# **TEAM ZERODAY**

# ALTERNATE AUTHENTICATION

What is authentication?

# Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes and enterprise information security.

Why is authentication important in cyber security?

# Authentication enables organizations to keep their networks secure by permitting only authenticated users or processes to gain access to their protected resources. This may include computer systems, networks, databases, websites and other network-based applications or services.

How does authentication work?

# During authentication, credentials provided by the user are compared to those on file in a database of authorized users' information either on the local operating system server or through an authentication server. If the credentials entered match those on file and the authenticated entity is authorized to use the resource, the user is granted access. User permissions determine which resources the user gains access to and also any other access rights that are linked to the user, such as during which hours the user can access the resource and how much of the resource the user is allowed to consume.

# Traditionally, authentication was accomplished by the systems or resources being accessed. For example, a server would authenticate users use it own password, login IDs, or usernames and passwords.

Why is user authentication is important?

# User authentication is a method that keeps unauthorized users from accessing sensitive information. For example user a only has access to relevant information and cannot see the sensitive information of users B

# Cybercriminals can gain access to a system and steal information when user authentication is not secure . the data breaches companies like adobe ,Equifax ,and yahoo faced are example of what happens when organizations fail to secure their user authentication hackers gained access to yahoo user accounts to steal contacts , calenders and private emails between 2012 and 2016. The Equifax data breach in 2017 exposed credit card of more than 147 million consumers .without a secure authentication process, any organization could be at risk .

Facial recognition

# It Matches the different face characteristics of an individual trying to gain access to an approved face stored in a data base . face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar like close relatives . facial liveness like ID R&D’s passive facial liveness prevents spoofing.

# Many people are familiar with face recognition technology through the Face ID used to unlock IPhones (however, this is only one application of face recognition). Typically, facial recognition does not rely on a massive database of photos to determine an individual’s identity — it simply identifies and recognizes one person as the sole owner of the device, while limiting access to others.

# Beyond unlocking phones, facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts. Facial technology systems can vary, but in general, they tend to operate as follows:

# Step 1: Face detection

# The camera detects and locates the image of a face, either alone or in a crowd. The image may show the person looking straight ahead or in profile.

# Step 2: Face analysis

# Next, an image of the face is captured and analyzed. Most facial recognition technology relies on 2D rather than 3D images because it can more conveniently match a 2D image with public photos or those in a database. The software reads the geometry of your face. Key factors include the distance between your eyes, the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin. The aim is to identify the facial landmarks that are key to distinguishing your face.

# Step 3: Converting the image to data

# The face capture process transforms analog information (a face) into a set of digital information (data) based on the person's facial features. Your face's analysis is essentially turned into a mathematical formula. The numerical code is called a face print. In the same way that thumbprints are unique, each person has their own face print.

# Step 4: Finding a match

# Your face print is then compared against a database of other known faces. For example, the FBI has access to up to [650 million photos](https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through), drawn from various state databases. On Face book, any photo tagged with a person’s name becomes a part of Face book's database, which may also be used for facial recognition. If your face print matches an image in a facial recognition database, then a determination is made.

# Of all the biometric measurements, facial recognition is considered the most natural. Intuitively, this makes sense, since we typically recognize ourselves and others by looking at faces, rather than thumbprints and irises. It is estimated that over half of the world's population is touched by facial recognition technology regularly.

Speaker recognition

# Speaker recognition is the identification of a person from characteristics of voices .  It is used to answer the question "Who is speaking?" The term voice recognition can refer to *speaker recognition* or  speaker recognition. Speaker verification (also called speaker authentication) contrasts with identification, and *speaker recognition* differs from Speaker diarisation  (recognizing when the same speaker is speaking).

# Voice authentication is a form of identifying someone based on unique biometric characteristics - in this case, their voice. A voice is unique as a fingerprint and consists of a combination of characteristics such as dialect, pitch and speed. Voice authentication is harder to spoof than fingerprints and can't be hacked like passwords, making it an extremely secure method of authentication. Additionally, voice authentication is more convenient than other forms of biometric authentication (such as iris scans) because a person can authenticate remotely.

# Banks and healthcare, two of the most security-minded industries, are adopting voice authentication because it's accurate and convenient for their customers to use. To enroll in voice authentication, a customer needs to call the organization so they can record a voice sample. The voice authentication software then uses the multiple characteristics of the voice to create a voiceprint for the customer.

# Once the system has a voiceprint, the customer will have an enhanced experience when they call customer service. For example, the [interactive voice response (IVR)](https://www.nice.com/products/digital-self-service/interactive-voice-response-ivr) system can recognize and authenticate their identity, which enables the customer to access self-service tasks like checking account balances. If the customer chooses to speak to an agent, the authentication information can be passed to the agent, which saves time and improves the customer experience because they don’t need to repeat any information

# Recognizing the speaker can simplify the task of translating speech in systems that have been trained on specific voices or it can be used to authenticate or verify the identity of a speaker as part of a security process. Speaker recognition has a history dating back some four decades as of 2019 and uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and learned behavioral patterns.

Advantage of authentication

# 1. It provides more layers of security than 2FA.

# 2. It assures consumer identity.

# 3. It meets regulatory compliances.

# 4. It comes with easy implementation.

# 5. It complies with Single Sign-On (SSO) solutions.

# 6. It adds next-level security, even remotely.

# 7. It is an effective cyber security solution.

TEAM MEMBERS NAME : THENNAVAN . E ,

SHAFIQ AHAMED . A. A ,

SARAVANAN .G