Internal Assessment:	
1.	Assessment consists of two class tests of 20 marks each.
2.	The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed.
3.	Duration of each test shall be one hour.
Term work:	
1.	Term Work should consist of at least 06 assignments (at least one assignment on each module).

2.	Assignment (best 5 assignments)	20 marks
	Attendance	5 marks
3.	It is recommended to use JFLAP software (www.jflap.org) for better teaching and learning processes.	

End Semester Theory Examination:	
1.	Question paper will comprise of 6 questions, each carrying 20 marks.
2.	The students need to solve total 4 questions.
3.	Question No.1 will be compulsory and based on entire syllabus.
4.	Remaining questions (Q.2 to Q.6) will cover all the modules of syllabus.

Useful Links:	
1.	www.jflap.org
2.	https://nptel.ac.in/courses/106/104/106104028/
3.	https://nptel.ac.in/courses/106/104/106104148/

Course Code:	Course Title	Credit
CSC502	Software Engineering	3

Prerequisite: Object Oriented Programming with Java , Python Programming	
Course Objectives:	
1	To provide the knowledge of software engineering discipline.
2	To apply analysis, design and testing principles to software project development.
3	To demonstrate and evaluate real world software projects.
Course Outcomes: On successful completion of course, learners will be able to:	
1	Identify requirements & assess the process models.
2	Plan, schedule and track the progress of the projects.
3	Design the software projects.
4	Do testing of software project.
5	Identify risks, manage the change to assure quality in software projects.

Module		Content	Hrs
1		**Introduction To Software Engineering and Process Models**	**7**
	1.1	Software Engineering-process framework, the Capability Maturity Model (CMM), Advanced Trends in Software Engineering	
	1.2	Prescriptive Process Models: The Waterfall, Incremental Process Models, Evolutionary Process Models: RAD & Spiral	
	1.3	Agile process model: Extreme Programming (XP), Scrum, Kanban	
2		**Software Requirements Analysis and Modeling**	**4**
	2.1	Requirement Engineering, Requirement Modeling, Data flow diagram, Scenario based model	
	2.2	Software Requirement Specification document format(IEEE)	
3		**Software Estimation Metrics**	**7**
	3.1	Software Metrics, Software Project Estimation (LOC, FP, COCOMO II)	
	3.2	Project Scheduling & Tracking	
4		**Software Design**	**7**
	4.1	Design Principles & Concepts	
	4.2	Effective Modular Design, Cohesion and Coupling, Architectural design	
5		**Software Testing**	**7**
	5.1	Unit testing, Integration testing,Validation testing, System testing	
	5.2	Testing Techniques, white-box testing: Basis path, Control structure testing black-box testing: Graph based, Equivalence, Boundary Value	
	5.3	Types of Software Maintenance, Re-Engineering, Reverse Engineering	
6		**Software Configuration Management, Quality Assurance and Maintenance**	**7**
	6.1	Risk Analysis & Management: Risk Mitigation, Monitoring and Management Plan (RMMM).	
	6.2	Quality Concepts and Software Quality assurance Metrics, Formal Technical Reviews, Software Reliability	
	6.3	The Software Configuration Management (SCM) ,Version Control and Change Control	
			39

Textbooks:	
1	Roger Pressman, "***Software Engineering: A Practitioner's Approach"***, 9th edition , McGraw-Hill Publications, 2019
2	Ian Sommerville, ***"Software Engineering"***, 9th edition, Pearson Education, 2011
3	Ali Behfrooz and Fredeick J. Hudson, ***"Software Engineering Fundamentals"***, Oxford University Press, 1997
4	Grady Booch, James Rambaugh, Ivar Jacobson, ***"The unified modeling language user guide"***, 2nd edition, Pearson Education, 2005
References:	
1	Pankaj Jalote, ***"An integrated approach to Software Engineering"***, 3rd edition, Springer, 2005
2	Rajib Mall, ***"Fundamentals of Software Engineering"***, 5th edition, Prentice Hall India, 2014
3	Jibitesh Mishra and Ashok Mohanty, ***"Software Engineering"***, Pearson , 2011
4	Ugrasen Suman, ***"Software Engineering – Concepts and Practices"***, Cengage Learning, 2013
5	Waman S Jawadekar, ***"Software Engineering principles and practice"***, McGraw Hill Education, 2004

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Only Four questions need to be solved.
4	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Useful Links	
1	https://nptel.ac.in/courses/106/105/106105182/
2	https://onlinecourses.nptel.ac.in/noc19_cs69/preview
3	https://www.mooc-list.com/course/software-engineering-introduction-edx

Course Code:	Course Title	Credit
CSC503	Computer Network	3

Prerequisite: None	
Course Objectives:	
1	To introduce concepts and fundamentals of data communication and computer networks.
2	To explore the inter-working of various layers of OSI.
3	To explore the issues and challenges of protocols design while delving into TCP/IP protocol suite.
4	To assess the strengths and weaknesses of various routing algorithms.
5	To understand various transport layer and application layer protocols.
Course Outcomes: On successful completion of course, learner will be able to	
1	Demonstrate the concepts of data communication at physical layer and compare ISO - OSI model with TCP/IP model.
2	Explore different design issues at data link layer.
3	Design the network using IP addressing and sub netting / supernetting schemes.
4	Analyze transport layer protocols and congestion control algorithms.
5	Explore protocols at application layer

Module		Content	Hrs
1		**Introduction to Networking**	**4**
	1.1	Introduction to computer network, network application, network software and hardware components (Interconnection networking devices), Network topology, protocol hierarchies, design issues for the layers, connection oriented and connectionless services	
	1.2	Reference models: Layer details of OSI, TCP/IP models. Communication between layers.	
2		**Physical Layer**	**3**
	2.1	Introduction to Communication Electromagnetic Spectrum	
	2.2	Guided Transmission Media: Twisted pair, Coaxial, Fiber optics.	
3		**Data Link Layer**	**8**
	3.1	DLL Design Issues (Services, Framing, Error Control, Flow Control), Error Detection and Correction(Hamming Code, CRC, Checksum) , Elementary Data Link protocols , Stop and Wait, Sliding Window(Go Back N, Selective Repeat)	
	3.2	**Medium Access Control sublayer** Channel Allocation problem, Multiple access Protocol(Aloha, Carrier Sense Multiple Access (CSMA/CD)	
4		**Network layer**	**12**
	4.1	Network Layer design issues, Communication Primitives: Unicast, Multicast, Broadcast. IPv4 Addressing (classfull and classless), Subnetting, Supernetting design problems ,IPv4 Protocol, Network Address Translation (NAT), IPv6	
	4.2	**Routing algorithms :** Shortest Path (Dijkastra's), Link state routing, Distance Vector Routing	
	4.3	**Protocols** - ARP,RARP, ICMP, IGMP	

	4.4	**Congestion control algorithms:** Open loop congestion control, Closed loop congestion control, QoS parameters, Token & Leaky bucket algorithms	
5		**Transport Layer**	**6**
	5.1	**The Transport Service**: Transport service primitives, Berkeley Sockets, Connection management (Handshake), UDP, TCP, TCP state transition, TCP timers	
	5.2	TCP Flow control (sliding Window), TCP Congestion Control: Slow Start	
6		**Application Layer**	**6**
	6.1	DNS: Name Space, Resource Record and Types of Name Server. HTTP, SMTP, Telnet, FTP, DHCP	

Textbooks:	
1	A.S. Tanenbaum, **Computer Networks**,4th edition Pearson Education
2	B.A. Forouzan, **Data Communications and Networking**, 5th edition, TMH
3	James F. Kurose, Keith W. Ross, **Computer Networking, A Top-Down Approach Featuring the Internet**,6th edition, Addison Wesley
References:	
1	S.Keshav,**An Engineering Approach To Computer Networking**, Pearson
2	Natalia Olifer & Victor Olifer,**Computer Networks: Principles, Technologies & Protocols for Network Design**, Wiley India, 2011.
3	Larry L.Peterson, Bruce S.Davie, **Computer Networks: A Systems Approach**, Second Edition ,The Morgan Kaufmann Series in Networking

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise of total six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only Four question need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.

Useful Links	
1	https://www.netacad.com/courses/networking/networking-essentials
2	https://www.coursera.org/learn/computer-networking
3	https://nptel.ac.in/courses/106/105/106105081
4	https://www.edx.org/course/introduction-to-networking

Course Code:	Course Title	Credit
CSC504	Data Warehousing and Mining	3

Prerequisite: Database Concepts	
Course Objectives:	
1.	To identify the significance of Data Warehousing and Mining.
2.	To analyze data, choose relevant models and algorithms for respective applications.
3.	To study web data mining.
4.	To develop research interest towards advances in data mining.
Course Outcomes: At the end of the course, the student will be able to	
1.	Understand data warehouse fundamentals and design data warehouse with dimensional modelling and apply OLAP operations.
2.	Understand data mining principles and perform Data preprocessing and Visualization.
3.	Identify appropriate data mining algorithms to solve real world problems.
4.	Compare and evaluate different data mining techniques like classification, prediction, clustering and association rule mining
5.	Describe complex information and social networks with respect to web mining.

Module	Content	Hrs
1	**Data Warehousing Fundamentals**	8
	Introduction to Data Warehouse, Data warehouse architecture, Data warehouse versus Data Marts, E-R Modeling versus Dimensional Modeling, Information Package Diagram, Data Warehouse Schemas; Star Schema, Snowflake Schema, Factless Fact Table, Fact Constellation Schema. Update to the dimension tables. Major steps in ETL process, OLTP versus OLAP, OLAP operations: Slice, Dice, Rollup, Drilldown and Pivot.	
2	**Introduction to Data Mining, Data Exploration and Data Pre-processing**	8
	Data Mining Task Primitives, Architecture, KDD process, Issues in Data Mining, Applications of Data Mining, Data Exploration: Types of Attributes, Statistical Description of Data, Data Visualization, Data Preprocessing: Descriptive data summarization, Cleaning, Integration & transformation, Data reduction, Data Discretization and Concept hierarchy generation.	
3	**Classification**	6
	Basic Concepts, Decision Tree Induction, Naïve Bayesian Classification, Accuracy and Error measures, Evaluating the Accuracy of a Classifier: Holdout & Random Subsampling, Cross Validation, Bootstrap.	
4	**Clustering**	6
	Types of data in Cluster analysis, Partitioning Methods (*k*-Means, *k*-Medoids), Hierarchical Methods (Agglomerative, Divisive).	
5	**Mining frequent patterns and associations**	6
	Market Basket Analysis, Frequent Item sets, Closed Item sets, and Association Rule, Frequent Pattern Mining, Apriori Algorithm, Association Rule Generation, Improving the Efficiency of Apriori, Mining Frequent Itemsets without candidate generation, Introduction to Mining Multilevel Association Rules and Mining Multidimensional Association Rules.	

6	**Web Mining**	**5**
	Introduction, Web Content Mining: Crawlers, Harvest System, Virtual Web View, Personalization, Web Structure Mining: Page Rank, Clever, Web Usage Mining.	

Textbooks:	
1	Paulraj Ponniah, ***" Data Warehousing: Fundamentals for IT Professionals"***, Wiley India.
2	Han, Kamber, ***"Data Mining Concepts and Techniques"***, Morgan Kaufmann 2nd edition.
3	M.H. Dunham, ***"Data Mining Introductory and Advanced Topics"***, Pearson Education.
References:	
1	Reema Theraja, ***"Data warehousing"***, Oxford University Press 2009.
2	Pang-Ning Tan, Michael Steinbach and Vipin Kumar, ***"Introduction to Data Mining"***, Pearson Publisher 2nd edition.
3	Ian H. Witten, Eibe Frank and Mark A. Hall, ***"Data Mining"***, Morgan Kaufmann 3rd edition.

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and second-class test when additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise of total six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example, If Q.2 part (a) from module 3 then part (b) can be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to the number of respective lecture hours as mentioned in the syllabus.
Useful Links	
1	https://onlinecourses.nptel.ac.in/noc20_cs12/preview
2	https://www.coursera.org/specializations/data-mining

Course Code:	Course Title	Credit
CSDLO5011	**Probabilistic Graphical Models**	3

Prerequisite: Engineering Mathematics, Discrete Structure	
Course Objectives:	
1	To give comprehensive introduction of probabilistic graphical models
2	To make inferences, learning, actions and decisions while applying these models
3	To introduce real-world trade-offs when using probabilistic graphical models in practice
4	To develop the knowledge and skills necessary to apply these models to solve real world problems.
Course Outcomes: At the end of the course, the student will be able to	
1	Understand basic concepts of probabilistic graphical modelling.
2	Model and extract inference from various graphical models like Bayesian Networks, Markov Models
3	Perform learning and take actions and decisions using probabilistic graphical models
4	Represent real world problems using graphical models; design inference algorithms; and learn the structure of the graphical model from data.
5	Design real life applications using probabilistic graphical models.

Module		Content	Hrs
1.		**Introduction to Probabilistic Graphical Modeling**	**5**
	1.1	Introduction to Probability Theory: Probability Theory, Basic Concepts in Probability, Random Variables and Joint Distribution, Independence and Conditional Independence, Continuous Spaces, Expectation and Variances	
	1.2	Introduction to Graphs: Nodes and Edges, Subgraphs, Paths and Trails, Cycles and Loops	
	1.3	Introduction to Probabilistic Graph Models: Bayesian Network, Markov Model, Hidden Markov Model	
	1.4	Applications of PGM	
2.		**Bayesian Network Model and Inference**	**10**
	2.1	Directed Graph Model: Bayesian Network-Exploiting Independence Properties, Naive Bayes Model, Bayesian Network Model, Reasoning Patterns, Basic Independencies in Bayesian Networks, Bayesian Network Semantics, Graphs and Distributions. Modelling: Picking variables, Picking Structure, Picking Probabilities, D-separation	
	2.2	Local Probabilistic Models: Tabular CPDs, Deterministic CPDs, Context Specific CPDs, Generalized Linear Models.	

	2.3	Exact inference variable elimination: Analysis of Complexity, Variable Elimination, Conditioning, Inference with Structured CPDs.	
3.		**Markov Network Model and Inference**	**8**
	3.1	**Undirected Graph Model :** Markov Model-Markov Network, Parameterization of Markov Network, Gibb's distribution, Reduced Markov Network, Markov Network Independencies, From Distributions to Graphs, Fine Grained Parameterization, Over Parameterization	
	3.2	Exact inference variable elimination: Graph Theoretic Analysis for Variable Elimination, Conditioning	
4.		**Hidden Markov Model and Inference**	**6**
	4.1	Template Based Graph Model : HMM- Temporal Models, Template Variables and Template Factors, Directed Probabilistic Models, Undirected Representation, Structural Uncertainty.	
5.		**Learning and Taking Actions and Decisions**	**6**
	5.1	Learning Graphical Models: Goals of Learning, Density Estimation, Specific Prediction Tasks, Knowledge Discovery. Learning as Optimization: Empirical Risk, over fitting, Generalization, Evaluating Generalization Performance, Selecting a Learning Procedure, Goodness of fit, Learning Tasks. Parameter Estimation: Maximum Likelihood Estimation, MLE for Bayesian Networks	
	5.2	Causality: Conditioning and Intervention, Correlation and Causation, Causal Models, Structural Causal Identifiability, Mechanisms and Response Variables, Learning Causal Models. Utilities and Decisions: Maximizing Expected Utility, Utility Curves, Utility Elicitation. Structured Decision Problems: Decision Tree	
6.		**Applications**	**4**
	6.1	Application of Bayesian Networks: Classification, Forecasting, Decision Making	
	6.2	Application of Markov Models: Cost Effectiveness Analysis, Relational Markov Model and its Applications, Application in Portfolio Optimization	
	6.3	Application of HMM: Speech Recognition, Part of Speech Tagging, Bioinformatics.	

Textbooks:	
1.	Daphne Koller and Nir Friedman, **"Probabilistic Graphical Models: Principles and Techniques"**, Cambridge, MA: The MIT Press, 2009 (ISBN 978-0-262-0139-2).
2.	David Barber, **"Bayesian Reasoning and Machine Learning"**, Cambridge University Press, 1st edition, 2011.
References:	

1.	Finn Jensen and Thomas Nielsen, **"Bayesian Networks and Decision Graphs (Information Science and Statistics)**", 2nd Edition, Springer, 2007.
2.	Kevin P. Murphy, **"Machine Learning: A Probabilistic Perspective"**, MIT Press, 2012.
3.	Martin Wainwright and Michael Jordan, M., **"Graphical Models, Exponential Families, and Variational Inference"**, 2008.

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be m onducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1.	Question paper will comprise of total six questions.
2.	All question carries equal marks
3.	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4.	Only Four question need to be solved.
5.	In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.
Useful Links	
1.	https://www.coursera.org/specializations/probabilistic-graphical-models
2.	https://www.mooc-list.com/tags/probabilistic-graphical-models
3.	https://scholarship.claremont.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2690&context=cmc_theses
4.	https://www.upgrad.com/blog/bayesian-networks/
5.	https://www.utas.edu.au/ data/assets/pdf_file/0009/588474/TR_14_BNs_a_resource_guide.pdf
6.	https://math.libretexts.org/Bookshelves/Applied_Mathematics/Book%3A_Applied_Finite_Mathematics_(Sekhon_and_Bloom)/10%3A_Markov_Chains/10.02%3A_Applications_of_Markov_Chains/10.2.01%3A_Applications_of_Markov_Chains_(Exercises)
7.	https://link.springer.com/chapter/10.1007/978-3-319-43742-2_24
8.	https://homes.cs.washington.edu/~pedrod/papers/kdd02a.pdf
9.	https://core.ac.uk/download/pdf/191938826.pdf
10.	https://cs.brown.edu/research/pubs/theses/ugrad/2005/dbooksta.pdf

11.	https://web.ece.ucsb.edu/Faculty/Rabiner/ece259/Reprints/tutorial%20on%20hmm%20and%20applications.pdf
12.	https://mi.eng.cam.ac.uk/~mjfg/mjfg_NOW.pdf
13.	http://bioinfo.au.tsinghua.edu.cn/member/jgu/pgm/materials/Chapter3-LocalProbabilisticModels.pdf

Suggested List of Experiments:	
Sr. No	**Experiment**
1.	Experiment on Probability Theory
2.	Experiment on Graph Theory
3.	Experiment on Bayesian Network Modelling
4.	Experiment on Markov Chain Modeling
5.	Experiment on HMM
6.	Experiment on Maximum Likelihood Estimation
7.	Decision Making using Decision Trees
8.	Learning with Optimization
**** Suggestion: Laboratory work based on above syllabus can be incorporated along with mini project in CSM501: Mini-Project.**	

Course Code:	Course Title	Credit
CSDLO5012	Internet Programming	3

Prerequisite: Data Structures, Programming Languages- JAVA, Python	
Course Objectives:	
1	To get familiar with the basics of Internet Programming.
2	To acquire knowledge and skills for creation of web site considering both client and server-side programming
3	To gain ability to develop responsive web applications and explore different web extensions and web services standards
4	To learn characteristics of RIA and React Js
Course Outcomes:	
1	Implement interactive web page(s) using HTML and CSS.
2	Design a responsive web site using JavaScript and demonstrate database connectivity using JDBC
3	Demonstrate Rich Internet Application using Ajax and demonstrate and differentiate various Web Extensions
4	Demonstrate web application using Reactive Js

Module		Content	Hrs
1		**Introduction to Web Technology**	**10**
	1.1	**Web Essentials**: Clients, Servers and Communication, The Internet, Basic Internet protocols, World wide web, HTTP Request Message, HTTP Response Message, Web Clients, Web Servers **HTML5** – fundamental syntax and semantics, Tables, Lists, Image, HTML5 control elements, Semantic elements, Drag and Drop, Audio – Video controls **CSS3** – Inline, embedded and external style sheets – Rule cascading, Inheritance, Backgrounds, Border Images, Colors, Shadows, Text, Transformations, Transitions, Animation, Basics of Bootstrap.	
2		**Front End Development**	**7**
	2.1	Java Script: An introduction to JavaScript–JavaScript DOM Model-Date and Objects-Regular Expressions- Exception Handling-Validation-Built-in objects-Event Handling, DHTML with JavaScript-JSON introduction – Syntax – Function Files – Http Request –SQL.	
3.		**Back End Development**	**7**
	3.1	**Servlets**: Java Servlet Architecture, Servlet Life Cycle, Form GET and POST actions, Session Handling, Understanding Cookies, Installing and Configuring Apache Tomcat Web Server, **Database Connectivity**: JDBC perspectives, JDBC program example **JSP:** Understanding Java Server Pages, JSP Standard Tag Library (JSTL), Creating HTML forms by embedding JSP code.	
4		**Rich Internet Application (RIA)**	**4**
	4.1	Characteristics of RIA, **Introduction to AJAX**: AJAX design basics, AJAX vs Traditional Approach, Rich User Interface using Ajax, jQuery framework with AJAX.	
5		**Web Extension: PHP and XML**	**6**
	5.1	XML –DTD (Document Type Definition), XML Schema, Document Object Model, Presenting XML, Using XML Parsers: DOM and SAX, XSL-eXtensible Stylesheet Language	

	5.2	**Introduction to PHP**- Data types, control structures, built in functions, building web applications using PHP- tracking users, PHP and MySQLdatabase connectivity with example.	
6		**React js**	**5**
	6.1	Introduction, React features, App "Hello World" Application, Introduction to JSX, Simple Application using JSX.	
			39

Textbooks:	
1	Ralph Moseley, M.T. Savliya, "Developing Web Applications", Willy India, Second Edition, ISBN: 978-81-265-3867-6
2	"Web Technology Black Book", Dremtech Press, First Edition, 978-7722-997
3	Robin Nixon, "Learning PHP, MySQL, JavaScript, CSS & HTML5" Third Edition, O'REILLY, 2014. (http://www.ebooksbucket.com/uploads/itprogramming/javascript/Learning_PHP_MySQL_Javascript_CSS_HTML5_Robin_Nixon_3e.pdf)
4	Dana Moore, Raymond Budd, Edward Benson,Professional Rich Internet Applications: AJAX and Beyond Wiley publications. https://ebooks-it.org/0470082801-ebook.htm
5.	Alex Banks and Eve Porcello, Learning React Functional Web Development with React and Redux,OREILLY, First Edition
References:	
1	Harvey & Paul Deitel& Associates, Harvey Deitel and Abbey Deitel, Internet and World Wide Web - How To Program, Fifth Edition, Pearson Education, 2011.
2	Achyut S Godbole and AtulKahate, —Web Technologies, Second Edition, Tata McGraw Hill, 2012.
3	Thomas A Powell, Fritz Schneider, —JavaScript: The Complete Reference, Third Edition, Tata McGraw Hill, 2013
4	David Flanagan, —JavaScript: The Definitive Guide, Sixth Edition, O'Reilly Media, 2011
5	Steven Holzner —The Complete Reference - PHP, Tata McGraw Hill, 2008
6	Mike Mcgrath—PHP & MySQL in easy Steps, Tata McGraw Hill, 2012.

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The firstclass test is to be conducted when approx. 40% syllabus is completed and the secondclass test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Useful Links	
1	https://books.goalkicker.com/ReactJSBook/
2	https://www.guru99.com/reactjs-tutorial.html
3	www.nptelvideos.in
4	www.w3schools.com
5	https://spoken-tutorial.org/
6	www.coursera.org
The following list can be used as a guideline for mini project:	

1	Create Simple web page using HTML5
2	Design and Implement web page using CSS3 and HTML5
3	Form Design and Client-Side Validation using: a. Javascript and HTML5, b. Javascript and Jquery
4	Develop interactive web pages using HTML 5 with JDBC database connectivity
5	Develop simple web page using PHP
6	Develop interactive web pages using PHP with database connectivity MYSQL
7	Develop XML web page using DTD, XSL
8	Implement a web page using Ajax and PHP
9	Case study based on Reactive js
10	Installation of the React DOM library.
*** Suggestion: Laboratory work based on above syllabus can be incorporated as mini project in CSM501: Mini-Project.**	

Course Code:	Course Title	Credit
CSDLO5013	Advance Database Management System	3

Prerequisite: Database Management System	
Course Objectives:	
1	To provide insights into distributed database designing
2	To specify the various approaches used for using XML and JSON technologies.
3	To apply the concepts behind the various types of NoSQL databases and utilize it for Mongodb
4	To learn about the trends in advance databases
Course Outcomes: After the successful completion of this course learner will be able to:	
1	Design distributed database using the various techniques for query processing
2	Measure query cost and perform distributed transaction management
3	Organize the data using XML and JSON database for better interoperability
4	Compare different types of NoSQL databases
5	Formulate NoSQL queries using Mongodb
6	Describe various trends in advance databases through temporal, graph based and spatial based databases

Module		Content	Hrs
1		**Distributed Databases**	**3**
	1.1	Introduction, Distributed DBMS Architecture, Data Fragmentation, Replication and Allocation Techniques for Distributed Database Design.	
2		**Distributed Database Handling**	**8**
	2.1	Distributed Transaction Management – Definition, properties, types, architecture Distributed Query Processing - Characterization of Query Processors, Layers/ phases of query processing.	
	2.2	Distributed Concurrency Control- Taxonomy, Locking based, Basic TO algorithm, Recovery in Distributed Databases: Failures in distributed database, 2PC and 3PC protocol.	
3		**Data interoperability – XML and JSON**	**6**
	3.1	XML Databases: Document Type Definition, XML Schema, Querying and Transformation: XPath and XQuery.	
	3.2	Basic JSON syntax, (Java Script Object Notation),JSON data types, Stringifying and parsing the JSON for sending & receiving, JSON Object retrieval using key-value pair and JQuery, XML Vs JSON	
4		**NoSQL Distribution Model**	**10**
	4.1	NoSQL database concepts: NoSQL data modeling, Benefits of NoSQL, comparison between SQL and NoSQL database system.	
	4.2	Replication and sharding, Distribution Models Consistency in distributed data, CAP theorem, Notion of ACID Vs BASE, handling Transactions, consistency and eventual consistency	
	4.3	Types of NoSQL databases: Key-value data store, Document database and Column Family Data store, Comparison of NoSQL databases w.r.t CAP theorem and ACID properties.	
5		**NoSQL using MongoDB**	**6**

	5.1	NoSQL using MongoDB: Introduction to MongoDB Shell, Running the MongoDB shell, MongoDB client, Basic operations with MongoDB shell, Basic Data Types, Arrays, Embedded Documents	
	5.2	Querying MongoDB using find() functions, advanced queries using logical operators and sorting, simple aggregate functions, saving and updating document. MongoDB Distributed environment: Concepts of replication and horizonal scaling through sharding in MongoDB	
6		**Trends in advance databases**	**6**
	6.1	**Temporal database:** Concepts, time representation, time dimension, incorporating time in relational databases.	
	6.2	**Graph Database:** Introduction, Features, Transactions, consistency, Availability, Querying, Case Study Neo4J	
	6.3	**Spatial database:** Introduction, data types, models, operators and queries	
			39

Textbooks:	
1	Korth, Siberchatz,Sudarshan, "Database System Concepts", 6th Edition, McGraw Hill
2	Elmasri and Navathe, "Fundamentals of Database Systems", 5th Edition, Pearson Education
3	Ozsu, M. Tamer, Valduriez, Patrick, "Principles of distributed database systems",3rd Edition, Pearson Education, Inc.
4	PramodSadalge, Martin Fowler, NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence, Addison Wesely/ Pearson
5	Jeff Friesen , Java XML and JSON,Second Edition, 2019, après Inc.
References:	
1	Peter Rob and Carlos Coronel,Database Systems Design, Implementation and Management, Thomson Learning, 5th Edition.
2	Dr. P.S. Deshpande, SQL and PL/SQL for Oracle 10g, Black Book, Dreamtech Press.
3	Adam Fowler, NoSQL for dummies, John Wiley & Sons, Inc.
4	Shashank Tiwari, Professional NOSQL, John Willy & Sons. Inc
5	Raghu Ramkrishnan and Johannes Gehrke, Database Management Systems, TMH
6	MongoDB Manual : https://docs.mongodb.com/manual

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise of total six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only Four question need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.
NOTE: Suggested that in Mini Projects (CSM501) can be included NoSQL databases for implementation as a backend.	

Useful Links	
1	https://cassandra.apache.org
2	https://www.mongodb.com
3	https://riak.com
4	https://neo4j.com
5	https://martinfowler.com/articles/nosql-intro-original.pdf

Lab Code	Lab Name	Credit
CSL501	Software Engineering Lab	1

Prerequisite: Object Oriented Programming with Java , Python Programming	
Lab Objectives:	
1	To solve real life problems by applying software engineering principles
2	To impart state-of-the-art knowledge on Software Engineering
Lab Outcomes: On successful completion of laboratory experiments, learners will be able to :	
1	Identify requirements and apply software process model to selected case study.
2	Develop architectural models for the selected case study.
3	Use computer-aided software engineering (CASE) tools.

Suggested List of Experiments - Assign the case study/project as detail statement of problem to a group of two/three students. Laboratory work will be based on course syllabus with minimum 10 experiments. Open source computer-aided software engineering (CASE) tools can be used for performing the experiment.

Sr. No.	Title of Experiment
1	Application of at least two traditional process models.
2	Application of the Agile process models.
3	Preparation of software requirement specification (SRS) document in IEEE format.
4	Structured data flow analysis.
5	Use of metrics to estimate the cost.
6	Scheduling & tracking of the project.
7	Write test cases for black box testing.
8	Write test cases for white box testing.
9	Preparation of Risk Mitigation, Monitoring and Management Plan (RMMM).
10	Version controlling of the project.

Term Work:	
1	Term work should consist of 10 experiments.
2	Journal must include at least 2 assignments on content of theory and practical of "Software Engineering"
3	The final certification and acceptance of term work ensures that satisfactory performance of laboratory work and minimum passing marks in term work.
4	Total 25 Marks (Experiments: 15-marks, Attendance Theory & Practical: 05-marks, Assignments: 05-marks)
Oral & Practical exam	
	Based on the entire syllabus of CSC502 and CSL501 syllabus

Lab Code	Lab Name	Credit
CSL502	Computer Network Lab	1

Prerequisite: None	
Lab Objectives:	
1	To practically explore OSI layers and understand the usage of simulation tools.
2	To analyze, specify and design the topological and routing strategies for an IP based networking infrastructure.
3	To identify the various issues of a packet transfer from source to destination, and how they are resolved by the various existing protocols
Lab Outcomes: On successful completion of lab, learner will be able to	
1	Design and setup networking environment in Linux.
2	Use Network tools and simulators such as NS2, Wireshark etc. to explore networking algorithms and protocols.
3	Implement programs using core programming APIs for understanding networking concepts.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1.	Study of RJ45 and CAT6 Cabling and connection using crimping tool.
2.	Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route)
3.	Build a simple network topology and configure it for static routing protocol using packet tracer. Setup a network and configure IP addressing, subnetting, masking.
4.	Perform network discovery using discovery tools (eg. Nmap, mrtg)
5.	Use Wire shark to understand the operation of TCP/IP layers: ● Ethernet Layer: Frame header, Frame size etc. ● Data Link Layer: MAC address, ARP (IP and MAC address binding) ● Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo) ● Transport Layer: TCP Ports, TCP handshake segments etc. ● Application Layer: DHCP, FTP, HTTP header formats
6.	Use simulator (Eg. NS2) to understand functioning of ALOHA, CSMA/CD.
7.	Study and Installation of Network Simulator (NS3)
8.	a. Set up multiple IP addresses on a single LAN. b. Using nestat and route commands of Linux, do the following: ● View current routing table ● Add and delete routes ● Change default gateway c. Perform packet filtering by enabling IP forwarding using IPtables in Linux.
9	Design VPN and Configure RIP/OSPF using Packet tracer.
10.	Socket programming using TCP or UDP
11.	Perform File Transfer and Access using FTP
12.	Perform Remote login using Telnet server

Term Work:	
1	Term work should consist of 10 experiments.
2	Journal must include at least 2 assignments on content of theory and practical of "Computer Network"
3	The final certification and acceptance of term work ensures that satisfactory performance of laboratory work and minimum passing marks in term work.
4	Total 25 Marks (Experiments: 15-marks, Attendance Theory& Practical: 05-marks,

	Assignments: 05-marks)
Oral & Practical exam	
	Based on the entire syllabus of CSC503: Computer Network

Useful Links	
1	https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer
2	https://www.coursera.org/projects/data-forwarding-computer-networks
3	https://www.edx.org/course/ilabx-the-internet-masterclass

Lab Code	Lab Name	Credit
CSL503	Data Warehousing and Mining Lab	1

Prerequisite: Database Concepts	
Lab Objectives:	
1.	Learn how to build a data warehouse and query it.
2.	Learn about the data sets and data preprocessing.
3.	Demonstrate the working of algorithms for data mining tasks such Classification, clustering, Association rule mining & Web mining
4.	Apply the data mining techniques with varied input values for different parameters.
5.	Explore open source software (like WEKA) to perform data mining tasks.
Lab Outcomes: At the end of the course, the student will be able to	
1.	Design data warehouse and perform various OLAP operations.
2.	Implement data mining algorithms like classification.
3.	Implement clustering algorithms on a given set of data sample.
4.	Implement Association rule mining & web mining algorithm.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	One case study on building Data warehouse/Data Mart • Write Detailed Problem statement and design dimensional modelling (creation of star and snowflake schema)
2	Implementation of all dimension table and fact table based on experiment 1 case study
3	Implementation of OLAP operations: Slice, Dice, Rollup, Drilldown and Pivot based on experiment 1 case study
4	Implementation of Bayesian algorithm
5	Implementation of Data Discretization (any one) & Visualization (any one)
6	Perform data Pre-processing task and demonstrate Classification, Clustering, Association algorithm on data sets using data mining tool (WEKA/R tool)
7	Implementation of Clustering algorithm (K-means/K-medoids)
8	Implementation of any one Hierarchical Clustering method
9	Implementation of Association Rule Mining algorithm (Apriori)
10	Implementation of Page rank/HITS algorithm

Term Work:	
1	Term work should consist of 10 experiments.
2	Journal must include at least 1 assignment on content of theory and practical of "Data Warehousing and Mining"
3	The final certification and acceptance of term work ensures that satisfactory performance of laboratory work and minimum passing marks in term work.
4	Total 25 Marks (Experiments: 15-marks, Attendance (Theory & Practical): 05-marks, Assignments: 05-marks)
Oral & Practical exam	
	Based on the entire syllabus of CSC504 : Data Warehousing and Mining

Course Code	Course Name	Credit
CSL504	Professional Communication & Ethics II	02

Course Rationale: This curriculum is designed to build up a professional and ethical approach, effective oral and written communication with enhanced soft skills. Through practical sessions, it augments student's interactive competence and confidence to respond appropriately and creatively to the implied challenges of the global Industrial and Corporate requirements. It further inculcates the social responsibility of engineers as technical citizens.	
Course Objectives	
1	To discern and develop an effective style of writing important technical/business documents.
2	To investigate possible resources and plan a successful job campaign.
3	To understand the dynamics of professional communication in the form of group discussions, meetings, etc. required for career enhancement.
4	To develop creative and impactful presentation skills.
5	To analyze personal traits, interests, values, aptitudes and skills.
6	To understand the importance of integrity and develop a personal code of ethics.
Course Outcomes: At the end of the course, the student will be able to	
1	Plan and prepare effective business/ technical documents which will in turn provide solid foundation for their future managerial roles.
2	Strategize their personal and professional skills to build a professional image and meet the demands of the industry.
3	Emerge successful in group discussions, meetings and result-oriented agreeable solutions in group communication situations.
4	Deliver persuasive and professional presentations.
5	Develop creative thinking and interpersonal skills required for effective professional communication.
6	Apply codes of ethical conduct, personal integrity and norms of organizational behaviour.

Module	Contents	Hours
1	**ADVANCED TECHNICAL WRITING: PROJECT/PROBLEM BASED LEARNING (PBL)**	**06**
	Purpose and Classification of Reports: **Classification on the basis of:** Subject Matter (Technology, Accounting, Finance, Marketing, etc.), Time Interval (Periodic, One-time, Special), Function (Informational, Analytical, etc.), Physical Factors (Memorandum, Letter, Short & Long) **Parts of a Long Formal Report:** Prefatory Parts (Front Matter), Report Proper (Main Body), Appended Parts (Back Matter) **Language and Style of Reports:** Tense, Person & Voice of Reports, Numbering Style of Chapters, Sections, Figures, Tables and Equations, Referencing Styles in APA & MLA Format, Proofreading through Plagiarism Checkers **Definition, Purpose & Types of Proposals:** Solicited (in conformance with RFP) & Unsolicited Proposals, Types (Short and Long proposals) **Parts of a Proposal:** Elements, Scope and Limitations, Conclusion **Technical Paper Writing:** Parts of a Technical Paper (Abstract, Introduction, Research Methods, Findings and Analysis, Discussion, Limitations, Future Scope and References), Language and Formatting, Referencing in IEEE Format	

2	**EMPLOYMENT SKILLS**	**06**
	Cover Letter & Resume: Parts and Content of a Cover Letter, Difference between Bio-data, Resume & CV, Essential Parts of a Resume, Types of Resume (Chronological, Functional & Combination) **Statement of Purpose:** Importance of SOP, Tips for Writing an Effective SOP **Verbal Aptitude Test:** Modelled on CAT, GRE, GMAT exams **Group Discussions:** Purpose of a GD, Parameters of Evaluating a GD, Types of GDs (Normal, Case-based & Role Plays), GD Etiquettes **Personal Interviews:** Planning and Preparation, Types of Questions, Types of Interviews (Structured, Stress, Behavioural, Problem Solving & Case-based), Modes of Interviews: Face-to-face (One-to one and Panel) Telephonic, Virtual	
3	**BUSINESS MEETINGS**	**02**
	Conducting Business Meetings: Types of Meetings, Roles and Responsibilities of Chairperson, Secretary and Members, Meeting Etiquette **Documentation:** Notice, Agenda, Minutes	
4	**TECHNICAL/ BUSINESS PRESENTATIONS**	**02**
	Effective Presentation Strategies: Defining Purpose, Analyzing Audience, Location and Event, Gathering, Selecting &Arranging Material, structuring a Presentation, Making Effective Slides, Types of Presentations Aids, Closing a Presentation, Platform skills **Group Presentations:** Sharing Responsibility in a Team, Building the contents and visuals together, Transition Phases	
5	**INTERPERSONAL SKILLS**	**08**
	Interpersonal Skills: Emotional Intelligence, Leadership & Motivation, Conflict Management & Negotiation, Time Management, Assertiveness, Decision Making **Start-up Skills:** Financial Literacy, Risk Assessment, Data Analysis (e.g. Consumer Behaviour, Market Trends, etc.)	
6	**CORPORATE ETHICS**	**02**
	Intellectual Property Rights: Copyrights, Trademarks, Patents, Industrial Designs, Geographical Indications, Integrated Circuits, Trade Secrets (Undisclosed Information) **Case Studies:** Cases related to Business/ Corporate Ethics	

List of assignments: (In the form of Short Notes, Questionnaire/ MCQ Test, Role Play, Case Study, Quiz, etc.)	
Sr. No.	**Title of Experiment**
1	Cover Letter and Resume
2	Short Proposal
3	Meeting Documentation
4	Writing a Technical Paper/ Analyzing a Published Technical Paper
5	Writing a SOP
6	IPR
7	Interpersonal Skills
Note:	
1	The Main Body of the project/book report should contain minimum 25 pages (excluding Front and Back matter).

2	The group size for the final report presentation should not be less than 5 students or exceed 7 students.
3	There will be an end–semester presentation based on the book report.
Assessment:	
Term Work:	
1	Term work shall consist of minimum 8 experiments.
2	The distribution of marks for term work shall be as follows: Assignment : 10 Marks Attendance : 5 Marks Presentation slides : 5 Marks Book Report (hard copy) : 5 Marks
3	The final certification and acceptance of term work ensures the satisfactory performance of laboratory work and minimum passing in the term work.
Internal oral: **Oral Examination will be based on a GD & the Project/Book Report presentation.**	
	Group Discussion : 10 marks Project Presentation : 10 Marks Group Dynamics : 5 Marks
Books Recommended: Textbooks and Reference books	
1	Arms, V. M. (2005). *Humanities for the engineering curriculum: With selected chapters from Olsen/Huckin: Technical writing and professional communication, second edition*. Boston, MA: McGraw-Hill.
2	Bovée, C. L., &Thill, J. V. (2021). *Business communication today*. Upper Saddle River, NJ: Pearson.
3	Butterfield, J. (2017). *Verbal communication: Soft skills for a digital workplace*. Boston, MA: Cengage Learning.
4	Masters, L. A., Wallace, H. R., & Harwood, L. (2011). *Personal development for life and work*. Mason: South-Western Cengage Learning.
5	Robbins, S. P., Judge, T. A., & Campbell, T. T. (2017). *Organizational behaviour*. Harlow, England: Pearson.
6	Meenakshi Raman, Sangeeta Sharma (2004) Technical Communication, Principles and Practice. Oxford University Press
7	Archana Ram (2018) Place Mentor, Tests of Aptitude for Placement Readiness. Oxford University Press
8	Sanjay Kumar &PushpLata (2018). Communication Skills a workbook, New Delhi: Oxford University Press.

Course Code	Course Name	Credits
CSM501	Mini Project 2A	02

Objectives	
1	To understand and identify the problem
2	To apply basic engineering fundamentals and attempt to find solutions to the problems.
3	Identify, analyze, formulate and handle programming projects with a comprehensive and systematic approach
4	To develop communication skills and improve teamwork amongst group members and inculcate the process of self-learning and research.
Outcome: Learner will be able to…	
1	Identify societal/research/innovation/entrepreneurship problems through appropriate literature surveys
2	Identify Methodology for solving above problem and apply engineering knowledge and skills to solve it
3	Validate, Verify the results using test cases/benchmark data/theoretical/ inferences/experiments/simulations
4	Analyze and evaluate the impact of solution/product/research/innovation /entrepreneurship towards societal/environmental/sustainable development
5	Use standard norms of engineering practices and project management principles during project work
6	Communicate through technical report writing and oral presentation. ● The work may result in research/white paper/ article/blog writing and publication ● The work may result in business plan for entrepreneurship product created ● The work may result in patent filing.
7	Gain technical competency towards participation in Competitions, Hackathons, etc.
8	Demonstrate capabilities of self-learning, leading to lifelong learning.
9	Develop interpersonal skills to work as a member of a group or as leader
Guidelines for Mini Project	
1	Mini project may be carried out in one or more form of following: Product preparations, prototype development model, fabrication of set-ups, laboratory experiment development, process modification/development, simulation, software development, integration of software (frontend-backend) and hardware, statistical data analysis, creating awareness in society/environment etc.
2	Students shall form a group of 3 to 4 students, while forming a group shall not be allowed less than three or more than four students, as it is a group activity.
3	Students should do survey and identify needs, which shall be converted into problem statement for mini project in consultation with faculty supervisor or head of department/internal committee of faculties.
4	Students shall submit an implementation plan in the form of Gantt/PERT/CPM chart, which will cover weekly activity of mini projects.
5	A logbook may be prepared by each group, wherein the group can record weekly work progress, guide/supervisor can verify and record notes/comments.
6	Faculty supervisors may give inputs to students during mini project activity; however, focus shall be on self-learning.
7	Students under the guidance of faculty supervisor shall convert the best solution into a working model using various components of their domain areas and demonstrate.
8	The solution to be validated with proper justification and report to be compiled in standard format of University of Mumbai. Software requirement specification (SRS) documents, research papers, competition certificates may be submitted as part of

	annexure to the report.
9	With the focus on self-learning, innovation, addressing societal/research/innovation problems and entrepreneurship quality development within the students through the Mini Projects, it is preferable that a single project of appropriate level and quality be carried out in two semesters by all the groups of the students. i.e. Mini Project 2 in semesters V and VI.
10	However, based on the individual students or group capability, with the mentor's recommendations, if the proposed Mini Project adhering to the qualitative aspects mentioned above, gets completed in odd semester, then that group can be allowed to work on the extension of the Mini Project with suitable improvements/modifications or a completely new project idea in even semester. This policy can be adopted on a case by case basis.

Term Work		
The review/ progress monitoring committee shall be constituted by the heads of departments of each institute. The progress of the mini project to be evaluated on a continuous basis, based on the SRS document submitted. minimum two reviews in each semester.		
In continuous assessment focus shall also be on each individual student, assessment based on individual's contribution in group activity, their understanding and response to questions.		
Distribution of Term work marks for both semesters shall be as below:		**Marks 25**
1	Marks awarded by guide/supervisor based on logbook	10
2	Marks awarded by review committee	10
3	Quality of Project report	05
Review / progress monitoring committee may consider following points for assessment based on either one year or half year project as mentioned in general guidelines		
One-year project:		
1	In one-year project (sem V and VI), first semester the entire theoretical solution shall be made ready, including components/system selection and cost analysis. Two reviews will be conducted based on a presentation given by a student group. – First shall be for finalization of problem – Second shall be on finalization of proposed solution of problem.	
2	In the second semester expected work shall be procurement of component's/systems, building of working prototype, testing and validation of results based on work completed in an earlier semester. □ First review is based on readiness of building working prototype to be conducted. □ Second review shall be based on poster presentation cum demonstration of working model in the last month of the said semester.	
Half-year project:		
1	In this case in one semester students' group shall complete project in all aspects including, – Identification of need/problem – Proposed final solution – Procurement of components/systems – Building prototype and testing	
2	Two reviews will be conducted for continuous assessment, – First shall be for finalization of problem and proposed solution – Second shall be for implementation and testing of solution.	

Mini Project shall be assessed based on following points	
1	Clarity of problem and quality of literature Survey for problem identification
2	Requirement Gathering via SRS/ Feasibility Study
3	Completeness of methodology implemented
4	Design, Analysis and Further Plan
5	Novelty, Originality or Innovativeness of project
6	Societal / Research impact
7	Effective use of skill set : Standard engineering practices and Project management standard
8	Contribution of an individual's as member or leader
9	Clarity in written and oral communication
10	Verification and validation of the solution/ Test Cases
11	Full functioning of working model as per stated requirements
12	Technical writing /competition/hackathon outcome being met

In one year project (sem V and VI), first semester evaluation may be based on first 10 criteria and remaining may be used for second semester evaluation of performance of students in mini projects.
In case of half year projects (completing in V sem) all criteria in generic may be considered for evaluation of performance of students in mini projects.

Guidelines for Assessment of Mini Project Practical/Oral Examination:	
1	Report should be prepared as per the guidelines issued by the University of Mumbai.
2	Mini Project shall be assessed through a presentation and demonstration of working model by the student project group to a panel of Internal and External Examiners preferably from industry or research organizations having experience of more than five years approved by the head of Institution.
3	Students shall be motivated to publish a paper/participate in competition based on the work in Conferences/students competitions.

Program Structure for Third Year Cyber Security
UNIVERSITY OF MUMBAI (With Effect from 2022-2023)

Semester VI

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned		
		Theory	Pract. Tut.	Theory	Pract.	Total
CSC601	Cryptography and Network Security	3	--	3	--	3
CSC602	Application Security and Secure Coding Principles	3	--	3		3
CSC603	Ethical Hacking & Digital Forensic	3	--	3	--	3
CSC604	Web X.0	3	--	3	--	3
CSDLO601x	**Department Level Optional Course -2**	3	--	3	--	3
CSL601	CNS Lab	--	2	--	1	1
CSL602	AS and SC Lab	--	2	--	1	1
CSL603	EH and DF Lab	--	2	--	1	1
CSL604	Web Lab	--	2	--	1	1
CSL605	ICT Security Lab (SBL)	--	4	--	2	2
CSM601	Mini Project Lab: 2B Application Security	--	4[$]	--	2	2
Total		**15**	**16**	**15**	**08**	**23**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract. &oral	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test 2	Avg					
CSC601	Cryptography and Network Security	20	20	20	80	3	--	--	100
CSC602	Application Security and Secure Coding Principles	20	20	20	80	3	--	--	100
CSC603	Ethical Hacking & Digital Forensic	20	20	20	80	3	--	--	100
CSC604	Web X.0	20	20	20	80	3	--	--	100
CSDLO601x	**Department Level Optional Course -2**	20	20	20	80	3	--	--	100
CSL601	CNS Lab	--	--	--	--	--	25	25	50
CSL602	AS and SC Lab	--	--	--	--	--	25	--	25
CSL603	EH and DF Lab	--	--	--	--	--	25	-	25
CSL604	Web Lab						25	25	50
CSL605	ICT Security Lab (SBL)	--	--	--	--	--	50	25	75
CSM601	Mini Project Lab: 2B Application Security	--	--	--	--	--	25	25	50
Total		**--**	**--**	**100**	**400**	**--**	**175**	**100**	**775**

$ indicates work load of Learner (Not Faculty), for Mini-Project. Students can form groups with minimum 2(Two) and not more than 4(Four). Faculty Load: 1hour per week per four groups.

CSDLO601X	**Department Optional Course – 2**
CSDLO6011	Enterprise Network Design
CSDLO6012	Blockchain Technology
CSDLO6013	Virtualization and cloud security
CSDLO6014	Cyber Security and Ransom ware incident response system

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned		
		Theory	Practical	Theory	Practical	Total
CSC601	Cryptography & Network Security	3	--	3	--	3

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		Test1	Test 2	Avg.					
CSC601	Cryptography & Network Security	20	20	20	80	3	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	The basic concepts of computer and Network Security
2	Various cryptographic algorithms including secret key management and different authentication techniques.
3	Different types of malicious Software and its effect on the security
4	Various secure communication standards including IPsec, SSL/TLS and email
5	The Network management Security and Network Access Control techniques in Computer Security
6	Different attacks on networks and infer the use of firewalls and security protocols.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Explain the fundamentals concepts of computer security and network security	L1,L2
2	Identify the basic cryptographic techniques using classical and block encryption methods	L1
3	Study and describe the system security malicious softwares	L1,L2
4	Describe the Network layer security, Transport layer security and application layer security	L1,L2
5	Explain the need of network management security and illustrate the need for NAC	L1,L2
6	Identify the function of an IDS and firewall for the system security	L1

Prerequisite: Basic concepts of Computer Networks & Network Design, Operating System

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic concepts of Computer Networks & Network Design, Operating System	**02**	-

I	Introduction to Network Security & cryptography	Computer security and Network Security(Definition), CIA, Services, Mechanisms and attacks,The OSI security architecture, Network security model Classical Encryption techniques (mono-alphabetic and poly-alphabetic substitution techniques: Vigenere cipher, playfair cipher, transposition techniques: keyed and keyless transposition ciphers). Introduction to steganography. **Self-Learning Topic**: Study some more classical encryption techniques and solve more problems on all techniques. Homomorphic encryption in cloud computing	**07**	CO1
II	Cryptography: Key management, distribution and user authentication	Block cipher modes of operation,Data Encryption Standard, Advanced Encryption Standard (AES). RC5 algorithm. Public key cryptography: RSA algorithm. Hashing Techniques: SHA256, SHA-512, HMAC and CMAC, Digital Signature Schemes – RSA, DSS. Remote user Authentication Protocols, Kerberos, Digital Certificate: X.509, PKI **Self-Learning Topic**: Study working of elliptical curve digital signature and its benefits over RSA digital signature..	**09**	CO2
III	Malicious Software	SPAM,Trojan horse, Viruses, Worms ,System Corruption, Attack Agents, Information Theft, Trapdoor, Keyloggers, Phishing, Backdoors, Rootkits, Denial of Service Attacks, Zombie **Self-Learning Topic**: Study the recent malicious softwares and their effects. How quantum computing is a threat to current security algorithms.	**04**	CO3
IV	IP Security, Transport level security and Email Security	IP level Security: Introduction to IPSec, IPSec Architecture, Protection Mechanism (AH and ESP), Transport level security: VPN. Need Web Security considerations, Secure Sockets Layer (SSL)Architecture,Transport Layer Security (TLS),HTTPS, Secure Shell (SSH) Protocol Stack. Email Security: Secure Email S/MIME **Self-Learning Topic**: Study gmail security and privacy from gmail help	**07**	CO4
V	Network Management Security and Network Access Control	Network Management Security:SNMPv3, NAC:Principle elements of NAC,Principle NAC enforcement methods, How to implement NAC Solutions, Use cases for network access control	**6**	CO5

		Self-Learning Topic: Explore any opensource network management security tool		
VI	System Security	IDS, Firewall Design Principles, Characteristics of Firewalls, Types of Firewalls **Self-Learning Topic**: Study firewall rules table	**04**	CO6

Text Books

1 William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.

2 Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill.

3 Mark Stamp's Information Security Principles and Practice, Wiley

4 Bernard Menezes, "Cryptography & Network Security", Cengage Learning.

References:

1 Applied Cryptography,Protocols,Algorithms and Source Code in C,Bruce Schneier,Wiley.

2 Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.

3 www.rsa.com

Online Resources

1. https://swayam.gov.in/
2. https://nptel.ac.in/
3. https://www.coursera.org/

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

- **Question paper format**

  - Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**

  - **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

  - A total of **four questions** need to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical /Oral	Tutorial	Total
CSC602	Application Security and Secure Coding Principles	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSC602	Application Security and Secure Coding Principles	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To introduce the basic concepts of application security
2	To understand Security related to Operating Systems, Internet and Social Networking Sites
3	To Understand Email Communication & Mobile Device Security
4	To Understand Cloud and Network Security
5	To introduce the basic concepts of secure coding practices
6	To apply the knowledge of application security to safeguard an application

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand & identify different application security threats.	L1,L2
2	Analyze the Security related to Operating Systems, Internet and Social Networking Sites	L1,L2,L3,L4
3	Understand the security aspects related to Email Communication & Mobile Device	L1,L2
4	Understand Cloud and Network Security	L1,L2
5	Evaluate the different Secure Coding Practices	L1,L2,L3,L4,L5
6	Apply application security testing concepts to safeguard	L1,L2,L3

Prerequisite: Data Security and Crytography

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Data Security Fundamentals and cryptography	**02**	--
I	Application Security	Web Application Security ,SQL Injection ,Forms and Scripts ,Cookies and Session	**08**	CO1

		Management ,General Attacks, Regular Application Security ,Running Privileges ,Application Administration ,Integration with OS Security ,Application Updates ,Spyware and Adware ,Network Access. **Self-learning Topics:** Remote Administration Security		
II	Security related to Operating Systems, Internet and Social Networking Sites	Security Recommendations for Windows Operating Systems, Mac OS, Studying Web Browser Concepts, Immediate Messaging Security, Child Online Safety, **Self-learning Topics:** Understanding Social Networking Concepts, and Facebook and Twitter Security Settings	**08**	CO2
III	Email Communication & Mobile Device Security	Understanding Email Security Concepts, Email Security Procedures, Knowing Mobile Device Security Concepts, Mobile Security Procedures, Understanding How to Secure iPhone, iPad, Android, and Windows Devices **Self-learning Topics:** How to Secure iPhone, iPad, Android, and Windows Devices	**06**	CO3
IV	Embedded Application and Cloud Security	Embedded Applications Security, Security of Embedded Applications Security Conclusions, Remote Administration Security, Reasons for Remote Administration, Remote Administration Using a Web Interface, Authenticating Web-Based Remote Administration, Custom Remote Administration Understanding Cloud Concepts, Securing Against Cloud Security Threats, Addressing Cloud Privacy Issues **Self-learning Topics:** Understanding Various Networking Concepts & Setting Up a Wireless Network in Windows and Mac. Understanding Wireless Network Security Countermeasures	**07**	CO4
V	Secure Coding Practices	Input Validation, Authentication and Authorization, Cryptography, Session Management, **Self-learning Topics:** Error Handling	**04**	CO5
VI	Application Security Testing	Introduction Application Security Testing, Different Application Security Testing – SAST, DAST, IAST, MAST. **Self-learning Topics:** Cross-Site Scripting Issues ,SQL Injection Attacks	**04**	CO6

Text Books:

1. Nina Godbole, “Information Systems Security”, Wiley Publication
2. Robert Bragg,Mark Rhodes-ousley,Keith Strasssberg “The complete reference Network Security” TMH , 2004

References Books:

1. Mark G. Graff, Kenneth R. van Wyk, “Secure Coding: Principles and Practices”, O'Reilly Media, Inc
2. William (Chuck) Easttom II, “Computer Security Fundamentals, 4th Edition”, Pearson publication

Online References:

1. https://nptel.ac.in/courses/106106146
2. https://www.coursera.org/specializations/secure-coding-practices?
3. https://www.coursera.org/learn/systems-application-security-sscp

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

- **Question paper format**

  - Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**

  - **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

  - A total of **four questions** need to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical/ Oral	Tutorial	Total
CSC603	Ethical hacking and digital forensics	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSC603	Ethical hacking and digital forensics	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand ethical hacking and different phases of an attack
2	To learn various tools used for hacking
3	To understand various steps involved in the Digital Forensics Methodology
4	To learn about the Digital Forensic Data Acquisition
5	To learn about Digital Forensic Investigation and Analysis
6	To learn about the steps involved in creating an investigation report

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Define the concept of ethical hacking and explore different phases in ethical hacking	L1,L2
2	Examine different tools for hacking and penetration testing	L1,L2,L3
3	Understand the need for Digital Forensics and its Life Cycle	L1,L2
4	Implement various Digital Forensic techniques to acquire a forensically sound copy of evidence	L1,L2,L3
5	Analyze the various pieces of evidence acquired after applying various forensic tools	L1,L2,L3,L4
6	Compile a detailed Forensic report after completing a forensic investigation	L6

Prerequisite:

1) Computer Networks
2) Cryptography and System Security

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping

0	Prerequisite	Computer Networks, cryptography and system security	**02**	
I	Computer Networks	**Introduction to Ethical Hacking**: Introduction to Ethical Hacking. Hacker Classifications: The Hats. Phases of Hacking. Introduction to footprinting, footprinting tools. Scanning methodology and tools. Enumeration techniques and enumeration tools. **Self-learning Topics:** OWASP top 10 Attacks	**06**	CO1
II	Computer Networks	**Introduction to penetration testing:** System hacking, hacking tools, Introduction to penetration testing and social engineering, Phases of penetration testing. **Self-learning Topics:** Google Hacking (GHDB) and Doxing	**04**	CO2
III		**Digital Forensics and Incident Response:** Introduction to Digital Forensics and Digital Evidence, The Need for Digital Forensics, Types of Digital Forensics, Digital Forensics Life Cycle. **Incident and Initial Response:** Introduction to Computer Security Incident, Goals of Incident response, Incident Response Methodology, Initial Response, Formulating Response Strategy. **Self-learning Topics:** New Challenges of Digital Forensic Investigations	**07**	CO3
IV		**Forensic Duplication and Acquisition:** **Forensic Duplication:** Introduction to Forensic Duplication, Types of Forensic Duplicates, Introduction to Forensic Duplication Tools. **Data Acquisition:** Introduction to Static and Live/Volatile Data, Static Data Acquisition from Windows (FTK Imager), Static Data Acquisition from Linux (dd/dcfldd), Live Data Acquisition from Windows (FTK Imager). Network Forensics (wireshark) **Self-learning Topics:** Open and Proprietary Tools for Digital Forensics, Network Forensic Tools	**07**	CO4
V		**Forensic Investigation and Analysis:** Investigating Registry Files, Investigating Log Files, Data Carving (Bulk Extractor), Introduction to Forensic Analysis, Live Forensic Analysis, Forensic Analysis of acquired data in Linux, Forensic Analysis of acquired data in Windows **Self-learning Topics:** Open and Proprietary Tools for Forensics Investigation	07	CO5
VI		**Evidence Handling and Forensic Reporting:** **Evidence Handling:** Faraday's Bag, Characteristics of an Evidence, Types of Evidence, Evidence Handling Methodology, Chain of Custody. **Forensic Reporting:** Goals of a Report, Layout of an Investigative Report, Guidelines for writing a report, Sample Forensic Report **Self-learning Topics:** Case Study on Real Life Incidents.	**06**	CO6

Text Books:

1. EC-Council **"Ethical Hacking and Countermeasures Attack Phases",** Cengage Learning
2. Computer Security Principles **and Practice, William Stallings, Sixth Edition, Pearson Education**
3. Build your own Security Lab, Michael Gregg, Wiley India

References:

1. Kevin Smith**, "Hacking How to Hack - The ultimate Hacking Guide",** Hacking Intelligence
2. Kevin Beaver**, "Hacking for dummies"** Wiley publication
3. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley
4. Digital Forensics by Nilakshi Jain & Kalbande, Wiley

Online References:

1. https://freevideolectures.com/course/4070/nptel-ethical-hacking
2. https://owasp.org/www-project-top-ten/
3. https://www.computersecuritystudent.com/
4. http://www.opentechinfo.com/learn-use-kali-linux/
5. https://pentesterlab.com
6. https://www.exploit-db.com/google-hacking-database

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

- **Question paper format**

  - Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**

  - **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

  - A total of **four questions** need to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical/ Oral	Tutorial	Total
CSC604	WEB X.0	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSC604	WEB X.0	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand the digital evolution of web technology.
2	To learn TypeScript and understand how to use it in web applications.
3	To learn the fundamentals of Node.js.
4	To make Node.js applications using the express framework.
5	To enable the use of AngularJS to create web applications that depend on the Model-View-Controller Architecture.
6	To gain expertise in a leading document-oriented NoSQL database, designed for speed, scalability, and developer agility using MongoDB.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand the basic concepts related to web analytics and semantic web.	L1,L2
2	Understand how TypeScript can help you eliminate bugs in your code and enable you to scale your code.	L1,L2
3	Develop back-end applications using Node.js.	L1,L2,L3
4	Construct web based Node.js applications using Express.	L1,L2,L3
5	Understand AngularJs framework and build dynamic, responsive single-page web applications.	L1,L2,L3
6	Apply MongoDB for frontend and backend connectivity using REST API.	L1,L2,L3

Prerequisite: HTML5, CSS3, JavaScript.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	**Introduction to HTML5,CSS3, Basics of JavaScript**	**02**	-
I	Introduction to WebX.0	Evolution of WebX.0; **Web Analytics 2.0**: Introduction to Web Analytics, Web Analytics 2.0, Clickstream Analysis, Strategy to choose your web analytics tool,	**04**	CO1

		Measuring the success of a website; **Web3.0 and Semantic Web**: Characteristics of Semantic Web, Components of Semantic Web, Semantic Web Stack, N-Triples and Turtle, Ontology, RDF and SPARQL **Self-learning Topics**: Semantic Web Vs AI, SPARQL Vs SQL.		
II	TypeScript	Overview, TypeScript Internal Architecture, TypeScript Environment Setup, TypeScript Types, variables and operators, Decision Making and loops, TypeScript Functions, TypeScript Classes and Objects, TypeScript Inheritance and Modules **Self-learning Topics**: Javascript Vs TypeScript	**06**	CO2
III	Node.js	Introducing the Node.js-to-Angular Stack (MEAN Stack), Environment setup for Node.js , First app, Asynchronous programming, Callback concept, Event loops, REPL, NPM, Event emitter, Buffers, Streams, Networking module, File system, Web module. **Self-learning Topics:** Node.js with MongoDB.	**07**	CO3
IV	Express	Introduction to Express ,Installing Express,Creating First Express application,The application, request, and response objects,Configuring Routes,Understanding Middleware,cookies, Session, Authentication **Self-learning Topics:** ExpressJs Templates	**06**	CO4
V	Introduction to AngularJS	Overview of AngularJS, Need of AngularJS in real websites, AngularJS modules, AngularJS built-in directives, AngularJS custom directives, AngularJS expressions,AngularJS Data Binding, AngularJS filters, AngularJS controllers, AngularJS scope, AngularJS dependency injection, AngularJS Services, Form Validation, Routing. **Self-learning Topics:** MVC model, DOM model.	**07**	CO5
VI	MongoDB and Building REST API using MongoDB	**MongoDB**: Understanding MongoDB, MongoDB Data Types, Administering User Accounts, Configuring Access Control, Adding the MongoDB Driver	**07**	CO6

		to Node.js, Connecting to MongoDB from Node.js, Accessing and Manipulating Databases, Manipulating MongoDB Documents from Node.js, Accessing MongoDB from Node.js, Using Mongoose for Structured Schema and Validation. **REST API**: Examining the rules of REST APIs, Evaluating API patterns, Handling typical CRUD functions (Create, Read, Update, Delete), Using Express and Mongoose to interact with MongoDB, Testing API endpoints. **Self-learning Topics**: MongoDB vs SQL Databases		

Text & Reference Books:

1.Boris Cherny, "Programming TypeScript- Making Your Javascript Application Scale", O'Reilly Media Inc.
2. Amos Q. Haviv, "MEAN Web Development" , PACKT Publishing
3.Brad Dayley, Brendan Dayley, Caleb Dayley, "Node.js, MongoDB and Angular Web Development:The definitive guide to using the MEAN stack to build web applications", 2nd Edition, Addison-Wesley Professional
5. Adam Bretz and Colin J. Ihrig, "Full Stack JavaScript Development with MEAN", SitePoint.
4. Dr. Deven Shah, "Advanced Internet Programming", StarEdu Solutions.
References:
1. Simon Holmes Clive Harber, "Getting MEAN with Mongo, Express, Angular, and Node", Manning Publications.
2. Yakov Fain and Anton Moiseev, "TypeScript Quickly", Manning Publications.

Online References:

1.https://www.coursera.org
2. https://udemy.com
3. https://www.tutorialspoint.com/meanjs/meanjs_overview.htm

Assessment:
Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**

- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

A total of **four questions** need to be answered

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned		
		Theory	Practical	Theory	Practical	Total
CSL601	CNS Lab	--	2	--	1	1

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		Test1	Test 2	Avg.					
CSL601	CNS Lab	--	--	--	--	--	25	25	50

Lab Objectives:

Sr No	Lab Objectives
1	To apply the knowledge of symmetric cryptography to implement classical ciphers
2	To analyze and implement public key encryption algorithms, hashing and digital signature algorithms
3	To explore the different network reconnaissance tools to gather information about networks
4	To explore the tools like sniffers, port scanners and other related tools for analyzing
5	To Scan the network for vulnerabilities and simulate attacks
6	To set up intrusion detection systems using open source technologies and to explore email security.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
Upon Completion of the course the learner/student should be able to:		
1	Illustrate symmetric cryptography by implementing classical ciphers	L1,L2,L3
2	Demonstrate Key management,distribution and user authentication	L1,L2,L3
3	Explore the different network reconnaissance tools to gather information about networks	L1,L2,L3
4	Use tools like sniffers, port scanners and other related tools for analyzing packets in a network	L1,L2,L3
5	Use open source tools to scan the network for vulnerabilities and simulate attacks	L1,L2,L3
6	Demonstrate the network security system using open source tools	L1,L2,L3

Prerequisite: Basic concepts of Computer Networks & Network Design, Operating System

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7 2. 4 GB RAM 3. 500 GB Hard disk	GPG tool, WHOIS, dig,traceroute, nslookup, wireshark, nmap, keylogger, kali lunix,

DETAILED SYLLABUS:

Sr. No.	Detailed Content	Hours	LO Mapping
I	Classical Encryption techniques (mono-alphabetic and poly-alphabetic substitution techniques: Vigenere cipher, playfair cipher)	**04**	**LO1**
II	1)Block cipher modes of operation using a)Data Encryption Standard b)Advanced Encryption Standard (AES). 2)Public key cryptography: RSA algorithm. 3)Hashing Techniques:HMAC using SHA 4)Digital Signature Schemes – RSA, DSS.	**05**	**LO2**
III	1) Study the use of network reconnaissance tools like WHOIS, dig,traceroute, nslookup to gather information about networks and domain registrars. 2)Study of packet sniffer tools wireshark, :- a. Observer performance in promiscuous as well as non-promiscuous mode. b. Show the packets can be traced based on different filters.	**04**	**LO3**
IV	1) Download and install nmap. 2) Use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.	**04**	**LO4**
V	a)Keylogger attack using a keylogger tool. b) Simulate DOS attack using Hping or other tools c) Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.	**05**	**LO5**
VI	1) Set up IPSec under Linux. 2) Set up Snort and study the logs. 3) Explore the GPG tool to implement email security	**04**	**LO6**

Text Books

1 Build your own Security Lab, Michael Gregg, Wiley India.
2 CCNA Security, Study Guide, TIm Boyles, Sybex.
3 Hands-On Information Security Lab Manual, 4th edition, Andrew Green, Michael Whitman, Herbert Mattord.
4 The Network Security Test Lab: A Step-by-Step Guide Kindle Edition, Michael Gregg.

References:

1 Network Security Bible, Eric Cole, Wiley India.
2 Network Defense and Countermeasures, William (Chuck) Easttom.
3 Principles of Information Security + Hands-on Information Security Lab Manual, 4th Ed. , Michael E. Whitman , Herbert J. Mattord.

Online Resource:

1. http://cse29-iiith.vlabs.ac.in/
2. https://www.dcode.fr/en

List of Experiments.:

1. Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.
2. Design and Implement a product cipher using Substitution ciphers.
3. Cryptanalysis or decoding Playfair, vigenere cipher.
4. Encrypt long messages using various modes of operation using AES or DES
5. Cryptographic Hash Functions and Applications (HMAC): to understand the need, design and applications of collision resistant hash functions.
6. Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA
7. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.
8. Study of packet sniffer tools wireshark: -
   a. Observer performance in promiscuous as well as non-promiscuous mode.
   b. Show the packets can be traced based on different filters.
9. Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.
10. Study of malicious software using different tools:
    a) Keylogger attack using a keylogger tool.
    b) Simulate DOS attack using Hping or other tools
    c) Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.
11. Study of Network security by
    a) Set up IPSec under Linux.
    b) Set up Snort and study the logs.
    c) Explore the GPG tool to implement email security

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus

		Teaching Scheme (Contact Hours)			Credits Assigned			
Course Code	**Course Name**	**Theory**	**Practical**	**Tutorial**	**Theory**	**Practical & Oral**	**Tutorial**	**Total**
CSL602	AS and SC Lab	--	2	--	--	1	--	01

Course Code	**Course Name**	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment			End Sem. Exam			
		Test 1	Test 2	Avg. of 2 Tests				
CSL602	AS and SC Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr No	Lab Objectives
1	To understand cyber-attacks and defense strategies.
2	To understand underlying principles of access control mechanisms
3	To explore software vulnerabilities, attacks and protection mechanisms of wireless networks and protocols, mobile devices and web applications
4	To develop and mitigate security management and policies
5	To understand and explore techniques used in digital forensics
6	To understand and use different tools.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
Upon Completion of the course the learner/student should be able to:		
1	Understand cyber attacks and apply access control policies and control mechanisms.	L1,L2
2	Identify malicious code and targeted malicious code	L1,L2
3	Detect and counter threats to web applications	L1,L2
4	Understand the vulnerabilities of Wi-Fi networks and explore different measures to secure wireless protocols, WLAN and VPN networks	L1,L2
5	Understand the ethical and legal issues associated with cyber crimes and be able to mitigate impact of crimes with suitable policies	L1,L2
6	Use different forensic tools to acquire and duplicate data from compromised systems and analyze the same	L1,L2

Prerequisite: Data Security

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7 2. 4 GB RAM 3. 500 GB Hard disk	Cracking tools, RATS, flawfinder,we-application vulnerabilities toolsWapiti etc.Kali Lunix,Cisco packet tracer,steganographic tools, Nessus tools etc.

DETAILED SYLLABUS:

Sr. No.	Experiment Name	Hours	LO
1	Use Password cracking using tools like John the Ripper/Cain and Abel/ Ophcrack to detect weak passwords.	**01**	LO1
2	Static code analysis using open source tools like RATS, Flawfinder etc.	**02**	LO2
3	Explore web-application vulnerabilities using open source tools like Wapiti, browser exploitation framework (BeEf), etc.	**02**	LO3
4	Performing a penetration testing using Metasploit (Kali Linux)	**02**	LO3
5	Exploring VPN security using Cisco Packet tracer(student edition)	**02**	LO4
6	Install and use a security app on an Android mobile	**02**	LO6
7	Vulnerability scanning using Nessus, Nikto (Kali Linux)	**02**	LO6
8	Detect SQL injection vulnerabilities in a website database using SQLMap	**02**	LO3, LO6
9	Exploring Router and VLAN security, setting up access lists using Cisco Packet tracer(student edition)	**02**	LO4
10	Exploring Authentication and access control	**02**	LO1
11	Use of steganographic tools like OpenStego, to detect data hiding or unauthorized file copying	**01**	LO3
12	Use the Nessus tool to scan the network for vulnerabilities.	**02**	LO6
13	Implement a code to simulate buffer overflow attack.	**02**	LO5
14	Set up IPSEC under LINUX	**02**	LO5

Text Books:

1. Build your own Security Lab, Michael Gregg, Wiley India
2. CCNA Security, Study Guide, Tim Boyles, Sybex
3. Web Application Hacker‘s Handbook, Dafydd Stuttard, Marcus Pinto, Wiley India

References Books:

1. Network Infrastructure Security, Randy Waver, Dawn Weaver, Cengage Learning
2. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus

		Teaching Scheme (Contact Hours)			Credits Assigned			
Course Code	**Course Name**	**Theory**	**Practical**	**Tutorial**	**Theory**	**Practical & Oral**	**Tutorial**	**Total**
CSL603	EH and DF Lab	--	2	--	--	1	--	01

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment			End Sem. Exam			
		Test 1	Test 2	Avg. of 2 Tests				
CSL603	EH and DF Lab	--	--	--	--	25	25	50

This course is designed so that a candidate can identify, analyze and remediate computer security breaches by learning and implementing the real-world scenarios in Cyber Investigations Laboratory, Network Security Laboratory and in Security and Penetration Testing Laboratory.

Lab Objectives:

Sr No	Lab Objectives
1	To detect the web application and browser vulnerabilities using various open-source tools
2	To explore the network vulnerabilities using various open-source tools
3	To conduct digital investigations that conform to accepted professional standards and are based on the investigative process, including the concept of the chain of evidence
4	To identify, preserve, examine, analyze, and report the findings from digital forensics investigation
5	To recover the digital evidences from various digital devices
6	To Explore various forensics tools in Kali Linux and use them to acquire, duplicate and analyze data and recover deleted data

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
Upon Completion of the course the learner/student should be able to:		
1	Explore and analyze different security tools to detect web application and browser vulnerabilities	L1,L2,L3
2	Explore and analyze network vulnerabilities using open-source tools	L1,L2,L3
3	Explore how to conduct a digital forensics investigation, including the concept of the chain of evidence	L1,L2,L3
4	Explore various forensics tools and use them to acquire, duplicate and analyze data and recover deleted data	L1,L2,L3
5	Report findings from digital forensic investigations	L1,L2,L3
6	Perform recovery of digital evidence from various digital devices using a	L1,L2,L3

	variety of software utilities	

Prerequisite: Computer Networks and Basic concept of security.

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7 2. 4 GB RAM 3. 500 GB Hard disk	Nikto/Wapiti/Burpsuite, Wireshark, TCP Dump, Ettercap / Bettercap, Kali Lunix, FTK Imager, Scalpel etc.

.

DETAIL SYALLBUS:

Sr. No.	Detailed Content	Hours	LO Mapping
1	To scan and audit web application vulnerability using open-source tools. Recommended Tools: Nikto / Wapiti / Burpsuite	**02**	LO1
2	To study and implement packet sniffing using open-source tools. Recommended Tools: Wireshark, TCP Dump	**02**	LO1
3	To study and implement session hijacking / man in the middle (MiTM) attack in a controlled virtual environment. Recommended Tools: Ettercap / Bettercap	**02**	LO2
4	To perform penetration testing and vulnerability exploitation. Recommended Tool: Metasploit (Kali Linux)	**02**	LO2
5	To perform static data acquisition from Windows OS Recommended Tool: FTK Imager	**02**	LO3
6	To acquire live data from Windows OS Recommended Tool: FTK Imager, TCP Dump	**02**	LO3
7	To perform static data acquisition from Linux OS Recommended Tool: dd, dcfldd	**02**	LO4
8	To perform static/live data acquisition from Linux Recommended Tool: Kali Linux, fdisk	**02**	LO4
9	To perform analysis of Forensic Duplicates Recommended Tool: Autopsy, bulk Extractor	**03**	LO4
10	To recover Evidence from Forensic Images Recommended Tool: Scalpel	**02**	LO5
11	To perform Data Carving from Forensic Images Recommended Tool: Bulk Extractor	**02**	LO5
12	Case Study on Chain of Custody and Evicence Integrity Validstion using Hash Values Recommended Tool: Hashdeep, md5sum	**03**	LO6

Text Books / References:

1. Build your own Security Lab, Michael Gregg, Wiley India
2. CCNA Security, Study Guide, Tim Boyles, Sybex.

3. Web Application Hacker‘s Handbook, Dafydd Stuttard, Marcus Pinto, Wiley India
4. Network Infrastructure Security, Randy Waver, Dawn Weaver, Cengage Learning.
5. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley.

Online References:

1. http://www.opentechinfo.com/learn-use-kali-linux/

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus

		Teaching Scheme (Contact Hours)			Credits Assigned			
Course Code	**Course Name**	**Theory**	**Practical**	**Tutorial**	**Theory**	**Practical & Oral**	**Tutorial**	**Total**
IoTL604	Web Lab	--	2	--	--	1	--	01

Course Code	**Course Name**	**Examination Scheme**						
		Theory Marks				**Term Work**	**Practical/ Oral**	**Total**
		Internal assessment			**End Sem. Exam**			
		Test1	**Test 2**	**Avg. of 2 Tests**				
IoTL604	Web Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr No	**Lab Objectives**
1	To familiarize with Open Source Tools for Web Analytics and Semantic Web.
2	To familiarize with Programming in TypeScript for designing Web Applications.
3	To orient students for developing Node.js backend applications.
4	To orient students for developing Express applications.
5	To understand AngularJS Framework for Single Page Web Applications.
6	To use REST API and MongoDB for Frontend and Backend Connectivity.

Lab Outcomes:

Sr. No.	**Lab Outcomes**	**Cognitive Levels of Attainment as per Bloom's Taxonomy**
Upon Completion of the course the learner/student should be able to:		
1	Understand open source tools for web analytics and semantic web apps development and deployment.	L1, L2
2	Understand the basic concepts of TypeScript for designing web applications.	L1, L2, L3
3	Construct back-end applications using Node.js.	L1, L2,L3
4	Construct back end applications using Express.	L1, L2,L3
5	Implement Single Page Applications using AngularJS Framework.	L1, L2, L3
6	Develop REST web services using MongoDB.	L1, L2, L3

Prerequisite: HTML5,CSS3 and Basics of JavaScript

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7 2. 4 GB RAM 3. 500 GB Hard disk	Angular IDE, Visual Studio Code, Notepad++, Python Editors, MySQL, XAMPP, MongoDB, JDK

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
I	Web Analytics & Semantic Web	Study **Any 1** tool in each 1. Study web analytics using open source tools like Matomo, Open Web Analytics, AWStats, Countly, Plausible. 2. Study Semantic Web Open Source Tools like Apache TinkerPop, RDFLib, Apache Jena, Protégé, Sesame.	**02**	LO1
II	TypeScript	Perform **Any 2** from the following 1. Small code snippets for programs like Hello World, Calculator using TypeScript. 2. Inheritance example using TypeScript 3. Access Modifiers example using TypeScript 4. Building a Simple Website with TypeScript	**04**	LO2
III	Node.js	Perform **Any 2** from the following 1. Build Hello World App in Node.js 2. Stream and Buffer in Node.js 3. Modules in Node.js(Networking, File system, Web module)	**06**	LO3
IV	Express	Perform **Any 2** from the following 1. Configuring Express Settings and creating Express application using request and response objects. 2. Build Express application by Sending and Receiving Cookies. 3. Create an Express application to implement sessions.	**04**	LO4
V	AngularJs	Perform **Any 2** from the following 1.Create a simple HTML "Hello World" Project using AngularJS Framework and apply ng-controller, ng-model,expression and filters. 2.Implement a single page web application using AngularJS Framework including Services, Events,Validations (Create functions and add events,	**04**	LO5

		add HTML validators, using $valid property of Angular, etc.) 3.Create an application for like Students Record using AngularJS.		
VI	MongoDB and Building REST API using MongoDB	Perform **Any 2** from the following 1. Connect MongoDB withNode.js and perform CRUD operations. 2. Build a RESTful API using MongoDB. 3. Build a TypeScript REST API using MongoDB.	**06**	LO6

Text Books:

1. Learning Node.js Development, Andrew Mead, Packt Publishing
2. John Hebeler, Matthew Fisher, Ryan Blace, Andrew Perez -Lopez, "Semantic Web Programming", Wiley Publishing, Inc, 1st Edition, 2009.
3. Boris Cherny, "Programming TypeScript- Making Your Javascript Application Scale", O'Reilly Media Inc., 2019 Edition.
4. Adam Bretz and Colin J. Ihrig, "Full Stack JavaScript Development with MEAN", SitePoint Pty. Ltd., 2015 Edition.
5. Brad Dayley, Brendan Dayley, Caleb Dayley, "Node.js, MongoDB and Angular Web Development: The definitive guide to using the MEAN stack to build web applications", 2nd Edition, AddisonWesley Professional, 2018 Edition.

References:

1. Simon Holmes Clive Harber, "Getting MEAN with Mongo, Express, Angular, and Node", Manning Publications, 2019 Edition.
2. Yakov Fain and Anton Moiseev, "TypeScript Quickly", Manning Publications, 2020 Edition.
3. Dr. Deven Shah, "Advanced Internet Programming", StarEdu Solutions, 2019 Edition.
4. Ethan Brown ,Web Development with Node and Express",O'Reilly

Online Reference:

Sr. No.	Website Name
1.	https://www.w3schools.com/nodejs/
2.	https://www.tutorialspoint.com/mongodb/index.htm
3.	https://www.mongodb.com/basics

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus

		Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical & Oral	Tutorial	Total
CSL605	ICT Security Lab (SBL)	--	4	--	--	2	--	2

Subject Code	Subject Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL605	ICT Security Lab (SBL)	--	--	--	--	50	--	50

Lab Objectives:

Sr No	Lab Objectives
1	To be able to thoroughly understand and categorize various protocols and it's vulnerabilities
2	To Have in-depth and proper conceptual understanding of how the real world Cyber security works, and how technologies work hand-in-hand to create quantitative change in cyber security
3	To have an exact understanding of the real-time/hands on problems in the computer system and operating system and how to deal with them
4	To have an exact understanding of the various vulnerabilities found in web application
5	To understand buffer overflow mechanism
6	To understand various frameworks for security and hands-on tools related to forensics and security

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
Upon Completion of the course the learner/student should be able to:		
1	Analyze and understand different network protocols	L1,L2,L3
2	Analyze and understand which packets pass through firewall	L1,L2,L3
3	Test and exploit systems using various tools and understand the impact of hacking in real time machines	L1,L2,L3
4	Demonstrate hacking techniques in Linux using various tools	L1,L2
5	Demonstrate web application hacking methodology	L1,L2
6	Demonstrate and understand buffer overflow	L1,L2

Prerequisite: Basic of Computer Network and Network Design.

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7	Kali Lunix, Security Tools.

2. 4 GB RAM 3. 500 GB Hard disk	

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	Prerequisite	Basic knowledge of computer networking and network design.	**02**	
I	High level protocols	1. Cover protocols including but not only smtp, imap, pop, dns, nat, dnssec, tor, http,https, ftp, ssl, tls, starttls, smb,icmp and create list of programs used to operate these protocols. 2. Study generic vulnerabilities in these protocols such as smb 1 eternal blue and vulnerabilities in HTTP get and trace requests.	**04**	LO1
II	Low level protocol knowledge	1. Analyze headers and bits that are set to 1 and 0 in headers for different kinds of operations, see tcp and udp packets and how they're scanned by firewalls and ids. 2. Use different header bits in nmap to initiate scans which bypass or make firewalls more detectable.	**02**	LO2
III	System Hacking	1. To understand how a system is hacked and privilege escalation is done. 2. Understand Keystroke loggers,sniffers,covering tracks,hiding files.	**04**	LO3
IV	Linux Hacking	1. Port scan detection tools, Password cracking in Linux. 2. Session Hijacking, Application Security tools.	**04**	LO4
V	Web application hacking methodology	1. Do a web application pentest on vulnerable web applications create a report using web application pentest methodology such as OWASP testing guide.	**08**	LO 5
VI	Understanding Buffer overflow	1. Introduction to Buffer overflow , exploitation and defense .	**02**	LO 6

Text Books:

1. OWASP Testing Guide V4.0, Open Web Application Security Project.
2. Ethical Hacking with Kali Linux, HUGO HOFFMAN
3. Certified Ethical Hacker Study Guide v11,Kimberly Graves.

4. Web Application Security Handbook,2nd Edition, Dafydd Stuttard, Marcus Pinto, Wiley

References:

1. Network Security Bible, Eric Cole, Wiley India.
2. CISSP Study Guide, Sybex.
3. https://owasp.org/Top10/

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus

List of Experiments.:

1. Analyze the behavior of networking protocols when interacting with servers using CLI and generic tools.
2. Study the behavior of protections such as idf and firewalls when altering headers in network packets.
3. Use Metasploit to exploit (Kali Linux)
4. Study of understanding escalating privileges and how to hide files.
5. Use NMap scanner to perform port scanning of various forms – PING SCAN,ACK, SYN, NULL, XMAS .
6. Use Ettercap to perform session hijacking.
7. Perform SQL injection attack.
8. Demonstrate cross-site scripting attack.
9. Performing a Buffer Overflow Attack Using Metasploit.
10. Perform Brute force attack using Burp Suite.
11. Study of OSINT Framework.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
CSM601	Mini Project :2B IoT & Mobile App Based.	--	04	--	--	02	--	02

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Pract. /Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg.				
CSM601	Mini Project :2B IoT & Mobile App Based.	--	--	--	--	25	25	50

Course Objectives

1. To acquaint with the process of identifying the needs and converting it into the problem.
2. To familiarize the process of solving the problem in a group.
3. To acquaint with the process of applying basic engineering fundamentals to attempt solutions to the problems.
4. To inculcate the process of self-learning and research.

Course Outcome: Learner will be able to…

1. Identify problems based on societal /research needs.
2. Apply Knowledge and skill to solve societal problems in a group.
3. Develop interpersonal skills to work as member of a group or leader.
4. Draw the proper inferences from available results through theoretical/ experimental/simulations.
5. Analyse the impact of solutions in societal and environmental context for sustainable development.
6. Use standard norms of engineering practices
7. Excel in written and oral communication.
8. Demonstrate capabilities of self-learning in a group, which leads to life long learning.
9. Demonstrate project management principles during project work.

Guidelines for Mini Project

- Students shall form a group of 3 to 4 students, while forming a group shall not be allowed less than three or more than four students, as it is a group activity.
- Students should do survey and identify needs, which shall be converted into problem statement for mini project in consultation with faculty supervisor/head of department/internal committee of faculties.
- Students hall submit implementation plan in the form of Gantt/PERT/CPM chart, which will cover weekly activity of mini project.
- A log book to be prepared by each group, wherein group can record weekly work progress, guide/supervisor can verify and record notes/comments.
- Faculty supervisor may give inputs to students during mini project activity;however, focus shall be on self-learning.
- Students in a group shall understand problem effectively, propose multiple solution and select best possible solution in consultation with guide/ supervisor.
- Students shall convert the best solution into working model using various components of their domain areas and demonstrate.

- The solution to be validated with proper justification and report to be compiled in standard format of University of Mumbai.
- With the focus on the self-learning, innovation, addressing societal problems and entrepreneurship quality development within the students through the Mini Projects, it is preferable that a single project of appropriate level and quality to be carried out in two semesters by all the groups of the students. i.e. Mini Project 1 in semester III and IV. Similarly, Mini Project 2 in semesters V and VI.
- However, based on the individual students or group capability, with the mentor's recommendations, if the proposed Mini Project adhering to the qualitative aspects mentioned above gets completed in odd semester, then that group can be allowed to work on the extension of the Mini Project with suitable improvements/modifications or a completely new project idea in even semester. This policy can be adopted on case by case basis.

Guidelines for Assessment of Mini Project:

Term Work

- The review/ progress monitoring committee shall be constituted by head of departments of each institute. The progress of mini project to be evaluated on continuous basis, minimum two reviews in each semester.
- In continuous assessment focus shall also be on each individual student, assessment based on individual's contribution in group activity, their understanding and response to questions.
- Distribution of Term work marks for both semesters shall be as below;
    - Marks awarded by guide/supervisor based on log book : 10
    - Marks awarded by review committee : 10
    - Quality of Project report : 05

Review/progress monitoring committee may consider following points for assessment based on either one year or half year project as mentioned in general guidelines.

One-year project:

- In first semester entire theoretical solution shall be ready, including components/system selection and cost analysis. Two reviews will be conducted based on presentation given by students group.
    - First shall be for finalisation of problem
    - Second shall be on finalisation of proposed solution of problem.
- In second semester expected work shall be procurement of component's/systems, building of working prototype, testing and validation of results based on work completed in an earlier semester.
    - First review is based on readiness of building working prototype to be conducted.
    - Second review shall be based on poster presentation cum demonstration of working model in last month of the said semester.

Half-year project:

- In this case in one semester students' group shall complete project in all aspects including,
    - Identification of need/problem
    - Proposed final solution
    - Procurement of components/systems
    - Building prototype and testing
- Two reviews will be conducted for continuous assessment,
    - First shall be for finalisation of problem and proposed solution
    - Second shall be for implementation and testing of solution.

Assessment criteria of Mini Project.

Mini Project shall be assessed based on following criteria;

1. Quality of survey/ need identification
2. Clarity of Problem definition based on need.
3. Innovativeness in solutions
4. Feasibility of proposed problem solutions and selection of best solution

5. Cost effectiveness
6. Societal impact
7. Innovativeness
8. Cost effectiveness and Societal impact
9. Full functioning of working model as per stated requirements
10. Effective use of skill sets
11. Effective use of standard engineering norms
12. Contribution of an individual's as member or leader
13. Clarity in written and oral communication

- In **one year, project**, first semester evaluation may be based on first six criteria's and remaining may be used for second semester evaluation of performance of students in mini project.
- In case of **half year project** all criteria's in generic may be considered for evaluation of performance of students in mini project.

Guidelines for Assessment of Mini Project Practical/Oral Examination:

- Report should be prepared as per the guidelines issued by the University of Mumbai.
- Mini Project shall be assessed through a presentation and demonstration of working model by the student project group to a panel of Internal and External Examiners preferably from industry or research organisations having experience of more than five years approved by head of Institution.
- Students shall be motivated to publish a paper based on the work in Conferences/students competitions.

Mini Project shall be assessed based on following points;

1. Quality of problem and Clarity
2. Innovativeness in solutions
3. Cost effectiveness and Societal impact
4. Full functioning of working model as per stated requirements
5. Effective use of skill sets
6. Effective use of standard engineering norms
7. Contribution of an individual's as member or leader
8. Clarity in written and oral communication

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical /Oral	Tutorial	Total
CSDLO6011	Enterprise Network Design	04	--		04	--	--	04

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test2	Avg. of two Tests				
CSDLO6011	Enterprise Network Design	20	20	20	80	- -	- -	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To be familiarized with the methodologies and approaches of the network design for an enterprise network.
2	To understand the network hierarchy and use modular approach to network design for an enterprise network.
3	To understand the campus design and data center design considerations for designing an enterprise campus.
4	To study Enterprise Edge WAN Technologies and design a WAN using them.
5	Designing an IP addressing plan and selecting a Route protocol for an enterprise network.
6	To design enterprise network for given user requirements in an application.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand the customer requirements and Apply a Methodology to design a Network.	L1,L2,L3
2	Structure and Modularize the design for an enterprise network.	L6
3	Design Basic Campus and Data Center for an enterprise network.	L6
4	Design Remote Connectivity for an enterprise network.	L6
5	Design IP Addressing and Select suitable Routing Protocols for an enterprise network.	L6
6	Explain SDN and its functioning.	L4,L5

Pre-requisite: Computer Networks

DETAIL SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Pre-requisite	1. OSI Reference Model and TCP/IP Protocol Suite 2. Routing IP Addresses 3. Internetworking Devices	**02**	
I	Applying a Methodology to Network Design:	The Service Oriented Network Architecture, Network Design Methodology, Identifying Customer requirements, Characterizing the Existing Network and Sites, Using the Top- Down Approach to Network Design, The Design Implementation Process. **Self-Learning Topics:** Study the basic concepts of Top-down network design approach with real time application.	**06**	CO1
II	Structuring and Modularizing the Network:	Network Hierarchy, Using a Modular Approach to Network Design, Services Within Modular Networks, Network Management Protocol: SNMP. **Self-Learning Topics:** Study different type of NMP protocols.	**05**	CO2
III	Designing Basic Campus and Data Center Networks	Campus Design Considerations, Enterprise Campus Design, Enterprise Data Center Design Considerations. **Self-Learning Topics:** Real time case study on Enterprise Data Center.	**06**	CO3
IV	Designing Remote Connectivity	Enterprise Edge WAN Technologies, WAN Transport Technologies, WAN Design, Using WAN Technologies, Enterprise Edge WAN and MAN Considerations, Enterprise Branch and Teleworker Design . **Self-Learning Topics:** Case study on WAN design.	**06**	CO4
V	Designing IP Addressing in the Network and Selecting Routing Protocols	Designing an IP Addressing Plan, Introduction to IPv6, Routing Protocol Features, Routing Protocols for the Enterprise, Routing Protocol Deployment, *Route* Redistribution, Route Filtering, Route Summarization **Self-Learning Topics:** Study of different routing protocols for Enterprise design.	**10**	CO5
VI	Software Defined Network	Understanding SDN and Open Flow : SDN Architecture – SDN Building Blocks, OpenFlow messages – Controller to Switch, Symmetric and Asynchronous messages, Implementing OpenFlow Switch,	**04**	CO6

		OpenFlow controllers , POX and NOX. **Self-Learning Topics:** Case study on SDN.		

Text Books:

1. Authorized Self-Study Guide, Designing for Cisco Internetwork Solutions (DESGN), Second Edition, Cisco Press-Diane Teare.
2. Network Analysis, Architecture, and Design 3rd Edition, Morgan Kaufman, James D.
3. CCDA Cisco official Guide
4. Software Defined Networking with Open Flow : PACKT Publishing Siamak Azodolmolky

References Books:

1. Top-Down Network Design (Networking Technology) 3rd Edition, Priscilla Oppenheimer ,Cisco Press Book
2. Network Planning and Design Guide Paperback – 2000,Shaun Hummel

Online References:

1. www.cisco.com
2. https://buildings.honeywell.com

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical/ Oral	Tutorial	Total
CSDLO6012	Blockchain Technology	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDLO6012	Blockchain Technology	20	20	20	80	--	--	--	100

Course Objectives:

Sr.No	Course Objectives
1	To get acquainted with the concept of Distributed ledger system and Blockchain.
2	To learn the concepts of consensus and mining in Blockchain through the Bitcoin network.
3	To understand Ethereum and develop-deploy smart contracts using different tools and frameworks.
4	To understand permissioned Blockchain and explore Hyperledger Fabric.
5	To understand different types of crypto assets.
6	To apply Blockchain for different domains IOT, AI and Cyber Security.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Describe the basic concept of Blockchain and Distributed Ledger Technology.	L1,L2
2	Interpret the knowledge of the Bitcoin network, nodes, keys, wallets and transactions	L1,L2,L3
3	Implement smart contracts in Ethereum using different development frameworks.	L1,L2,L3
4	Develop applications in permissioned Hyperledger Fabric network.	L1,L2,L3
5	Interpret different Crypto assets and Crypto currencies	L1,L2,L3
6	Analyze the use of Blockchain with AI, IoT and Cyber Security using case studies.	L4,

Prerequisite: Cryptography and Distributed Systems

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	**Cryptography and Distributed Systems (prerequisite)**	Hash functions, Public – Private keys, SHA, ECC, Digital signatures, Fundamental concepts of Distributed systems	**02**	—-
I	**Introduction to DLT and Blockchain**	Distributed Ledger Technologies (DLTs) Introduction, Types of Blockchains **Blockchain:** Origin, Phases, Components **Block in a Blockchain**: Structure of a Block, Block Header Hash and Block Height, The Genesis Block, Linking Blocks in the Blockchain, Merkle Tree. **Self-learning Topics:** Blockchain Demo	**04**	CO1
II	**Consensus and Mining**	What is Bitcoin and the history of Bitcoin, Bitcoin Transactions, Bitcoin Concepts: keys, addresses and	**08**	CO2

		wallets, Bitcoin Transactions, validation of transactions, PoW consensus **Bitcoin Network**: Peer-to-Peer Network Architecture, Node Types and Roles, Incentive based Engineering, The Extended Bitcoin Network, Bitcoin Relay Networks, Network Discovery, Full Nodes, Exchanging "Inventory", Simplified Payment Verification (SPV) Nodes, SPV Nodes and Privacy, Transaction Pools, Blockchain Forks **Self-learning Topics:** Study and compare different consensus algorithms like PoA, PoS, pBFT		
III	**Permissionless Blockchain: Ethereum**	Components, Architecture of Ethereum, Miner and mining node, Ethereum virtual machine, Ether, Gas, Transactions, Accounts, Patricia Merkle Tree, Swarm, Whisper and IPFS, Ethash, End to end transaction in Ethereum, **Smart Contracts**: Smart Contract programming using solidity, Metamask (Ethereum Wallet), Setting up development environment, Use cases of Smart Contract, Smart Contracts: Opportunities and Risk. **Smart Contract Deployment**: Introduction to Truffle, Use of Remix and test networks for deployment **Self-learning Topics:** Smart contract development using Java or Python	**10**	CO3
IV	**Permissioned Blockchain : Hyperledger Fabric**	Introduction to Framework, Tools and Architecture of Hyperledger Fabric Blockchain. **Components**: Certificate Authority, Nodes, Chain codes, Channels, Consensus: Solo, Kafka, RAFT Designing Hyperledger Blockchain **Self-learning Topics:** Fundamentals of Hyperledger Composer	**07**	CO4
V	**Crypto assets and Cryptocurrencies**	ERC20 and ERC721 Tokens, comparison between ERC20 & ERC721, ICO, STO, Different Crypto currencies **Self-learning Topics:** Defi, Metaverse, Types of cryptocurrencies	**04**	CO5
VI	**Blockchain Applications & case studies**	Blockchain in IoT, AI , Cyber Security **Self-learning Topics:** Applications of Blockchain in various domains Education, Energy, Healthcare, real-estate, logistics, supply chain	**04**	CO6

Text Books:

1. "Mastering Bitcoin, PROGRAMMING THE OPEN BLOCKCHAIN", 2nd Edition by Andreas M. Antonopoulos, June 2017, Publisher(s): O'Reilly Media, Inc. ISBN: 9781491954386.
2. Mastering Ethereum, Building Smart Contract and Dapps, Andreas M. Antonopoulos Dr. Gavin Wood, O'reilly.
3. Blockchain Technology, Chandramouli Subramanian, Asha A George, Abhillash K. A and Meena Karthikeyen, Universities press.
4. Hyperledger Fabric In-Depth: Learn, Build and Deploy Blockchain Applications Using Hyperledger Fabric, Ashwani Kumar, BPB publications
5. Solidity Programming Essentials: A beginner's Guide to Build Smart Contracts for Ethereum and Blockchain, Ritesh Modi, Packt publication
6. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond, Chris Burniske & Jack Tatar.

Reference:

1. Mastering Blockchain, Imran Bashir, Packt Publishing 2. Mastering Bitcoin Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos, O'Reilly Media
2. Blockchain Technology: Concepts and Applications, Kumar Saurabh and Ashutosh Saxena, Wiley.
3. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them, Antony Lewis.for Ethereum and Blockchain, Ritesh Modi, Packt publication.
4. Mastering Bitcoin Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos, O'Reilly Media

Online References:

1. NPTEL courses:
    a. Blockchain and its Applications,
    b. Blockchain Architecture Design and Use Cases
2. www.swayam.gov.in/
3. www.coursera.org
4. https://ethereum.org/en/
5. https://www.trufflesuite.com/tutorials
6. https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.h
7. Blockchain demo: https://andersbrownworth.com/blockchain/
8. Blockchain Demo: Public / Private Keys & Signing: https://andersbrownworth.com/blockchain/public-private-keys/

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

- **Question paper format**

    - Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**

    - **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

    - A total of **four questions** need to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical/ Oral	Tutorial	Total
CSDLO6013	Virtualization and Cloud Security	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
CSDLO6013	Virtualization and Cloud Security	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand Virtualization
2	To learn various tools used for Virtualization
3	To understand various steps involved in the Virtualization
4	To learn about different trends in cloud computing
5	To learn about Data Security in Cloud
6	To learn about Identity and Access Management in Cloud

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Define the concept of Virtualization and explore different tools in Virtualization	L1,L2,L3
2	Examine different types for Virtualization	L1,L2
3	Understand the need for Cloud Security	L1,L2
4	Implement various Data security techniques in cloud security	L1,L2,L3
5	Implement various Access Management techniques in cloud security	L1,L2,L3
6	Understand different trends in cloud computing	L1,L2

Prerequisite: Computer Networks, Cryptography and System Security

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Computer Networks, cryptography and system security	**02**	
I	Introduction to Cloud Computing	Definition, Characteristics, Components, Cloud Deployment Models, NIST Architecture of Cloud Computing, Advantages of Cloud Computing, Cloud	**04**	CO1

		Computing Challenges. Identification of frames in cloud. Public, Private, Hybrid, **Self-Learning Topics:** Case study on different types of cloud ie private, public etc.		
II	Introduction to Virtualization	Introduction, Characteristics of Virtualization, Full Virtualization, Para virtualization, Hardware-Assisted Virtualization, Operating System Virtualization, Application Server Virtualization, Application Virtualization, Network Virtualization, Storage Virtualization, Service Virtualization Computing Platforms: Amazon Web Services (AWS) EC2 ,S3, Google App Engine, Microsoft Azure etc. **Self-Learning Topics:** Study different AWS services.	**06**	CO1
III	Virtualization	Hypervisors: Hosted Structure (Type II Hypervisor) Bare-metal Structure (Type I Hypervisor) Implementation Levels of Virtualization Resource Virtualization CPU Virtualization, Memory Virtualization, Device and I/O Virtualization Technology Examples KVM Architecture, Xen Architecture, VMWare, Hyper-V **Self-Learning Topics:** Case study on virtualization	**08**	CO2
IV	Cloud Security	Risks in Cloud Computing: Introduction, Risk Management, Cloud Impact, Enterprise-Wide, Risk Management, Risks internal and external in Cloud Computing Cloud Security Services: Security Authorization Challenges in the Cloud, Secure Cloud Software Requirements, Content level security. Cloud Hosting risks, **Self-Learning Topics:** Case study on Cloud Secuirty.	**06**	CO3
V	Data Security in Cloud	Introduction, Current state, Data Security. Application Security in Cloud, Security in IaaS Environment, Security in PaaS Environment, Security in SaaS Environment, Cloud Service Reports by CPS, Security for Virtualization Software,	**07**	CO4 CO5

		Host Security in PasS, SaaS and IaaS, Security as a Service, Benefits of SaaS, Challenges with SaaS, Identity Management as a Service (Id MaaS). Security related to storage. **Self-Learning Topics:** Study various benefits of Maas, SaaS, PaaS and Iaas		
VI	Future Cloud Computing	Mobile Cloud Computing Autonomic Cloud Computing Multimedia Cloud Energy aware Cloud computing Jungle Computing. Case study on upcoming cloud computing area **Self-Learning Topics:** Case study on future in cloud computing.	**06**	CO6

Text Books:

1) Cloud Computing and Services ,Arup Vithal | Bhushan Jadhav, StarEdu Solutions, SYBGEN Learning India Pvt. Ltd
2) Cloud Computing: A Practical Approach for Learning and Implementation, A. Srinivasan, J. ,Suresh, Pearson.
3) Cloud Computing and Virtualization , Dac-Nhuong Le,Raghvendra Kumar, Wiley & Sons
4) Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz
Russell Dean Vines , Wiley & Sons.

Reference Books:

1. Cloud Computing Black Book , Kailash Jayaswal , Dreamtech Publication.
2. MASTERING CLOUD COMPUTING**, "BUYYA"** Tata Mcgraw Hill publication
3. CLOUD COMPUTING A PRACTICAL APPROACH, "VELTE", Tata Mcgraw Hill publication

Online References:

1. https://docs.aws.amazon.com/
2. https://docs.microsoft.com/en-us/azure
3. https://docs.docker.com/get-started/

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

- **Question paper format**

  - Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**

  - **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

  - A total of **four questions** need to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical/ Oral	Tutorial	Total
CSDLO6014	Cyber Security and Ransom ware incident response system	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
CSDLO6014	Cyber Security and Ransom ware incident response system	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand the concept of incident response in cyber security.
2	Understand the concept of cyber risk and detection of events.
3	Understand the monitoring system for incident response.
4	To Understand modern human-operated cyber attacks
5	To understand the concept of focusing on threat actor tactics, techniques, and procedures.
6	To Collect and analyze ransomware-related cyber threat intelligence from various sources.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand and apply the concepts of incident response in cyber security.	L1,L2,L3
2	Understand the concept of cyber risk and detection of events.	L1,L2,L3
3	Understand the monitoring system for incident response.	L1,L2
4	Understand modern human-operated cyber-attacks.	L1,L2
5	Apply the concept of focusing on threat actor tactics, techniques, and procedures.	L1,L2,L3
6	Collect and analyze ransomware-related cyber threat intelligence from various sources.	L1,L2,L3,L4

Prerequisite: Computer Networks, Cryptography and System Security

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping

0	Prerequisite	Computer Networks, cryptography and system security	**02**	
I	Introduction to incident response Strategy	Introduction, significance of incident response: Why Does This Happen? Strategy vs. Tactics, Changing the Culture. Necessary perquisites: Establishing the Identify and Protect Functions, Defined Cyber security Program, How Does Each Program Support Incident Response? Incidents response frameworks: NIST 800-61, Organizing a Computer Incident Response Capability, Handling an Incident, NIST CSF Implementations, Detection, Respond, Recover. Implementation. Purpose, Scope, Definitions, Responds to incidents. **Self-Learning Topics:** Study the high-level activities found in incident response.	**06**	CO1
II	Cyber Risk and Detection of Events	Cyber risk, The Mandiant Cyber Attack Life Cycle, Tie the Risk Assessment and Kill Chain, Building Detective Capabilities, Identification of Security Events, Containment, Containment strategy, Removing attacker's artifacts, Vulnerabilities scanning. **Self-Learning Topics:** Study the different Vulnerabilities used for scanning.	**06**	CO1
III	Continuous Monitoring of Incident Response Program	Components of Continuous Monitoring, How Continuous Monitoring works, Incorporating Continuous Monitoring into the NIST CSF Environment. **Self-Learning Topics:** Case study on incident response system.	**05**	CO2
IV	Cyber Threat Intelligence and Ransomware attack	Overview and history of ransomware attack. Life Cycle of a Human-Operated Ransomware Attack. Incident response process. Strategic Cyber Threat Intelligence, Operational Cyber Threat Intelligence, Tactical Cyber Threat Intelligence. **Self-learning Topics:** Study the different human operated ransomware attack.	**08**	CO3
V	Understanding Ransomware Affiliates Tactics, Techniques and Procedures	Gaining initial access, Executing malicious code, Obtaining persistent access, Escalating privileges, Collecting and exfiltrating data, Ransomware deployment. **Self-learning Topics:** Case Study on Ransomware deployment.	**06**	CO4 CO5

VI	Collecting Ransomware Related Cyber Threat Intelligence	Threat Research Reports, Community, Threat actors **Self-learning Topics:** Practical case study on Ransomware incident response system.	**06**	CO6

Text & Reference Books:

1. 1. Cyber Security Incident Response How to contain Eradicate and Recover of incidents, Eric C. Thompson, Apress 2018.
2. Incident Response Techniques for Ransomware Attacks, by Oleg Skulkin, 2022, pack publisher.
3. Cybersecurity Incident & Vulnerability Response Playbooks, 2021
4. Computer Security incident handling guide.

Online References:

1. www.udemy,com
2. www.nptel.ac.in

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marksQ.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
CSM601	Mini Project Lab: 2B Application Security	--	04	--	--	02	--	02

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Pract. /Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg.				
CSM601	Mini Project Lab: 2B Application Security	--	--	--	--	25	25	50

Course Objectives

1. To acquaint with the process of identifying the needs and converting it into the problem.
2. To familiarize the process of solving the problem in a group.
3. To acquaint with the process of applying basic engineering fundamentals to attempt solutions to the problems.
4. To inculcate the process of self-learning and research.

Course Outcome: Learner will be able to…

1. Identify problems based on societal /research needs.
2. Apply Knowledge and skill to solve societal problems in a group.
3. Develop interpersonal skills to work as member of a group or leader.
4. Draw the proper inferences from available results through theoretical/ experimental/simulations.
5. Analyse the impact of solutions in societal and environmental context for sustainable development.
6. Use standard norms of engineering practices
7. Excel in written and oral communication.
8. Demonstrate capabilities of self-learning in a group, which leads to life long learning.
9. Demonstrate project management principles during project work.

Guidelines for Mini Project

- Students shall form a group of 3 to 4 students, while forming a group shall not be allowed less than three or more than four students, as it is a group activity.
- Students should do survey and identify needs, which shall be converted into problem statement for mini project in consultation with faculty supervisor/head of department/internal committee of faculties.
- Students hall submit implementation plan in the form of Gantt/PERT/CPM chart, which will cover weekly activity of mini project.
- A log book to be prepared by each group, wherein group can record weekly work progress, guide/supervisor can verify and record notes/comments.
- Faculty supervisor may give inputs to students during mini project activity;however, focus shall be on self-learning.
- Students in a group shall understand problem effectively, propose multiple solution and select best possible solution in consultation with guide/ supervisor.

- Students shall convert the best solution into working model using various components of their domain areas and demonstrate.
- The solution to be validated with proper justification and report to be compiled in standard format of University of Mumbai.
- With the focus on the self-learning, innovation, addressing societal problems and entrepreneurship quality development within the students through the Mini Projects, it is preferable that a single project of appropriate level and quality to be carried out in two semesters by all the groups of the students. i.e. Mini Project 1 in semester III and IV. Similarly, Mini Project 2 in semesters V and VI.
- However, based on the individual students or group capability, with the mentor's recommendations, if the proposed Mini Project adhering to the qualitative aspects mentioned above gets completed in odd semester, then that group can be allowed to work on the extension of the Mini Project with suitable improvements/modifications or a completely new project idea in even semester. This policy can be adopted on case by case basis.

Guidelines for Assessment of Mini Project:

Term Work

- The review/ progress monitoring committee shall be constituted by head of departments of each institute. The progress of mini project to be evaluated on continuous basis, minimum two reviews in each semester.
- In continuous assessment focus shall also be on each individual student, assessment based on individual's contribution in group activity, their understanding and response to questions.
- Distribution of Term work marks for both semesters shall be as below;
    - Marks awarded by guide/supervisor based on log book : 10
    - Marks awarded by review committee : 10
    - Quality of Project report : 05

Review/progress monitoring committee may consider following points for assessment based on either one year or half year project as mentioned in general guidelines.

One-year project:

- In first semester entire theoretical solution shall be ready, including components/system selection and cost analysis. Two reviews will be conducted based on presentation given by students group.
    - First shall be for finalisation of problem
    - Second shall be on finalisation of proposed solution of problem.
- In second semester expected work shall be procurement of component's/systems, building of working prototype, testing and validation of results based on work completed in an earlier semester.
    - First review is based on readiness of building working prototype to be conducted.
    - Second review shall be based on poster presentation cum demonstration of working model in last month of the said semester.

Half-year project:

- In this case in one semester students' group shall complete project in all aspects including,
    - Identification of need/problem
    - Proposed final solution
    - Procurement of components/systems
    - Building prototype and testing
- Two reviews will be conducted for continuous assessment,
    - First shall be for finalisation of problem and proposed solution
    - Second shall be for implementation and testing of solution.

Assessment criteria of Mini Project.

Mini Project shall be assessed based on following criteria;

1. Quality of survey/ need identification
2. Clarity of Problem definition based on need.

3. Innovativeness in solutions
4. Feasibility of proposed problem solutions and selection of best solution
5. Cost effectiveness
6. Societal impact
7. Innovativeness
8. Cost effectiveness and Societal impact
9. Full functioning of working model as per stated requirements
10. Effective use of skill sets
11. Effective use of standard engineering norms
12. Contribution of an individual's as member or leader
13. Clarity in written and oral communication

- In **one year, project**, first semester evaluation may be based on first six criteria's and remaining may be used for second semester evaluation of performance of students in mini project.
- In case of **half year project** all criteria's in generic may be considered for evaluation of performance of students in mini project.

Guidelines for Assessment of Mini Project Practical/Oral Examination:

- Report should be prepared as per the guidelines issued by the University of Mumbai.
- Mini Project shall be assessed through a presentation and demonstration of working model by the student project group to a panel of Internal and External Examiners preferably from industry or research organisations having experience of more than five years approved by head of Institution.
- Students shall be motivated to publish a paper based on the work in Conferences/students competitions.

Mini Project shall be assessed based on following points;

1. Quality of problem and Clarity
2. Innovativeness in solutions
3. Cost effectiveness and Societal impact
4. Full functioning of working model as per stated requirements
5. Effective use of skill sets
6. Effective use of standard engineering norms
7. Contribution of an individual's as member or leader
8. Clarity in written and oral communication