COURSE TITLE	**IDENTITY AND ACCESS MANAGEMENT**
COURSE CODE	**01CC0508**
COURSE CREDITS	**3**

Objective:

1 This course aims to equip students with a comprehensive understanding of Identity and Access Management (IAM) by covering core principles such as authentication, authorization, access control models, and identity lifecycle. Students will explore key IAM technologies like SSO, MFA, Directory Services, and PAM; design and implement secure IAM solutions aligned with organizational and compliance needs; manage digital identities through provisioning and governance; and identify and mitigate security risks associated with IAM systems.

Course Outcomes: After completion of this course, student will be able to:

1 Explain the fundamentals of Identity and Access Management (IAM), including its components, goals, and relevance in cybersecurity.

2 Explain key IAM technologies such as SSO, MFA, OAuth, SAML, and LDAP.

3 Implement IAM solutions using industry tools, including configuring identity federation and access policies.

4 Manage identity provisioning, de-provisioning, and governance processes in enterprise environments.

5 Analyze IAM security risks and recommend appropriate mitigation strategies and best practices.

Pre-requisite of course: Basic understanding of computer networks and operating systems. Familiarity with fundamental cyber security concepts. Prior exposure to web technologies or scripting

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to Identity and Access Management** Overview of IAM : Definition and importance of IAM, Evolution of IAM, Key concepts: Identity, Authentication, Authorization, and Accountability, IAM Framework :Components of IAM: Users, Roles, Permissions, Policies IAM lifecycle: Provisioning, Authentication , Auditing, IAM Standards and Protocols: SAML (Security Assertion Markup Language), OAuth 2.0 and OpenID Connect, LDAP (Lightweight Directory Access Protocol), IAM Challenges : Security risks and threats, Compliance and regulatory requirements (GDPR, HIPAA, etc.), Scalability and performance issues	5
2	**Authentication and Authorization** Authentication Methods : Password based authentication, Multifactor authentication (MFA), Biometric authentication, Token based authentication, Authorization Models : Role Based Access Control (RBAC), Attribute Based Access Control (ABAC), Discretionary Access Control (DAC),, Mandatory Access Control (MAC), Federated Identity Management : Single Sign On (SSO), Identity federation and trust relationships, Cross domain authentication, Emerging Trends in Authentication :, Password less authentication, Behavioral biometrics, Zero Trust Architecture.	6
3	**IAM Technologies and Tools** Directory Services : Active Directory, LDAP Directories, Cloud based directory services (e.g., Azure AD, AWS Directory Service), IAM Solutions, Cloud based IAM solutions (e.g., Okta, Ping Identity, Auth0), On premise IAM solutions (e.g., Oracle Identity Manager, IBM Security Identity Manager), Privileged Access Management (PAM) : Managing privileged accounts, Tools like CyberArk, Thycotic, and Beyond Trust Identity Governance and Administration (IGA) : Role management Access certification and recertification, Tools like SailPoint and Saviynt	7
4	**IAM Implementation and Best Practices** IAM Deployment Models: On premise vs. cloud based IAM, Hybrid IAM solutions, IAM Implementation Steps : Requirements gathering and analysis, Designing IAM architecture, Deployment and integration with existing systems, IAM Policy Development: Creating access control policies, Policy enforcement and monitoring, IAM Auditing and Compliance, Logging and monitoring access events,, Auditing IAM systems for compliance, Reporting and incident response	7
5	**Advanced Topics in IAM** IAM in Cloud Environments: Cloud IAM challenges and solutions, Managing identities across multi-cloud environments, IAM for IoT and Edge Computing : Identity management for IoT devices, Securing edge computing environments, Blockchain and Decentralized Identity : Self-sovereign identity (SSI), Blockchain based identity solutions, AI and Machine Learning in IAM :Behavioral analytics for threat detection, AI driven access control	7
Total Hours		**32**

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Research and Present on IAM Concepts: Students research Identity and Access Management (IAM), including identity, authentication, authorization, and accountability, and present its importance in cybersecurity.	2
2	**Practical 2** Analyze an IAM Security Breach Case Study: Analyze a real-world IAM-related breach (e.g., credential theft or privilege escalation), identifying vulnerabilities, attack vectors, and impact.	2
3	**Practical 3** Explore Authentication Methods: Study and compare different authentication methods such as password-based, multi-factor authentication (MFA), biometric, and token-based authentication.	2
4	**Practical 4** Implement Role-Based Access Control (RBAC): Design a simple RBAC model by defining roles, assigning permissions, and mapping users to roles in a simulated environment..	2
5	**Practical 5** Perform LDAP Directory Exploration: Use an LDAP browser tool to explore directory structures and retrieve user information using LDAP queries.	2
6	**Practical 6** Simulate Single Sign-On (SSO): Design and document a federated identity system showing how SSO works across multiple applications using trust relationships.	2
7	**Practical 7** Study IAM Protocols (SAML, OAuth 2.0, OpenID Connect): Analyze the working of IAM protocols and create a flow diagram showing authentication and authorization process	2
8	**Practical 8** Create IAM Policies and Access Rules: Design access control policies based on models like RBAC, ABAC, DAC, and MAC for a hypothetical organization.	2
9	**Practical 9** IAM Auditing and Logging Analysis: Study IAM logs and identify suspicious activities, understanding auditing and compliance requirements (e.g., GDPR, HIPAA).	2
10	**Practical 10** Mini Project: Design an IAM System: For a hypothetical organization, design a complete IAM solution including authentication methods, authorization model, policies, and auditing mechanisms.	2
Total Hours		**20**

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Textbook :

1 "Identity and Access Management: Business Performance Through Connected Intelligence", Ashok Kumar D, Notion Press, 2024

References:

1 Identity Management: A Primer, Identity Management: A Primer, Graham Williamson, Syngress / Elsevier, 2016

2 Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Tim Mather, Subra Kumaraswamy, and Shahed Latif, O'Reilly Media, 2009

3 OAuth 2 in Action, OAuth 2 in Action, Justin Richer and Antonio Sanso, Manning Publications, 2017

4 LDAP System Administration, LDAP System Administration, Gerald Carter, O'Reilly Media, 2003

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	5.00	10.00	35.00	35.00	15.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory or class-room.

Supplementary Resources:

1 "Identity and Data Security for Web Development: Best Practices" by Jonathan LeBlanc and Tim Messerschmidt

2 "Federated Identity Management: Concepts, Technologies, and Systems" by David Brossard

3 "Blockchain and Decentralized Identity: The Future of Digital Identity Management" by Alex Preukschat

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)