University of Mumbai

No. AAMS_UGS/ICC/2023-24/65

Sub: B.E. (Cyber Security) (Sem – VII & VIII).

CIRCULAR:-

Attention of the Principals of the Affiliated Colleges and Directors of the Recognized Institutions in Faculty of Science & Technology is invited to this office Circular No. AAMS (UG)/115 of 2022-23 dated 20th October, 2022 relating to the B.E. (Cyber Security) (Sem – V & VI) (CBCS) (REV- 2019 'C' Scheme).

They are hereby informed that the recommendations made by the Board of Deans at its meeting held on 27th October, 2023 **vide** item No. 6.5 (N) have been accepted by the Academic Council at its meeting held on 01st November, 2023 **vide** item No. 6.5 (N) and that in accordance therewith, syllabus of **B.E. (Cyber Security) (Sem – VII & VIII) (CBCS) (REV- 2019 'C' Scheme)** is introduced and the same has been brought into force with effect from the academic year 2023-24.

(The said circular is available on the University's website www.mu.ac.in).

MUMBAI – 400 032
24th November, 2023

(Prof. Sunil Bhirud)
I/c. REGISTRAR

To,

The Principals of the Affiliated Colleges and Directors of the Recognized Institutions in Faculty of Science & Technology.

A.C/6.5(N) /01/11/2023

Copy forwarded with Compliments for information to:-

1) The Chairman, Board of Deans,
2) The Dean, Faculty of Science & Technology,
3) The Chairman, Board of Studies,
4) The Director, Board of Examinations and Evaluation,
5) The Director, Department of Students Development,
6) The Director, Department of Information & Communication Technology,
7) The Director, Institute of Distance and Open Learning (IDOL Admin), Vidyanagari,
8) The Co-ordinator, MKCL.

Copy for information and necessary action :-

1. **The Deputy Registrar, College Affiliations & Development Department (CAD),**
2. **College Teachers Approval Unit (CTA),**
3. **The Deputy Registrar, (Admissions, Enrolment, Eligibility and Migration Department (AEM),**
4. **The Deputy Registrar, Academic Appointments & Quality Assurance (AAQA)**
5. **The Deputy Registrar, Research Administration & Promotion Cell (RAPC),**
6. **The Deputy Registrar, Executive Authorities Section (EA)**
   He is requested to treat this as action taken report on the concerned resolution adopted by the Academic Council referred to the above circular.
7. **The Deputy Registrar, PRO, Fort, (Publication Section),**
8. **The Deputy Registrar, Special Cell,**
9. **The Deputy Registrar, Fort Administration Department (FAD) Record Section,**
10. **The Deputy Registrar, Vidyanagari Administration Department (VAD),**

Copy for information :-

1. **The Director, Dept. of Information and Communication Technology (DICT), Vidyanagari,**
   He is requested to upload the Circular University Website
2. **The Director of Department of Student Development (DSD),**
3. **The Director, Institute of Distance and Open Learning (IDOL Admin), Vidyanagari,**
4. **All Deputy Registrar, Examination House,**
5. **The Deputy Registrars, Finance & Accounts Section,**
6. **The Assistant Registrar, Administrative sub-Campus Thane,**
7. **The Assistant Registrar, School of Engg. & Applied Sciences, Kalyan,**
8. **The Assistant Registrar, Ratnagiri sub-centre, Ratnagiri,**
9. **P.A to Hon'ble Vice-Chancellor,**
10. **P.A to Pro-Vice-Chancellor,**
11. **P.A to Registrar,**
12. **P.A to All Deans of all Faculties,**
13. **P.A to Finance & Account Officers, (F & A.O),**
14. **P.A to Director, Board of Examinations and Evaluation,**
15. **P.A to Director, Innovation, Incubation and Linkages,**
16. **P.A to Director, Department of Lifelong Learning and Extension (DLLE),**
17. **The Receptionist,**
18. **The Telephone Operator,**

Copy with compliments for information to :-

19. **The Secretary, MUASA**
20. **The Secretary, BUCTU.**

AC – 01/11/2023
Item No. – 6.5(N)

University of Mumbai

Syllabus for

B.E. (Cyber Security)

Semester – VII & VIII

Choice Based Credit System

REV- 2019 'C' Scheme

(With effect from the academic year 2023-24)

University of Mumbai

Syllabus for Approval

Sr. No.	Heading	Particulars
1	Title of Course	B.E. (Cyber Security)
2	Eligibility for Admission	After Passing Third Year Engineering as per the Ordinance 0.6243
3	Passing Marks	40%
4	Ordinances / Regulations (if any)	Ordinances 0.6243
5	No. of years/Semesters:	4 years / 8 semesters
6	Level	Under Graduation
7	Pattern	Semester
8	Status:	New REV-2019 'C' Scheme
9	To be implemented from Academic Year :	With effect from Academic Year: 2023-2024

Offg. Associate Dean
Faculty of Science and Technology

Offg. Dean
Faculty of Science and Technology

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.

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.

Preface by Board of Studies Team

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

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

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

Program Specific Outcome for graduate Program in Cyber Security

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

Program Structure for Fourth Year Engineering Semester VII & VIII
UNIVERSITY OF MUMBAI
(With Effect from 2023-24)
Semester VII

Course Code	Course Name	Teaching scheme (Contact Hours)		Credits Assigned		
		Theory	Pract	Theory	Pract	Total
CSC701	Machine Learning & Cyber Security	3	--	3	--	3
CSC702	Advance Web X.0 Security	3	--	3		3
CSDO701X	**Department Optional Course – 3**	**3**	**--**	**3**	**--**	**3**
CSDO702X	**Department Optional Course –4**	**3**	**--**	**3**	**--**	**3**
ILO701X	**Institute Optional Course – 1**	**3**	**--**	**3**	**--**	**3**
CSL701	DevSecOps Lab	--	2	--	1	1
CSL702	Web Application Security Lab	--	2	--	1	1
CSL703	ML & Security Lab	--	2	--	1	1
CSL704	Open-Source Intelligence (OSINT) Lab	--	2	--	1	1
CSP701	Major Project I	--	6#	--	3	3
Total		**15**	**14**	**15**	**7**	**22**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test1	Test2	Avg					
CSC701	Machine Learning & Cyber Security	20	20	20	80	3	--	--	100
CSC702	Advance Web X.0 Security	20	20	20	80	3	--	--	100
CSDO701X	**Department Optional Course – 3**	**20**	**20**	**20**	**80**	**3**	**--**	**--**	**100**
CSDO702X	**Department Optional Course –4**	**20**	**20**	**20**	**80**	**3**	**--**	**--**	**100**
ILO701X	**Institute Optional Course – 1**	**20**	**20**	**20**	**80**	**3**	**--**	**--**	**100**
CSL701	DevSecOps Lab	--	--	--	--	--	25	25	50
CSL702	Web Application Security Lab	--	--	--	--	--	25	25	50
CSL703	ML & Security Lab	--	--	--	--	--	25	25	50
CSL704	Open-Source Intelligence (OSINT) Lab	--	--	--	--	--	25	25	50
CSP701	Major Project I	--	--	--	--	--	25	25	50
Total		**--**	**--**	**100**	**400**	**--**	**125**	**125**	**750**

# indicates work load of Learner (Not Faculty), for Major Project

CSDO701X	Department Optional Course –3
CSDO7011	Advance Cloud Computing Security
CSDO7012	Software Testing & Quality Assurance (STQA)
CSDO7013	Storage Area Network
CSDO7014	Supervisory Control and Data acquisition (SCADA) Security

CSDO702X	Department Optional Course –4
CSDO7021	Cyber Security Management
CSDO7022	User Interface Design with Security
CSDO7023	MANET
CSDO7024	Information retrieval system

 # Institute Level Optional Course (ILO)

Every student is required to take one Institute Elective Course for Semester VII, which is not closely allied to their disciplines. Different sets of courses will run in the both the semesters.

ILO701X	Institute Optional Course – 1 (Common for all branches will be notified)
ILO7011	Product Lifecycle Management
ILO7012	Reliability Engineering
ILO7013	Management Information System
ILO7014	Design of Experiments
ILO7015	Operation Research
ILO7016	Cyber Security and Laws
ILO7017	Disaster Management and Mitigation Measures
ILO7018	Energy Audit and Management
ILO7019	Development Engineering

Program Structure for Fourth Year Engineering Semester VII & VIII
UNIVERSITY OF MUMBAI
(With Effect from 2023-24)

Semester VIII

Course Code	Course Name	Teaching Scheme (Contact Hours)		Credits Assigned		
		Theory	Pract	Theory	Pract	Total
CSC801	Malware Analysis	3	--	3	--	3
CSDO801X	**Department Optional Course – 5**	**3**	**--**	**3**	**--**	**3**
CSDO802X	**Department Optional Course – 6**	**3**	**--**	**3**	**--**	**3**
ILO801X	**Institute Optional Course – 2**	**3**	**--**	**3**	**--**	**3**
CSL801	Mobile Forensic Lab	--	2	--	1	1
CSL802	Dark Web Investigation Lab	--	2	--	1	1
CSP801	Major Project II	--	12#	--	6	6
Total		**12**	**16**	**12**	**8**	**20**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
CSC801	Malware Analysis	20	20	20	80	3	--	--	100
CSDO801X	**Department Optional Course – 5**	**20**	**20**	**20**	**80**	**3**	**--**	**--**	**100**
CSDO802X	**Department Optional Course – 6**	**20**	**20**	**20**	**80**	**3**	**--**	**--**	**100**
ILO801X	**Institute Optional Course – 2**	**20**	**20**	**20**	**80**	**3**	**--**	**--**	**100**
CSL801	Mobile Forensic Lab	--	--	--	--	--	25	25	50
CSL802	Dark Web Investigation Lab	--	--	--	--	--	25	25	50
CSP801	Major Project II	--	--	--	--	--	100	50	150
Total		**--**	**--**	**80**	**320**	--	**150**	**100**	**650**

# indicates workload of Learner (Not Faculty), for Major Project

Students group and load of faculty per week.

Mini Project 1 and 2:
Students can form groups with minimum 2 (Two) and not more than 4 (Four)
Faculty Load: 1 hour per week per four groups.

Major Project 1 and 2:
Students can form groups with minimum 2 (Two) and not more than 4 (Four)
Faculty Load: In Semester VII – ½ hour per week per project group.
In Semester VIII – 1 hour per week per project group

CSDO801X	**Department Optional Course – 5**
CSDO8011	Social & Ethical issues of the Internet
CSDO8012	IoTs & Embedded Security
CSDO8013	Cognitive Psychology in Cyber Security
CSDO8014	Intelligent Forensic

CSDO802X	**Department Optional Course –6**
CSDO8021	Advance Blockchain Technology
CSDO8022	Metaverse
CSDO8023	Green IT
CSDO8024	Cyber Security laws & legal aspects

IOTIO801X	**Institute Optional Course – 2 (Common for all branches will be notified)**
ILO8011	Project Management
ILO8012	Finance Management
ILO8013	Entrepreneurship Development and Management
ILO8014	Human Resource Management
ILO8015	Professional Ethics and CSR
ILO8016	Research Methodology
ILO8017	IPR and Patenting
ILO8018	Digital Business Management
ILO8019	Environmental Management

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSC701	**Machine Learning & Cyber Security**	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					
CSC701	**Machine Learning & Cyber Security**	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand basic concepts of artificial intelligence.
2	To develop problem solving ability using machine learning algorithms.
3	To examine clustering and classification based on machine learning techniques.
4	To study anomaly detection and analyze network traffic.
5	To detect, classify and analyze malware.
6	To understand Cyber Security Mechanisms Using Deep Learning techniques.

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 role of artificial intelligence in cyber security.	L1, L2
2	Use machine learning algorithms for solving the security issues.	L1, L2, L3
3	Provide solutions for real time security problems using machine learning algorithms.	L1, L2, L3
4	Develop awareness of latest trends and advances in security using machine learning.	L1, L2, L3, L4, L5, L6
5	Detect, classify and analyze malware.	L1, L2, L3, L4
6	Analyze Cyber Security Mechanisms Using Deep Learning techniques.	L1, L2, L3, L4

Prerequisite: Linear algebra, Probability theory and Basic statistics

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Linear algebra Basic Probability and Distributions-Binomial, Poisson, Normal, Exponential, Gaussian Basic statistics Eigen vectors and Eigenvalues	**02**	-
I	Introduction to Artificial Intelligence (AI)	What is AI, its goals, types of AI Types of agents, intelligent agent, agent environment search algorithms	**04**	CO1
II	Basics of Machine Learning in Cyber security	Definitions of machine Introduction to Machine Learning: Supervised Machine Learning, Unsupervised Machine Learning, Semi-supervised Machine Learning, Reinforcement Machine Learning Regression and its types. Applications of machine learning Real-World Uses of Machine Learning in cyber security, Spam Fighting: An Iterative Approach Limitations of Machine Learning in Security	**06**	CO2
	Self-learning topics	Case Studies on Taxonomy of machine learning algorithms		
III	Clustering and Classification	Supervised Classification Algorithms: Naive Bayes Classifier, Support Vector Machines (SVM), Decision Trees, Decision Forest, Nearest Neighbor, Neural Network. Practical Considerations in Classification: Selecting a Model Family, Training Data Construction, Feature Selection, Overfitting and Underfitting, Choosing Thresholds and Comparing Models. Clustering: K-means, Hierarchical clustering, Fuzzy C-Means Clustering, Density-Based Clustering, State of the Art of Clustering Applications. Optimization techniques	**08**	CO3
	Self-learning topics	Exploiting XSS Vulnerability in C&C Panels to Detect Malwares		
IV	Anomaly detection and Network Traffic Analysis Using ML	Anomaly Detection: Feature Engineering for Anomaly Detection Anomaly Detection with Data and Algorithms Challenges of Using Machine Learning in Anomaly Detection Network Traffic Analysis: Theory of Network Defense Building a Predictive Model to Classify Network Attacks.	**6**	CO4
	Self-learning topics	Network Anomaly Detection Using k-means Stages of a network attack		
V	Malware: detection & analysis	Malware Detection using support vector machine. Maximizing the Margin and Hyperplane Optimization, Lagrange Multiplier, Kernel Methods Permission-Based Static Android Malware Detection Using SVM. Malware Analysis: Defining Malware Classification, Malware: Behind the Scenes, Feature Generation, Data Collection, Feature Selection, From Features to Classification, How to Get Malware Samples and Labels	**8**	CO5

	Self-learning topics	API Call-Based Static Android Malware Detection		
VI	Deep Learning in Security	Introduction to deep learning in cyber security Cyber Security Mechanisms Using Deep Learning Algorithms Applying deep learning in various use cases	**05**	CO6
	Self-learning topics	Network Cyber threat Detection		

Textbooks:

1. Machine Learning and Security by Clarence Chio, David Freeman, O'Reilly Media; 1st edition, 2018
2. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
3. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s): Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

References:

1. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.
2. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.
3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.
4. Tom Mitchell. Machine Learning. McGraw Hill, 1997.

Online References:

1. What Is Machine Learning in Security? - Cisco
2. 5 Top Machine Learning Use Cases for Security

MOOC Courses:

1. NOC: Introduction to Machine Learning(Course sponsored by Aricent), IIT Madras
2. https://nptel.ac.in/courses/106/106/106106202/
3. Free Online Course: Machine Learning Security from Amazon | Class Central

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 marks.** Q.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** needs to be answered.

Subject Code	Subject Name	Theory	Practical	Tutorial	Theory	Practical/Oral	Tutorial	Total
CSC702	Advance Web X.0 Security	03	--	--	03	--	--	03

Subject Code	Subject Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSC702	Advance Web X.0 Security	20	20	20	80	--	--	--	100

Sr. No.	Course Objectives:
The course aims:	
1	To familiarize yourself with advanced web application security fundamentals.
2	To understand the methodical way of discovering vulnerabilities and plan strategies for mitigation.
3	To gain insight about the web application Penetration testing methods
4	To understand authentication and session management in web applications.
5	To discover and defend client-side web security attacks.
6	To gain insight about injection attacks on web datastore and web server.

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	To identify and describe web application security threats.	L1, L2
2	To review, discover and manage vulnerabilities of web Applications and plan strategies for mitigation.	L1, L2, L3, L4
3	To understand the web penetration testing workflow and organize a checklist for penetration testing with the help of usage of tools.	L1, L2, L3, L4
4	To apply access control, authorization and authentication mechanisms in web applications.	L1, L2, L3
5	To explore various client -side web application security aspects.	L1, L2, L3
6	To explain various injection attacks on data and server in web application	L1, L2, L3

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Introduction to Web applications Cookies, Session, Headers, Same-origin , Terminology And Tools	02	-
I	Introduction to Web X.0 security	N/W security vs application security, open web application security projects (OWASP), OWASP Top 10 flaws, Security fundamentals: Input validation, Attack surface reduction, classifying and prioritizing threats	04	CO1
II	Vulnerability Assessment	Defensive Software Architecture - Analyzing Feature Requirements, Authentication and Authorization Comprehensive Code Reviews: How to start code review, Archetypical vulnerabilities Versus Custom Logic Bugs, Secure coding Anti-patterns. Vulnerability Discovery- Security Automation (Static, Dynamic analysis), Vulnerability Regression Testing, Responsible Disclosure Programs Vulnerability Analysis- Vulnerability Management: Reproducing Vulnerabilities, Ranking Vulnerability Severity, Common and Advanced Vulnerability Scoring System Regression Testing, Mitigation Strategies	07	CO2
III	Web application Penetration testing	Web Intrusion/penetration Test workflow: OWASP checklist for web intrusion tests, Burp Pro based. Identifying hidden web contents Personal information, Email addresses, Credentials, CMS, files, Administration URL Common web page testing checklist entry points, backend or third-party web services, API calls, check flaws, errors, authentication at various levels and privileges, header security best practices, cookie/sessionID, duration, client source code, logout exits. Special page testing checklist Login page, CAPTCHA, Registration page, reset password, Upload Page Reporting	07	CO3
IV	Web Authentication, Session management	Access Control Overview: Basic components of access control, High-level access control process. Authentication fundamentals; Two-factor and three-factor authentication; Web Application Authentication, securing password-based authentication, securing web authentication mechanism. Authorization Fundamentals, Goals, Detailed authorization check process, Types of permissions, Authorization layers, Controls by layers, Custom authorization mechanisms, client-side attacks, Time of Check to Time of Use (TOCTTOU) Exploit, Web Authorization Best Practices, Attacks against authorization, Session Management Fundamentals, why do we need session management, Weaknesses in Token Generation, Weaknesses in Session Token Handling, Attacks against sessions, Securing web application session management, Session Management Best Practices	07	CO4

V	Client-side Security	Cross-site scripting (XSS): XSS Discovery and Exploitation, Stored XSS, Reflected XSS, DOM-Based XSS, Mutation-Based XSS Defending Against XSS Attacks: Anti-XSS Coding Best Practices, Sanitizing User Input, Content Security Policy for XSS Prevention Cross-Site Request Forgery (CSRF): Query Parameter Tampering, Alternate GET Payloads, CSRF Against POST Endpoints Defending Against CSRF Attacks: Header Verification, CSRF Tokens, Anti-CSRF Coding Best Practices	06	CO5
VI	Datastore and Server Security	SQL Injection; Setting Database Permissions; Stored Procedure Security; Insecure Direct Object References; Injecting into NoSQL, injecting into XPath, Injecting OS Commands, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, Injecting into Mail Services	06	CO6

Text Books:

1. Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman O'Reilly (Module 2)
2. Web application Security a beginners guide by Bryan Sullivan and Vincent Liu TMH
3. The Web Application Hacker's handbook, Defydd Stuttard, Wiley Publishing
4. Practical Web Penetration Testing by Gus khawaja, packt publication

References:

1. Joel Scambray, Vincent Liu , Caleb Sima ,"Hacking exposed", McGraw - Hill
2. Professional Pen Testing for Web application, Andres andreu, wrox press
3. Web Application Vulnerabilities: Detect, Exploit, Prevent,by Steven Palmer,Syngress publishing

Online References: **1.** **https://www.udemy.com/course/web-application-security/**

2. **https://owasp.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 marks.** Q.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** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO7011	**Advanced Cloud Computing Security**	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					
CSDO7011	**Advanced Cloud Computing Security**	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand the concept of security and its significance in the context of cloud computing.
2	To study cloud infrastructure security and mitigation techniques
3	To understand the working of Data center and Data Protection techniques
4	To develop a comprehensive understanding of challenges and solutions in secure identity management for cloud environments
5	To study Compliance and Security Audits policies for cloud data
6	To understand the Cloud Native 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	Understand the concept of security and its importance in the context of cloud computing.	L2
2	Analyze cloud infrastructure security and apply different mitigation techniques.	L3, L4
3	Apply different data protection techniques in data centers.	L3
4	Design and implement secure identity management solutions for cloud environments	L6
5	Interpret and appropriately apply the policies on Compliance and Security Audits for cloud data	L2, L3
6	Demonstrate cloud security tools for designing, implementing, and managing cloud-native security	L2, L6

Prerequisite: Knowledge of Cloud Computing and Cryptography and Network Security

DETAILED SYLLABUS

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basics of cloud computing, network and system security	**2**	

I	**Fundamentals Of Cloud Security Concepts**	What is security, why is it required in cloud computing, Different types of security in cloud, attacks, and vulnerabilities **Cloud Security Concepts** - CIA Triad (Confidentiality, integrity, availability), privacy, authentication, non-repudiation, access control, defence in depth, least privilege, Traditional vs Cloud Security, importance, challenges in different cloud environment (public, private, hybrid, muti-cloud) **Self-Learning Topic:** Real-world Example of CIA Triad - Bank ATM	**5**	**CO1**
II	**Cloud Infrastructure Security: Threats and Mitigation Techniques**	**Secure Infrastructure architecture** **Infrastructure Security:** Network Level, Host Level and Application Level Common attack vectors and threats **Mitigation techniques**- Isolation, Virtualization and Segmentation, Intruder Detection and prevention, Firewall, OS Hardening and minimization, Verified and measured boot. **Self-Learning Topics:** DoS, Man-in-the-Cloud, Insecure APIs, Insider Threats, Cookie Poisoning, Cloud Malware Injection,	**7**	**CO2**
III	**Cloud Data Security**	Cloud security principles Aspects of Data Security **Mitigation techniques**: Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key **Data center Security and Data Protection:** Physical and network **data** center security, Implementation of security in Virtual Data centers, East-west Traffic Protections, Types of firewall, IDS and IPS, DMZ **Provider Data and Its Security** **Self-Learning Topics:** **Case studies:** Capital One Data Breach, Uber's AWS Data Breach, Dow Jones Data Leak, Accenture AWS S3 Data Exposure, Verizon AWS S3 Data Exposure	**6**	**CO3**
IV	**Secure Identity Management in The Cloud: Challenges And Solutions**	IAM overview, Trust Boundaries and IAM, Architecture / Lifecycle process, IAM standards and protocols, IAM Challenges **Cloud Authorization Management:** **Identity management** - User Identification, Authentication and Authorization **Roles-based Access Control** - Multi-factor authentication, Single Sign-on, Identity Federation **Cloud Service Provider IAM Practice** **Self-Learning Topic:** IAM service in AWS	**6**	**CO4**
V	**Disaster Recovery Auditing: Mitigating Risk and Ensuring Compliance**	Cloud disaster recovery, types of disasters recovery, benefits of disaster recovery, cloud disaster recovery planning **Privacy:** Data life cycle, key privacy concerns in cloud, privacy risk management and compliance, legal and regulatory implications, **Cloud Audit and Compliance:** Internal Policy Compliance, Governance, Risk, and Compliance (GRC), Benefits, GRC Program Implementation, Cloud Security Alliance, **Self-Learning Topics:** HIPAA, ISO, PCI	**7**	**CO5**
VI	**Cloud Native Security in The Modern Organization**	Overview of Cloud Native Security, where it fits in the Modern Organization, purpose of Security, Cloud Native Security Architecture, Threats to Cloud Native Applications 3 R's and 4 C's of Cloud Native Security Cloud Native Security Controls, Cloud Native Security Tools, Cloud Native security architecture principles, DevSecOps,	**6**	**CO6**

		How to Measure the Impact of Security, Cloud-Native Application Protection Platform (CNAPP) **Self Learning Topic:** Case study on Secure the Cloud		

Textbooks:

1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather, Subra Kumaraswamy, and Shahed Latif, O'Reilly

2. Cloud Native Security Cookbook: Recipes for a Secure Cloud 1st Edition by Josh Armitage , O'Reilly

3. Cloud Security: A Comprehensive Guide to Secure Cloud Computing by Ronald L. Krutz and Russell Dean Vines, Wiley

References:

1. "Securing the Cloud: Cloud Computer Security Techniques and Tactics" by Vic (J.R.) Winkler, SYNGRESS

2. "Identity and Access Management as a Service: Security as a Service" by Wei Meng Lee

3. Cloud Security for Dummies by Ted Coombs, O'Reilly

Online References:

1. https://www.coursera.org/learn/cloud-computing-security#about
2. https://www.coursera.org/specializations/cybersecurity-cloud
3. https://www.edx.org/course/cloud-computing-security
4. **https://www.ibm.com/topics/cloud-security**
5. **https://www.vmware.com/topics/glossary/content/east-west-security.html**
6. **https://www.vmware.com/topics/glossary/content/data-center-security.html**
7. **https://cloud.google.com/learn/what-is-disaster-recovery**
8. **https://www.splunk.com/en_us/blog/learn/cloud-native-security.html**

1. 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 marks.** Q.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** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Pract/Oral	Tutorial	Total
CSDO7012	**Software Testing & Quality Assurance (STQA)**	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					
CSDO7012	**Software Testing & Quality Assurance (STQA)**	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To provide students with knowledge in Software Testing techniques.
2	To provide knowledge of Black Box and White Box testing techniques.
3	To provide skills to design test case plans for testing software.
4	To prepare test plans and schedules for testing projects.
5	To understand how testing methods can be used in a specialized environment.
6	To understand how testing methods can be used as an effective tool in providing quality assurance concerning software.

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	Investigate the reason for bugs and analyze the principles in software testing to prevent and remove bugs.	L1, L2, L3, L4
2	Understand various software testing methods and strategies.	L1, L2
3	Manage the testing process and testing metrics.	L1, L2, L3, L4
4	Understand fundamental concepts of software automation and use automation tools.	L1, L2
5	Apply the software testing techniques in the real time environment.	L1, L2. L3
6	Use practical knowledge of a variety of ways to test software and quality attributes.	L1, L2. L3

Prerequisite: Programming Language (C++, Java), Software Engineering

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Software Engineering Concepts, Basics of programming Language	**02**	
I	Testing Methodology	Introduction, Goals of Software Testing, Software Testing Definitions, Model for Software Testing, Effective Software Testing vs Exhaustive Software Testing, Software Failure Case Studies, Software Testing Terminology, Software Testing Life Cycle (STLC), Software Testing methodology, Verification and Validation, Verification requirements, Verification of high-level design, Verification of low-level design, validation. **Self-learning Topics:** Study any system/application, find requirement specifications and design the system. Select software testing methodology suitable to the application.	**07**	CO1
II	Testing Techniques	Dynamic Testing: Black Box Testing: Boundary Value Analysis, Equivalence Class Testing, State Table Based testing, Cause-Effect Graphing Based Testing, Error Guessing. White Box Testing Techniques: need, Logic Coverage Criteria, Basis Path Testing, Graph Matrices, Loop Testing, Data Flow testing, Mutation testing. Static Testing. Validation Activities: Unit validation, Integration, Function, System, Acceptance Testing. Regression Testing: Progressive vs. Regressive, Regression Testing, Regression Testability, Objectives of Regression Testing, Regression Testing Types, Define Problem, Regression Testing Techniques. **Self-learning Topics:** Select the test cases (positive and negative scenarios) for the selected system and Design Test cases for the system using any two studied testing techniques.	**09**	CO2
III	Managing the Test Process	Test Management: test organization, structure and of testing group, test planning, detailed test design and test Specification. Software Metrics: need, definition and Classification of software matrices. Testing Metrics for Monitoring and Controlling the Testing Process: attributes and corresponding metrics, estimation model for testing effort, architectural design, information flow matrix used for testing, function point and test point analysis. Efficient Test Suite Management: minimizing the test suite and its benefits, test suite minimization problem, test suite prioritization of its type, techniques and measuring effectiveness. **Self-learning Topics:** Design quality matrix for your selected system	**08**	CO3
IV	Test Automation	Automation and Testing Tools: need, categorization, selection and cost in testing tool, guidelines for testing tools. Study of testing tools: JIRA, Bugzilla, TestDirector and IBM Rational Functional Tester, Selenium etc. **Self-learning Topics:** Write down test cases, execute and manage using studied tools	**05**	CO4

V	Testing for specialized environment	Agile Testing, Agile Testing Life Cycle, Testing in Scrum phases, Challenges in Agile Testing Testing Web based Systems: Web based system, web technology evaluation, traditional software and web-based software, challenges in testing for web-based software, testing web-based testing. **Self-learning Topics:** Study the recent technical papers on software testing for upcoming technologies (Mobile, Cloud, Blockchain, IoT)	**04**	CO5
VI	Quality Management	Software Quality Management, McCall's quality factors and Criteria, ISO 9000:2000, SIX sigma, Software quality management **Self-learning Topics:** Case Studies to Identify Quality Attributed Relationships for different types of Applications (Web based, Mobile based etc.)	**04**	CO6

Textbooks:

1. Software Testing Principles and Practices Naresh Chauhan Oxford Higher Education
2. Software Testing and quality assurance theory and practice by Kshirasagar Naik, Priyadarshi Tripathy, Wiley Publication

References Books:

1. Effective Methods for Software Testing, third edition by Willam E. Perry, Wiley Publication
2. Software Testing Concepts and Tools by Nageswara Rao Pustular , Dreamtech press

Online References:

1. www.swayam.gov.in
2. www.coursera.org
3. http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1099 -1689
4. https://onlinecourses.nptel.ac.in/noc17_cs32/preview
5. https://www.youtube.com/channel/UC8w8_H_1uDfi2ftQx7a64uQ

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 marks.** Q.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** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
CSDO7013	**Storage Area Network**	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					
CSDO7013	**Storage Area Network**	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To provide the knowledge of types of Storage Network.
2	To examine NAS technology and its applications in Storage Area Networks.
3	To study Emerging Technologies in SAN.
4	To define backup, recovery, disaster recovery and business continuity in the storage area Network.
5	To learn cloud-based storage virtualization technologies in SAN.
6	To understand the logical and physical components of storage infrastructures.

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	Identify the limitations of the client-server architecture and evaluate the need for data protection and storage centric architectures such as Intelligent storage system.	L1, L2
2	Understand various SAN technologies.	L1, L2
3	Analyze and examine NAS technologies and its application in Storage Area Network.	L1, L2, L4
4	Explain Different I/O Techniques in SAN.	L1, L2
5	Elaborate Cloud based storage virtualization technologies in SAN.	L1, L2, L4
6	Explain and build Storage infrastructure management with security.	L1, L2, L3

Prerequisite: Operating System, Computer Organization, Computer Network

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Components of a Storage System Environment, Disk drive components, RAID levels, Cloud Computing	**02**	**--**
I	Introduction to Storage Area Network	**Intelligent Storage Systems (ISS)**, Storage Provisioning, Types of Intelligent Storage Systems **Evolution of Storage System:** Server-Centric IT Architecture and its Limitations, Storage-Centric IT Architecture and its Advantages, SAN & its advantages. **Self-learning Topics:** Case Study on Replacing a server with Storage networks**.**	**04**	CO1
II	Networked Attached Storage & its application	**Local File Systems:** File systems and databases, Journaling, Snapshots, Volume manager **Network File Systems, and File Servers:** Network Attached Storage (NAS), Performance bottlenecks in file servers, Acceleration of network file systems, Case study: The Direct Access File System (DAFS), **Shared Disk File Systems:** A case study The General Parallel File System (GPFS), **Applying NAS solution:** NAS workload characterization, applying NAS to departmental workloads, enterprise web workloads, and specialized workloads; Considerations when integrating SN and NAS: Differences and similarities, the need to integrate, future storage connectivity and integration. **Self-learning Topics:** Case study on Successful SAN Deployment steps**.**	**07**	CO2
III	Storage I/O Techniques	The Physical I/O Path from the CPU to the Storage System, SCSI, The Fiber Channel Protocol Stack, Fiber Channel SAN, IP Storage, InfiniBand-based Storage Networks, Fiber Channel over Ethernet (FCoE). **Self-learning Topics: C**ase Study on FCoE SAN.	**06**	CO3
IV	Backup and Data Archive	**Introduction to Business Continuity:** Information Availability, BC Terminology, BC Planning Lifecycle, Failure Analysis, Business Impact Analysis **Backup and Archive:** Backup Purpose, Backup Considerations, Backup Granularity, Recovery Considerations, Backup Methods, Backup Architecture, Backup and Restore Operations, Backup Topologies **Self-learning Topics:** Case Study on Replication strategy	**06**	CO4
V	Storage Area Network as a Service for Cloud Computing & Virtualization	**Virtualization and the cloud:** Cloud infrastructure virtualization, Cloud platforms, Storage virtualization, SAN virtualization **Virtualization Appliances:** Black Box Virtualization, In-Band Virtualization Appliances, Out-of-Band Virtualization Appliances High Availability for Virtualization Appliances, Appliances for Mass Consumption. **Storage Automation and Virtualization:** Policy-Based Storage Management, Application-Aware Storage Virtualization, Virtualization-Aware Applications. **Self-learning Topics:** Case study on symmetric and asymmetric virtualization in networks.	**06**	CO5

VI	Securing and Managing storage infrastructure	**Securing and Storage Infrastructure:** Information Security Framework, Risk Triad, Storage Security Domains, Security Implementations in Storage Networking, Securing Storage Infrastructure in Virtualized and Cloud Environments. **Managing storage infrastructure:** Monitoring the Storage Infrastructure, Storage Infrastructure Management activities, Storage Infrastructure Management, Challenges, Information Lifecycle Management, Storage Tiering. **Self-learning Topics:** Case study on SAN Management and Standards.	**08**	CO6

Textbooks:

1. G. Somasundaram, Alok Shrivastava, EMC Educational Services, "Information Storage and Management", Wiley India.
2. Storage Virtualization, Author: Clark Tom, Publisher: Addison Wesley Publishing Company
3. Ulf Troppens, Wolfgang Muller-Friedt, Rainer Wolafka, "Storage Networks Explained" Wiley Publication
4. "Introduction to Storage Area Networks" Jon Tate, Pall Beck, Hector Hugo Ibarra, Shanmuganathan Kumaravel, Libor Miklas, IBM Redbooks.

References:

1. Richard Barker and Paul Massiglia, ìStorage Area Network Essentials: A Complete Guide to Understanding and Implementing SANsî, Wiley India.
2. Storage Networks: The Complete Reference, by Robert Spalding (Author)
3. "Storage Network Management and Retrieval", Vaishali Khairnar, Nilima Dongre. Wiley

Online References:

1. /dhttps://www.itprc.com/ultimate-guide-to-storage-area-networks/
2. https://www.techtarget.com/searchstorageefinition/storage-area-network-SAN
3. https://www.snia.org/educational-library/object-storage-trends-use-cases-2021
4. https://www.sciencedirect.com/topics/computer-science/network-attached-storage
5. https://www.techtarget.com/searchstorage/tip/Understand-your-storage-infrastructure-management
6. https://sites.google.com/site/testwikiforfirstciscolab/shd/14-securing-the-storage-infrastructue
7. https://www.techtarget.com/searchdatabackup/tip/What-is-the-difference-between-archives-and-backups.

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 marks.** Q.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** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
CSDO7014	**Supervisory Control and Data acquisition (SCADA) Security**	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					
CSDO7014	**Supervisory Control and Data acquisition (SCADA) Security**	20	20	20	80	--	--	--	100

Course Objectives:

The course aims:

Sr. No.	Course Objectives
1	To understand SCADA systems operations and measuring the effectiveness of viable security controls.
2	To identify the challenges in securing current SCADA systems.
3	To interpret incident response, prioritization and notification in SCADA systems.
4	To plan SCADA contingency processes for Disaster Recovery and Business Continuity.
5	To assimilate Project Management for SCADA Systems.
6	Study new age SCADA systems utilities.

Course Outcomes:

On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
1	Understand SCADA systems operations and measuring the effectiveness of viable security controls.	L1, L2
2	Identify and analyze the challenges in securing current SCADA systems.	L1, L2, L4
3	Interpret incident response, prioritization, and notification in SCADA systems.	L1, L2, L3
4	Plan SCADA contingency processes for Disaster Recovery and Business Continuity.	L1, L2. L3
5	Assimilate Project Management for SCADA Systems.	L1, L2, L3
6	Demonstrate new age SCADA systems utilities.	L1, L2

Prerequisite: Computer Network and Security

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Computer Network and Security	**02**	
I	Industrial Control Systems and Metrics Framework	Evolution of Industrial Control Systems, ICS Industrial Sectors and their Interdependencies, ICS Operation and Components, ICS versus IT Systems Security, Metrics: Security group knowledge, Attack group knowledge, Access, Vulnerabilities, Damage potential, Detection and Recovery, Defining cybersecurity metrics. **Self-Study:** Other Types of Control Systems	**05**	CO1
II	The Cyberthreat to SCADA systems and Commercial product vulnerabilities	Directed attacks, Thwarted attacks, Successful attacks, Identified incidents, Microsoft: the leading supplier of software with vulnerabilities, Other major vendors: Oracle, IBM Google, Adobe, Apple, and Cisco. **Self-Study:** Improvement of SCADA Security	**07**	CO2
III	Incident Response and SCADA	Difficulties with SCADA and incident response, Incident analysis, Incident prioritization, Incident notification, choosing a containment strategy, Evidence gathering and handling, Basic forensics for standard computers, Identifying the attacker, Eradication and recovery, Evidence retention. **Self-Study:** Case study: DHS (Department of Homeland Security)	**07**	CO3
IV	Disaster recovery and business continuity of SCADA	Business continuity process, Types of plans, Examples of SCADA systems at risk, SCADA contingency planning process, SCADA system contingency plan development, Recovery phase, Sequence of recovery activities, Recovery procedures, Recovery escalation and notification, Reconstitution phase, Plan appendices, Maintenance of data security, integrity, and backup, Protection of resources, Identification of alternate storage and processing facilities. **Self-Study:** Client/server systems and Telecommunications systems	**07**	CO4
V	Project management for SCADA systems	Introduction, Areas of knowledge needed, Similarities and differences with the SCADA community, managing stakeholders and projects, how to be successful with SCADA implementations. **Self-Study:** Case study: SCADA implementations	**05**	CO5
VI	Supervisory control applications & Operator interface	Operating System Utilities, SCADA System Utilities, Program Development Tools, Access-Control Mechanisms, Standard System Displays, Logs and Reports. **Self-Study:** Standardized APIs, Site/Industry–Specific Displays, Historical Trending	**06**	CO6

Textbooks:

1. Guide to Industrial Control Systems (ICS) Security, Revision 2 by Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn
2. Handbook of SCADA/Control Systems, Second Edition by Robert Radvanovsky, Jacob Brodsky
3. Cybersecurity for SCADA Systems, Second Edition by Willam Shaw
4. Cyber-security of SCADA and Other Industrial Control Systems By Edward J. M. Colbert, Alexander Kott

References Books:

1. "Industrial Automation and Control System Security Principles" by Ronald L. Krutz and Russell Dean Vines
2. "SCADA Security: What's Broken and How to Fix It" by Robert Radvanovsky and Jacob Brodsky
3. "SCADA Security: Protecting Critical Infrastructure Systems" by Jack Whitsitt
4. "SCADA and Me: A Book for Children and Management" by Robert M. Lee

Online References:

1. https://www.inductiveautomation.com/resources/article/what-is-scada
2. https://www.dpstele.com/scada/introduction-fundamentals-implementation.php
3. https://www.parasyn.com.au/scada-services-rtu-solutions/#whataretheapplicationsusedinscada?
4. https://www.parasyn.com.au/scada-services-rtu-solutions/#whatarethegreatestproblemswithscadasystems?
5. https://www.forcepoint.com/cyber-edu/scada-security

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 marks.** Q.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** needs to be answered.