Securing Digital Identity: Biometrics, Identification, and Authentication Essentials

Duration: 24 hours

Course Overview:

In an increasingly digital world, safeguarding identity has become more critical than ever. This course offers a comprehensive overview of modern identity and access management (IAM) frameworks with a focused exploration of biometrics, identification, and authentication technologies. Participants will gain in-depth knowledge of how identification and authentication mechanisms operate, the role of biometrics in strengthening access control, and the associated privacy and ethical implications. The course also highlights emerging trends, common tools, and the risks organizations must manage while implementing these systems. This foundational course is designed to build awareness and understanding of the principles, challenges, and future of identity security in enterprise environments

Target Audience:

- IT professionals and system administrators
- Information security officers
- Risk and compliance teams
- Identity and access management (IAM) specialists
- Professionals responsible for privacy, cybersecurity, and digital transformation initiatives

1. Introduction to Identity and Access Management (IAM)

- Definition and Purpose of IAM
- Key Components: Identification, Authentication, and Authorization
- Role of Biometrics in Modern IAM Systems

2. Understanding Identification

- What is Identification?
- Identification vs. Authentication
- User Identity Lifecycle

3. Authentication Methods

- Types of Authentication (Single-Factor, Two-Factor, Multi-Factor)
- Knowledge, Possession, and Inherence Factors

- Authentication Protocols (e.g., SAML, OAuth, OpenID)

4. Biometrics: Concepts and Applications

- What is Biometric Authentication?
- Types of Biometric Modalities:
  - Fingerprint
  - Iris/Retina Scan
  - Face Recognition
  - Voice Recognition
  - Behavioral Biometrics
- Real-World Applications: Airports, Banking, Consumer Devices

5. Strengths and Limitations of Biometrics

- Accuracy, Usability, and Cost Factors
- False Acceptance and False Rejection Rates
- Spoofing and Anti-Spoofing Techniques

6. Biometric System Architecture

- Biometric Enrollment and Verification Process
- Storage and Template Protection
- Integration with IAM Systems

7. Privacy and Ethical Considerations

- Data Protection Regulations (e.g., GDPR, PDPL, HIPAA)
- Consent and Transparency in Biometric Data Collection
- Ethical Issues and Bias in Biometric Systems

8. Trends and Future of Biometric Authentication

- Advancements in AI and Machine Learning in Biometrics
- Multimodal Biometrics
- Contactless and Remote Biometric Systems

9. Risk Management in Biometric and Authentication Systems

- Threats to Identity Systems (Phishing, Spoofing, Insider Attacks)
- Mitigation Strategies
- Policy and Compliance Considerations