AC:

Item No:

UNIVERSITY OF MUMBAI

Bachelor of Engineering

in

Computer Science and Engineering (Internet of Thing and Cyber Security including Blockchain)

~~Second Year with Effect from AY 2021-22~~

~~Third Year with Effect from AY 2022-23~~

~~Final Year with Effect from AY 2023-24~~

(REV- 2019 ‘C’ Scheme) from Academic Year 2020 – 21

Under

FACULTY OF SCIENCE & TECHNOLOGY

(As per AICTE guidelines with effect from the academic year 2019–2020)

AC:

Item No:

UNIVERSITY OF MUMBAI

Sr. No.	Heading	Particulars
1	Title of the Course	**Third Year Engineering Computer Science and Engineering (Internet of Thing and Cyber Security including Blockchain)**
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	**8 semesters**
6	Level	~~P.G.~~ / **U.G.**/ ~~Diploma / Certificate~~ (Strike out which is not applicable)
7	Pattern	~~Yearly~~ / **Semester** (Strike out which is not applicable)
8	Status	~~New~~ / Revised (Strike out which is not applicable)
9	To be implemented from Academic Year	**With effect from Academic Year: 2022-2023**

Dr. S. K. Ukarande	Dr Anuradha Muzumdar
Associate Dean	Dean
Faculty of Science and Technology	Faculty of Science and Technology
University of Mumbai	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 Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain) (effective from the year 2021-22). AICTE has introduced Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain) as one of the nine emerging technology and hence many colleges affiliated with the University of Mumbai has started four years UG program for Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain). 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 Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain)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 Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain) 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 Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain) 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 Internet of Thing domain. The syllabus is peer-reviewed by experts from reputed industries and as per their suggestions, it covers future emerging trends in Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain) technology and research opportunities available due to these trends. .

We would like to thank senior faculties of IT, Computer and Electronics 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 Computer Science and Engineering in the (Internet of Thing and Cyber Security including Blockchain).

Program Specific Outcome for graduate Program in Computer Science and Engineering (Internet of Thing and Cyber Security including Blockchain)

1. Apply Core of IoT, Cyber Security & Blockchain knowledge to develop stable and secure Application.
2. Identify the issues of IoT, Cyber Security including Blockchain in real time application and in all three area of domain.
3. Ability to apply and develop IoT & Cyber Security including Blockchain multidisciplinary projects.

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

Curriculum Equivalence

TE-Internet of Thing, TE-Cyber Security and TE-Computer Science and Engineering (Internet of Thing and Cyber Security including Blockchain) Sem-V all subjects are equivalent to TE-Computer Engineering Sem-V subjects.

Sr. No.	Sem	Name of Subject	Equivalence Subject	Equivalence Subject Code	Branch
1	VI	Cryptography and Network Security	Cryptography and Network Security	CSC601 IoTCSBCC601	TE-Cyber Security, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
2	VI	Application Security and Secure Coding Principles	Application Security and Secure Coding Principles	CSC602 IoTCSBCDLO6012	TE-Cyber Security, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
3	VI	Ethical Hacking & Digital Forensic	Ethical Hacking & Digital Forensic	CSC603 IoTCSBCDLO6013	TE-Cyber Security, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
4	VI	Web X.0	Web X.0	IoTC604 CSC604 IoTCSBCC604	TE-Internet of Thing, TE-Cyber Security, TE- Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
5	VI	CNS Lab	CNS Lab	CSL601 IoTCSBCL601	TE-Cyber Security, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
6	VI	IoT Architecture and Protocols	IoT Architecture and Protocols	IoTC601 IoTCSBCC602	TE-Internet of Thing, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
7	VI	IoT Architecture and Protocols Lab	IoT Architecture and Protocols Lab	IoTL601 IoTCSBCL602	TE-Internet of Thing, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
8	VI	Web Lab	Web Lab	IoTL604 CSL604 IoTCSBCL604	TE-Internet of Thing, TE-Cyber Security, TE- Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)

9	VI	Enterprise Network Design	Enterprise Network Design	IoTDLO6011 CSDLO6011 IoTCSBCDLO6011	TE-Internet of Thing, TE-Cyber Security, TE- Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
10	VI	Blockchain Technology	Blockchain Technology	IoTDLO6012 CSDLO6012 IoTCSBCC603	TE-Internet of Thing, TE-Cyber Security, TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)
11	VI	Virtualization and cloud security	Virtualization and cloud security	CSDLO6013 IoTCSBCDLO6014	TE-Cyber Security , TE-Computer Science and Engineering(nternet of Thing and Cyber Security including Blockchain)

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 Computer Science and Engineering (Internet of Thing and Cyber Security including Blockchain)

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
IoTCSBCC601	Cryptography and Network Security	3	--	3	--	3
IoTCSBCC602	IoT Architecture and Protocols	3	--	3		3
IoTCSBCC603	Blockchain Technology	3	--	3	--	3
IoTCSBCC604	Web X.0	3	--	3	--	3
IoTCSBCDLO601x	**Department Level Optional Course -2**	3	--	3	--	3
IoTCSBCL601	CNS Lab	--	2	--	1	1
IoTCSBCL602	IoT Architecture and Protocols Lab	--	2	--	1	1
IoTCSBCL603	Blockchain Technologies Lab	--	2	--	1	1
IoTCSBCL604	Web Lab	--	2	--	1	1
IoTCSBCL605	Mobile Application Security and Penetration Testing Lab (SBL)	--	4	--	2	2
IoTCSBCM601	Mini Project Lab: 2B Blockchain Security Model.	--	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					
IoTCSBCC601	Cryptography and Network Security	20	20	20	80	3	--	--	100
IoTCSBCC602	IoT Architecture and Protocols	20	20	20	80	3	--	--	100
IoTCSBCC603	Blockchain Technology	20	20	20	80	3	--	--	100
IoTCSBCC604	Web X.0	20	20	20	80	3	--	--	100
IoTCSBCDLO601x	**Department Level Optional Course -2**	20	20	20	80	3	--	--	100
IoTCSBCL601	CNS Lab	--	--	--	--	--	25	25	50
IoTCSBCL602	IoT Architecture and Protocols Lab	--	--	--	--	--	25	--	25
IoTCSBCL603	Blockchain Technologies Lab	--	--	--	--	--	25	-	25

IoTCSBCL604	Web Lab						25	25	50
IoTCSBCL605	Mobile Application Security and Penetration Testing Lab (SBL)	--	--	--	--	--	50	25	75
IoTCSBCM601	Mini Project Lab: 2B Blockchain Security Model.	--	--	--	--	--	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.

IoTCSBCDLO601X	**Department Optional Course – 2**
IoTCSBCDLO6011	Enterprise Network Design
IoTCSBCDLO6012	Application Security and Secure Coding Principles
IoTCSBCDLO6013	Ethical Hacking and Digital Forensic
IoTCSBCDLO6014	Virtualization and cloud security

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned		
		Theory	Practical	Theory	Practical	Total
IoTCSBCC601	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.					
IoTCSBCC601	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	L1

	methods	
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 **Self-Learning Topic**: Explore any opensource network management security tool	**6**	CO5
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**
IoTCSBCC602	IoT Architecture and Protocols	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**					
IoTCSBCC 602	IoT Architecture and Protocols	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	**Course Objectives**
The course aims:	
1	To understand IoT Characteristics and Conceptual Framework.
2	To comprehend network architecture and design of IoT

3	To understand smart objects in IoT.
4	To correlate the connection of smart objects and IoT access technologies.
5	To explore network layer and application layer protocols for IoT.
6	To explore IoT security aspect.

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 IoT Characteristics and Conceptual Framework.	L1,L2
2	Differentiate between the levels of the IoT architectures.	L1,L2
3	Interpret sensor network and its components.	L1,L2
4	Analyze the IoT access technologies.	L1,L2,L3,L4
5	Illustrate various protocols at network layer and application layer for IoT.	L1,L2,L3
6	Analyze and evaluate security issues in IoT and risk analysis structure.	L1,L2,L3,L4

Prerequisite:

1. Python programming
2. C programing language
3. Computer Networks

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	ports, Timers ,Programming of controller , How to use IDE to write code of microcontroller, TCP-IP protocol stack	**02**	
I	Introduction to IoT	1.1 Introduction to IoT- Defining IoT, Characteristics of IoT, Conceptual Framework of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT, Communication models & APIs, Basics of networking Communication protocol, wireless sensor networks. 1.2 Convergence of IT and OT , IoT Challenges, IoT protocol vs Web Protocol stack **Self-learning Topics:** Hardware and software development tools for - *A*rduino, NodeMCU, ESP32, Raspberry Pi pico	**04**	CO1
II	IoT Network Architecture and Design	**2.1 Drivers Behind New Network Architectures** : Scale,Security,Constrained Devices and Networks ,Data,Legacy Device Support **2.2 Architecture :** The IoT World Forum (IoTWF) Standardized Architecture :Layer 1-7, IT and OT Responsibilities in the IoT Reference Model,Additional IoT Reference Models, A Simplified IoT Architecture, The Core IoT Functional Stack ::Layer 1-3 , Analytics Versus Control Applications , Data Versus Network Analytics Data Analytics Versus Business Benefits , Smart Services, **2.3 IoT Data Management and Compute Stack** :Fog Computing , Edge Computing ,The Hierarchy of Edge, Fog, and Cloud	**06**	CO2

III	Smart Objects IoT	**3.1 Sensors, Actuators, and Smart Objects , Sensors , Actuators,** **3.2 Micro-Electro-Mechanical Systems (MEMS)** Smart Objects: A Definition , Trends in Smart Objects, **3.3 Sensor Networks** , Wireless Sensor Networks (WSNs) , Communication Protocols for WSN,RFID ,NFC **Self-learning Topics:** RFID in Libraries	**04**	CO3
IV	Connecting Smart Objects	**4.1 Communications Criteria** : Range , Frequency Bands , Power Consumption , Topology , Constrained Devices , Constrained-Node Networks , Data Rate and Throughput , Latency and Determinism , Overhead and Payload , **4.2 IoT Access Technologies** : Standardization and Alliances , Physical Layer , MAC Layer , Topology ,Security and Conclusion of IEEE 802.15.4 , IEEE 802.15.4g and 802.15.4e ,IEEE 1901.2a ,IEEE 802.11ah , LoRaWAN, and NB-IoT and Other LTE Variations , LTE Cat 0 , LTE-M, NB-IoT **Self-learning Topics:** case studies	**08**	CO4
V	IoT Network Layer and Application protocols	5.1 The Business Case for IP , The Key Advantages of Internet Protocol ,Adoption or Adaptation of the Internet Protocol ,The Need for Optimization ,Constrained Nodes , Constrained Networks IP Versions , Optimizing IP for IoT , 5.2 From 6LoWPAN to 6Lo, Header Compression, Fragmentation , Mesh Addressing ,Mesh-Under Versus Mesh-Over Routing , 6Lo Working Group , 6TiSCH , RPL , Objective Function Rank, RPL Headers ,Metrics , Authentication and Encryption on Constrained Nodes , ACE , DICE, Profiles and Compliances, Internet Protocol for Smart Objects Alliance ,Wi-SUN Alliance, Thread, IPv6 Ready Logo 5.3 The Transport Layer , IoT Application Transport Methods,Generic Web-Based Protocols , 5.4 IoT Application Layer Protocols , CoAP, MQTT, AMQP **Self-learning Topics:** case studies	**08**	CO5
VI	Securing IoT	6.1 **A Brief History of OT Security** Common Challenges in OT Security : Erosion of Network Architecture,Pervasive Legacy Systems,Insecure Operational Protocols like Modbus, DNP3 ,ICCP ,OPC , (IEC) Protocols,Device Insecurity **6.2 Security Knowledge:** IT and OT Security Practices and Systems Vary, The Purdue Model for Control Hierarchy, OT Network Characteristics Impacting Security, Security Priorities: CIA, Security Focus 6.3 **Formal Risk Analysis Structures**: OCTAVE and FAIR, FAIRThe Phased Application of Security in an Operational Environment , Secured Network Infrastructure and Assets, Deploying Dedicated Security Appliances, Higher-Order Policy Convergence and Network Monitoring **Self-learning Topics:** OWASP IoT Top 10 attacks ,X.509, SSL & TSL basics	**06**	CO6

Text Books:

1. Arsheep Bahga (Author), Vijay Madisetti, Internet Of Things: A Hands-On Approach Paperback, Universities Press, Reprint 2020
2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, IoT Fundamentals Networking Technologies, Protocols, and Use Cases for the Internet of Things CISCO.

References:

1. Pethuru Raj, Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases by , CRC Press.
2. Raj Kamal, Internet of Things, Architecture and Design Principles, McGraw Hill Education, Reprint 2018.
3. Perry Lea, Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security, Packt Publications, Reprint 2018.
4. Amita Kapoor, "Hands on Artificial intelligence for IoT", 1st Edition, Packt Publishing, 2019.
5. Sheng-Lung Peng, Souvik Pal, Lianfen Huang Editors: Principles of Internet of Things (IoT)Ecosystem:Insight Paradigm, Springer

Online References:

1. https://owasp.org/www-project-internet-of-things/
2. NPTEL: Sudip Misra, IIT Khargpur, Introduction to IoT: Part-1, https://nptel.ac.in/courses/106/105/106105166/
3. NPTEL: Prof. Prabhakar, IISc Bangalore, Design for Internet of Things, https://onlinecourses.nptel.ac.in/noc21_ee85/preview

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
IoTCSBCDLO 603	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					
IoTCSBCDLO6 03	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 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	**08**	CO2
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	**10**	CO3

		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		
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
IoTCSBCC604	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					
IoTCSBCC604	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, 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	**04**	CO1

		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 to Node.js, Connecting to MongoDB from Node.js, Accessing and Manipulating Databases, Manipulating	**07**	CO6

		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
IoTCSBCL601	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.					
IoTCSBCL601	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	L1,L2,L3

	attacks	
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**
IoTCSBCL602	IoT Architecture and Protocols 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**				
IoTCSBCL 602	IoT Architecture and Protocols Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	**Lab Objectives**
The Lab aims:	
1	To Understand the definition and significance of the Internet of Things.
2	To Discuss the architecture, operation, and business benefits of an IoT solution.
3	To Examine the potential business opportunities that IoT can uncover.
4	To Explore the relationship between IoT, cloud computing, and Data Analytics.
5	To Identify how IoT differs from traditional data collection systems.
6	To Explore the interconnection and integration of the physical world and be able to design & develop IOT applications.

Lab Outcomes:

Sr. No.	**Lab Outcomes**	**Cognitive levels of attainment as per Bloom's Taxonomy**
On successful completion, of course, learner/student will be able to:		
1	Adapt different techniques for data acquisition using various IoT sensors	L1,L2,L3

	for different applications.	
2	Demonstrate the working of actuators based on the collected data.	L1,L2,L3
3	Use different IoT simulators and correlate working of IoT protocols.	L1,L2,L3
4	Adapt different techniques for Integrating IoT services to other third-party Clouds.	L1,L2,L3
5	Execute data analysis and encryption methodologies for deployment of IoT applications.	L1,L2,L3,L4
6	Implement IoT protocols for communication to realize the revolution of internet in mobile devices, cloud and sensor networks.	L1,L2,L3,L4

Prerequisite:

1. Python programming
2. C programing language
3. Computer Networks

Hardware & Software Requirements:

Hardware Requirement:	Software requirement:
PC i3 processor and above. Arduino using Wifi/Raspberry Pi	Contiki, Cooja or any other simulator. AWS/Azure services. Internet Connection

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	Prerequisite	Experimentation with Microprocessor and Microcontroller , Experimentation with python and c	**02**	
I	Arduino	Introduction to Arduino, Hardware requirements, Software requirements, Arduino Programming Language, Arduino Uno Wired & Wireless connectivity, LCD commands, Serial Communication commands. Program for blinking LED using Arduino. Traffic Light pattern using Arduino. ESP8266 WiFi Module	**05**	LO1, LO2
II	Raspberry Pi	Introduction to Raspberry Pi, Installation of NOOBS and Raspbian on SD card, Libraries on Raspberry Pi, getting static IP address of Raspberry Pi, Interfacing of Relay, DHT11, DC Motor and LCD with Raspberry Pi.	**05**	LO1,LO2
III	Contiki OS	Contiki OS : History of Contiki OS,Applications, Features, ,Communication Components in Contiki OS, Cooja simulator ,Running Cooja Simulator,	**05**	LO3
IV	Cooja Simulator	Using the Contiki OS with the Cooja simulator to program the IoT for broadcasting data from sensors	**03**	LO5,LO6
V	Protocols and Security with Cooja	Understanding of 6LowPAN , COAP and protocol implementation in Cooja . Encryption Decryption techniques for IoT	**03**	LO5,LO6
VI	IoT data to Cloud	Installing the Remote desktop server. Installation of Pi camera, Face recognition, serial peripheral interface using Raspberry Pi. . DHT11 data logger with ThingSpeak/ thingsboard/ AWS/ Azure server .	**03**	LO4,L06

Text & Reference Books:

1. Jake VanderPlas,“ Python Data Science Handbook”, O’Reilly publication
2. Joakim Verona,” Practical DevOps”, PACKT publishing
3. Honbo Zhou,” The internet of things in the cloud”, CRC press, Taylor and Francis group
4. Perry Lea,” Internet of things for architects”, PACKT publishing

Online References:

1. https://spoken-tutorial.org/watch/Arduino/Introduction+to+Arduino/English/
2. https://pythonprogramming.net/introduction-raspberry-pi-tutorials/
3. https://iotbytes.wordpress.com/basic-iot-actuators/
4. http://www.contiki-os.org/
5. https://www.bevywise.com/iot-simulator/
6. https://mqtt.org/

List of Experiments.

1. To study and implement interfacing of different IoT sensors with Raspberry Pi pico/Arduino/ModeMCU.

2. To study and implement interfacing of actuators based on the data collected using IoT sensors. (like led switch ON/OFF, stepper motor)

3. To study and demonstrate Contiki OS for RPL (like Create 2 border router and 10 REST clients, Access border router from other network (Simulator))

4. To study and demonstrate working of 6LoWPAN in Contiki OS (simulator)

5. Write a program on Raspberry Pi to push and retrieve the data from cloud like thingspeak/thingsboard/AWS/ Azure etc

6. To study and implement IoT Data processing using Pandas.

7. Write a program on Arduino / Raspberry Pi subscribe to MQTT broker for temperature data and print it

8. Write a program to create TCP Server on Arduino/Raspberry Pi and respond with humidity data to TCP client when Requested

9. Write a program for ESP8266 DHT11/DHT22 Temperature and Humidity Web Server with Arduino IDE

10. Write a program to Control Your ESP8266 From Anywhere in the World

11. Write a program for Arduino / Raspberry Pi Publishing MQTT Messages to ESP8266

12 Write a program to collect data from sensor encrypt data send it to receiver (server) and decrypt is at receiving end Ardino/Raspberry Pi/ Contiki OS (simulator)

Term Work: Term Work shall consist of at least 10 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**
IoTCSBCL603	Blockchain Technologies 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**				
IoTCSBCL603	Blockchain Technologies Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr.No	**Lab Objectives**
The Lab aims:	
1	To develop and deploy smart contracts on local Blockchain.
2	To deploy the smart contract on test networks.
3	To develop and test smart contract using Remix IDE and Metamask.
4	To construct a permissioned Hyperledger fabric network.
5	To design and develop crypto currency.
6	To develop and test a DApp using Ethereum/Hyperledger

Lab Outcomes:

Sr.No	Lab Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Develop and test smart contract on local Blockchain.	L3,L4
2	Develop and test smart contract on Ethereum test networks.	L3,L4
3	Write and deploy smart contract using Remix IDE and Metamask.	L4
4	Write and deploy chain code in Hyperledger Fabric.	L4
5	Design and develop Cryptocurrency.	L4
6	Develop a Full-fledged DApp using Ethereum/Hyperledger.	L5

Prerequisite: Java, python, Javascript

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	Prerequisite	Java, Python, JavaScript	**02**	—
I	Local Blockchain and smart contracts	Introduction to Truffle, establishing local Blockchain using Truffle, Solidity programming language, chain code(Java/JavaScript/Go), deployment on Truffle local Blockchain Mini Project: Allocation of the groups	**03**	LO1
II	Deployment and publishing smart contracts on Ethereum test network	Ethereum Test networks (Ropsten/Gorelli/Rinkeby),deployment on test networks, Web3.js/Web3.py for interaction with Ethereum smart contract Mini Project: Topic validation and finalizing software requirements	**03**	LO2
III	Remix IDE and Metamask	Smart contract development and deployment using Metamask and Remix Mini Project: Study the required programming language for smart contract/chain code	**04**	LO3
IV	Chain code deployment in Hyperledger Fabric	Chain code deployment in Hyperledger fabric Mini project: Study required front end tools	**04**	LO4
V	Crypto currency Design	Design and develop Crypto currency Mini Project: Study Integration of front end with smart contract/chain code	**04**	LO5
VI	Mini-project on Design and Development of a DApps using Ethereum/Hyperledger Fabric	Implementation of Mini Project 1. Design, configure and testing of mini project Report submission as per guidelines	**06**	LO6

Mini project

1. Students should carry out mini-project in a group of three/four students with a subject In-charge

2. The group should meet with the concerned faculty during laboratory hours and the progress of work discussed must be documented.
3. Each group should perform a detailed literature survey and formulate a problem statement.
4. Each group will identify the hardware and software requirement for their defined mini project problem statement.
5. Design, develop and test their smart contract/chain code.
6. Each group may present their work in various project competitions and paper presentations

Documentation of the Mini Project

The Mini Project Report can be made on following lines:

1. Abstract
2. Contents
3. List of figures and tables
4. Chapter-1 (Introduction, Literature survey, Problem definition, Objectives, Proposed Solution, Technology/platform used)
5. Chapter-2 (System design/Block diagram, Flow chart, Software requirements, cost estimation)
6. Chapter-3 (Implementation snapshots/figures with explanation, code, future directions)
7. Chapter-4 (Conclusion)
8. References

Text Books:

1. Ethereum Smart Contract Development, Mayukh Mukhopadhyay, Packt publication.
2. Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum and Blockchain, Ritesh Modi, Packt publication.
3. Hands-on Smart Contract Development with Hyperledger Fabric V2, Matt Zand, Xun Wu and Mark Anthony Morris, O’Reilly.

References:

1. Mastering Blockchain, Imran Bashir, Packt Publishing
2. Introducing Ethereum and Solidity, Chris Dannen, APress.
3. Hands-on Blockchain with Hyperledger, Nitin Gaur, Packt Publishing.

Online References:

1. https://trufflesuite.com/
2. https://metamask.io/
3. https://remix.ethereum.org/
4. https://www.hyperledger.org/use/fabric

Term-Work: Term-Work shall consist of 5 experiments and Mini-Project on above guidelines/syllabus. Also Term-work must include at least 2 assignments and Mini-Project report.

Term Work Marks: 25 Marks (Total marks) =15 Marks (5 Experiments + Mini Project) + 5 Marks (Assignments) +

5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the Mini Project and Presentatio**n.**

		Teaching Scheme (Contact Hours)			Credits Assigned			
Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical & Oral	Tutorial	Total
IoTCSBCL604	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				
IoTCSBCL604	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, add HTML validators, using $valid property of Angular, etc.) 3.Create an application for like Students Record using AngularJS.	**04**	LO5
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

Course Code	**Course Name**	**Teaching Scheme (Contact Hours)**			**Credits assigned**			
		Theory	**Practical**	**Tutorial**	**Theory**	**Practical/ Oral**	**Tutorial**	**Total**

IoTCSBCL605	Mobile Application Security & Penetration Testing (SBL)	--	02	--	--	01	--	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					
IoTCSBCL605	Mobile Application Security & Penetration Testing (SBL)	--	--	--	--	25	25	–	50

Lab Objectives:

Sr No	Lab Objectives
1	To get acquainted with the concept of Android application ecosystem and development tools
2	To learn the concepts of developing and deploying android based applications
3	To understand Android security models, tools and frameworks
4	To understand Mobile Penetration testing concepts and tools.
5	To understand modeling threats for an droid applications
6	To apply different attacks on android applications

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	Describe the basic concept of Mobile OS, architectures and development environments.	L1,L2
2	Interpret the android development process and develop android applications	L1,L2,L3
3	Interpret different security concepts in Android applications	L1,L2,L3
4	Understand the concepts of penetration testing in mobile environments	L1,L2,L3
5	Analyze and develop attack plans and threat models for mobile application	L1,L2,L3
6	Interpret and develop the different attacks on Android applications using case studies	L1,L2,L3,L4

Prerequisite: System Security basics, Network Security basics and Mobile Application Development.

DETAILED SYLLABUS

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	Basics of security	Security attacks, vulnerabilities and OS and Network security	**02**	**-**
I	Fundamentals of Android Application Development	Different types of mobile applications platforms, Introduction of Android, features of Android, Android Application Architecture, Android Development Tools, Application packages (APK), Debug Bridge, Application sandboxing and signing, build process, and rooting, Application Manifest File, Android Application Lifecycle and Application Class. **Self-Learning Topics:** **iOS architecture**	**02**	LO1
II	Building android applications	Android Activity: Creating activities, Activity lifecycle and Android Activity classes. User Interface: Fundamental Android UI Design, Layouts, Fragments, Designing UI with views, Adapters, Linking Activities Using intents, Creating Intent Filters, Displaying notifications, and Broadcast Receivers, Content Providers and Database Connectivity **Self-Learning Topics:** **Android Firebase Connectivity and various APIs**	**04**	LO2
III	Basics of Mobile Application Security	Android permission model, key challenges in mobile application security, impact of mobile application security, Android vulnerabilities, The need for mobile application penetration testing, The mobile application penetration testing methodology, The OWASP mobile security project and risks. **Self-Learning Topics:** **Basic Security attack, threats, risks and pentesting methods**	**03**	LO3
IV	Building test environments and Mobile Pentesting tools	Android security tools: APKAnalyser, The drozer tool, APKTool, The dex2jar API, Androguard, QARK, MOBSF, Reversing the application. Mobile app penetration testing environment setup, Monkeyrunner, Genymotion. **Self-Learning Topics:** **Other vulnerable android apps like AndroGoat, Damn Vulnerable Bank**	**03**	LO4

V	Building Attack Paths – Threat Modeling an Application	Assets, Threats, Threat agents, Vulnerabilities, Risk, Approach to threat models. Threat modeling a mobile application: creating a threat model, Threat modeling methodologies, Using STRIDE to classify threats, A typical mobile application threat model, Building attack plans and attack trees, Threat model outcomes, Risk assessment. **Self-Learning Topics:** **Threat Modeling Methodologies like OCTAVE, PASTA, VAST etc. , Risk Analysis and Mobile Ransomware**	**06**	LO5
VI	Attacking Android Applications and Case Studies	Setting up the target app and analyzing the app using drozer, attacking android components, Attacking WebViews, SQL injection, Man-in-the-Middle (MitM) attacks, Encryption and decryption on the client side, Storage/archive analysis, Log analysis, Assessing implementation vulnerabilities, Binary patching. Attack case studies. **Self-Learning Topics:** **Various Case studies on Mobile attacks and vulnerabilities**	**06**	LO6

Text Books:

1. Mobile Application Penetration Testing, Vijay Kumar Velu, June 2017, Publisher(s): Packt publication, ISBN: 978-1-78588-337-8.
2. Mobile Application Hacker’s Handbook, Dominic Chell, Tyrone Erasmus, Shaun Colley and Ollie Whitehouse, Wiley publication.
3. Learning Pentesting for Android Devices, Aditya Gupta, Packt Publication.

Reference:

1. Android Security Internals: An In-Depth Guide to Android’s Security Architecture, Nikolay Elenkov, No Starch Press.

Online References:

1. https://nptel.ac.in/courses/106106147
2. Udemy courses:

a. https://www.udemy.com/course/mobile-application-security-and-penetration-testing-e/

b. https://www.udemy.com/course/android-penetration-testing-using-diva/

c. https://www.udemy.com/course/advanced-mobile-penetration-testing-of-android-applications/

3. https://www.eccouncil.org/programs/certified-penetration-testing-professional-cpent/

List of Experiments.

1. To install and configure Android Studio / Genymotion and Implement simple Android apk.

2. Building Android applications User interfaces using various Views and Layouts.

3. Developing Android applications using Receivers and Content Providers.

4. Developing user interactive Database applications (Using SQLite or other) in Android.

5. Deploying and Publishing Android application.

6. Reversing Android applications (APKs) APKTOOL, dex2jar and JD-GUI

7. Implementation of Android Rooting using tools like SRSroot/iRoot/ Root Genius/ Kingo etc.

8. Android Security Analysis for Hardcoding issues and Insecure Data Storage using DIVA

9. Android Security Analysis for Input Validation and Access Control using DIVA

10. Android Manifest File Analysis and SDK Misuse detection using MobSF tool

11. Android Application component detection using MobSF tool

12. Android Dynamic Code Analysis

13. Insecure logging and Client-side injection

14. Modeling Threats in android using STRIDE

15. Android Security Case Studies (minimum Two)

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

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
IoTCSBCM601	Mini Project :2B Blockchain & Security Model.	--	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.				
IoTCSB CM601	Mini Project :2B Blockchain & Security Model.	--	--	--	--	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
IoTCSBCDLO6011	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				
IoTCSBCDLO6011	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, OpenFlow controllers , POX and NOX. **Self-Learning Topics:** Case study on SDN.	**04**	CO6

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
IoTCSBCDLO6012	Application Security and Secure Coding Principles	03	--	--	03	--	--	03

<table>
<tr><th rowspan="4">Course Code</th><th rowspan="4">Course Name</th><th colspan="8">Examination Scheme</th></tr>
<tr><th colspan="4">Theory Marks</th><th rowspan="3">Term Work</th><th rowspan="3">Practical</th><th rowspan="3">Oral</th><th rowspan="3">Total</th></tr>
<tr><th colspan="3">Internal assessment</th><th rowspan="2">End Sem. Exam</th></tr>
<tr><th>Test1</th><th>Test 2</th><th>Avg. of 2 Tests</th></tr>
</table>

IoTCSBC DLO6012	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 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	**08**	CO1
II	Security related to Operating Systems, Internet and Social	Security Recommendations for Windows Operating Systems, Mac OS, Studying Web Browser Concepts, Immediate Messaging Security, Child Online Safety,	**08**	CO2

	Networking Sites	**Self-learning Topics:** Understanding Social Networking Concepts, and Facebook and Twitter Security Settings		
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
IoTCSBCDLO6013	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					
IoTCSBCDLO6013	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,	**06**	CO6

		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.		

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:
2. https://freevideolectures.com/course/4070/nptel-ethical-hacking
3. https://owasp.org/www-project-top-ten/
4. https://www.computersecuritystudent.com/
5. http://www.opentechinfo.com/learn-use-kali-linux/
6. https://pentesterlab.com
7. 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
IoTCSBCDLO6014	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					
IoTCSBCDLO6014	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 Computing Challenges. Identification of frames in cloud. Public, Private, Hybrid, **Self-Learning Topics:** Case study on different types of cloud ie private, public etc.	**04**	CO1
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, 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	**07**	CO4 CO5
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.