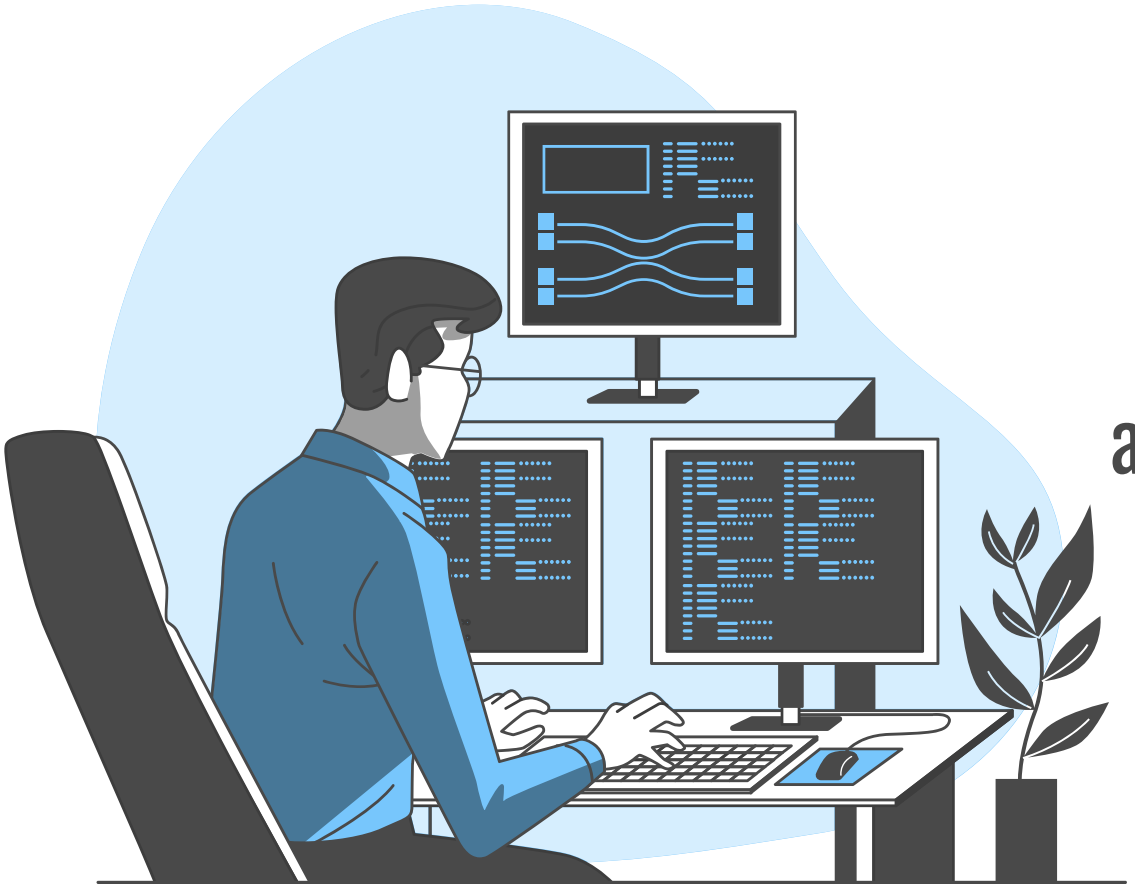


2.2 Need, Relevance and Criteria for authenticating of ICT resources

Dr. Priyanka Bhardwaj

Authentication

Authentication is the process of verifying the identity of a person, service, or device attempting to access a system or resource, ensuring they are who they claim to be. It's a core part of cybersecurity that happens before access is granted and involves presenting credentials, such as passwords, biometrics, or security tokens, which are then checked against a database to confirm legitimacy. Different authentication factors exist, categorized as "something you know" (password), "something you have" (phone), and "something you are" (fingerprint).

How Authentication Works

01

Identification:
A user or system presents its identity to the system.

02

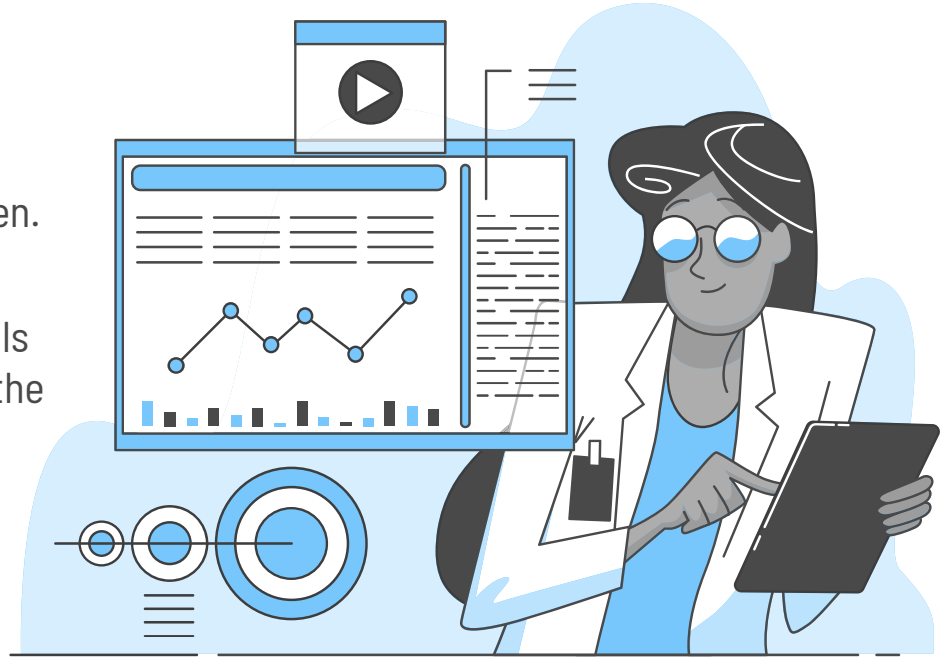
Credential Presentation:
The user provides proof of identity, which can be a password, a PIN, a fingerprint scan, or a hardware token.

03

Verification:
The system checks these credentials against a stored record to confirm the identity is valid.

04

Access Granting:
If the credentials match, the user is authenticated and gains access to the resource.



Dr. Priyanka Bhardwaj

Types of Authentication Factors

Something you know:

This includes knowledge-based factors, such as passwords, PINs, or security questions.

Something you have:

This involves physical objects that only the user possesses, like a mobile device, a security key, or a hardware token.

Something you are (or do):

These are biometric factors that are unique to the individual, such as fingerprints, facial scans, or behavioral patterns.

Types of Authentication

Single-Factor Authentication (SFA)

Two-factor Authentication (2FA)

Multi-Factor Authentication (MFA)

Biometric Authentication

Passwordless Authentication

Multi-Factor Authentication (MFA)

MFA is a more robust security measure that requires users to provide two or more different types of authentication factors to verify their identity. This layered approach significantly enhances security by making it much harder for attackers to gain unauthorized access, even if one factor is compromised.


Authentication
VS
Authorization
*****
****
Sign
***
VERIFY
Who are you?
Verify the user's identity.
Can you do that?
Determine user permissions.

Need for Authentication

Information Integrity:

The vast amount of information available through ICT can be unreliable, making it essential to verify its accuracy to avoid misinformation.

Security:

Authentication safeguards organizational and user data by ensuring only authorized individuals can access sensitive systems and resources, preventing cyber threats.

Ethical Responsibility:

For educational institutions and businesses, authenticating ICT resources is an ethical imperative to ensure learners and users receive credible, trustworthy information.

Security:

Proper authentication helps manage access to resources, preventing unauthorized use and ensuring resources are allocated effectively.

Dr. Priyanka Bhardwaj

Relevance of Authentication

Enhanced Learning:

In education, authentic resources lead to better learning outcomes because students receive accurate and relevant information, fostering critical thinking and digital literacy.

Improved Decision-Making:

For organizations, authentic data leads to better insights and informed strategic decisions, increasing competitiveness and operational efficiency.

User Trust and Credibility:

By providing verified resources, institutions build trust with their users, establishing a reputation for reliability and quality.

Legal and Regulatory Compliance:

Authentication helps organizations comply with data privacy laws and regulatory requirements by protecting sensitive information and systems.

Criteria for Authentication

Accuracy and Reliability:
Verify that the information presented is factually correct and up-to-date, often by checking the source and its credibility.

Appropriateness:
Ensure the resource is suitable for its intended audience (e.g., age-appropriate for students) and aligns with curriculum or organizational goals.

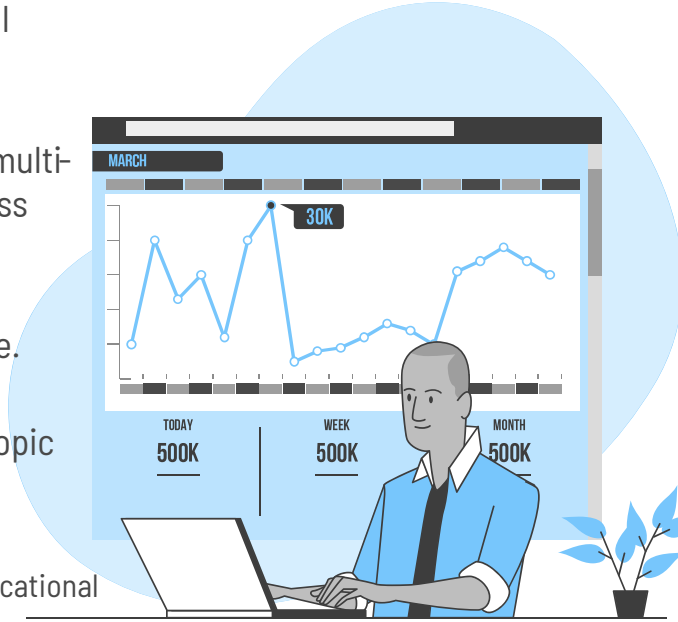
Usability and Accessibility:
The resource should be easy to use and access, with intuitive design and technical requirements that don't create unnecessary barriers.

Security:
This involves strong authentication processes to verify identity (e.g., passwords, multi-factor authentication) and confirm users have the necessary permissions to access resources.

Technical Compatibility:
Resources must be compatible with existing hardware and software infrastructure.

Content Completeness and Clarity:
The information should be comprehensive and easy to understand, covering the topic adequately.

Motivation and Engagement:
Resources should be engaging enough to capture and maintain user interest, particularly in educational contexts.



Thanks!

Do you have any questions?

Dr. Priyanka Bhardwaj