MANTRA
Innovation that counts

Biometrics Log In
The new Face of Identity Management and Cybersecurity

Table of Contents:

Abstract

Nowadays, identity and access management demand the deployment of biometrics for apparent security and safety reasons. Their ready to use functionality, uniqueness and more complex to fake features make biometrics the most desirable means in security management. Biometric login is a secured login method to access and verify anything from tiny wearable devices and office door access systems to perform financial operations utilizing one's biometrics as a means. What started as using a simple username and password methodology is now a highly secure login/access mannerism with a highly reduced risk of data loss and identity theft with the help of Multi-Factor Authentication **MAF** involving biometrics.

Introduction

Biometrics is the most accurate and reliable form of authentication and verification method. Wearable devices, smartphones, attendance logs, core banking systems, and ID cards are only a few examples of biometric applications in our daily life.

Traditional password schemes have security flaws and more prone to spoofing, and lengthy passwords are difficult to remember. Most businesses offer access to workers based on their unique ID cards, which are created using forgeable information such as an employee's email address, password, and date of birth. On the other hand, biometric identity is the safest method of verification we have today. People keep their biometrics with them always, safe and ready to use at any time. Face recognition, iris scanning, fingerprint scanning, and palm scanning are just a few of the bio login methods available to users.

We live in a world where biometrics is unavoidable for secure verification applications. The application of biometrics varies from one sector to another; however, the end goal remains the same, i.e. accurate and secured Identity Management. Starting with the Government sector, utilizing biometrics for surveillance, criminal identification to provide subsidiary and beneficiary programs to the concerned class of individuals. The private sector has utilized the same for their workforce management to the machine and network access for secured monitoring purposes.

As the work from home is going to stay for a while, biometric authentication will be a superior technology for businesses to secure their information scattered across various locations in the form of laptops, hardware like Pen Drives and Hard Disks. It's just a glimpse of how biometrics can transform the future. Biometrics will bring more changes in personal computing and data security for corporations.

How does biometric login works?

Simply, we can say a biometric login offers additional security in the traditional security system. Instead of using a password or pattern, biometric devices connected to the personal computer use biometric data of the user to give access to the device. The best example of biometric login is the fingerprint sensor on your smartphone.

Nobody has to carry anything with them or in their minds while you seek access to a door or log into your desktop at your workplace. Biometric login can give two types of access; owner and guest access.

When somebody tries to access a computer, it will ask for the biometric data—say, fingerprint. When the person presses his finger against the sensing device connected to the system, it compares with the saved biometry of its owner. If it matches, the computer will give access or else will deny it.

Applications of biometric login

Current authentication methods based on passwords and ID cards are no longer considered safer methods. Biometric login methods are going to replace passwords where data security and workplace accountability are paramount. Following are the applications where biometric login is used.

1. Monitoring employee attendance

Biometric employee attendance methods truly require the presence of the person at the point of attendance. Fingerprint sensors were widely used for attendance registration. Due to the outbreak of the covid-19 crisis, organizations stopped using fingerprint sensors because of the possibility to spread the virus. Hence, contactless verification methods like face recognition are getting the attention of organizations.

The traditional punching system creates queues in front of the punching device every day. It is a time-consuming process, so there is a chance that employees can miss the time frame and losing their productive time in the queue. On the other hand, bio login devices can bring the punching process to each employee's desk. The bio login devices connected to each desktop in an office will be part of the attendance management system. The attendance management system will automatically record an employee's attendance when he or she connects to his or her office desktop.

2. Access control to applications/Network system

Access control to applications and network systems is essential for organizations for better data security. Consider a common desktop is available in an office space; employees, from manager to office boy, can access that computer. The access required for the manager is different from those of an accountant. So how do we distinguish? Setting up separate user profiles with enrolled biometrics for each individual offers an extra sense of security and adds one more layer of spoof-proof protection in the existing channel.

Biometric authentication will make the network system more robust. Here, the local network inside an organization will have the biometric data of all employees. The employee can use any desktop in the network using his biometric authentication, and he will get all his authorized access to the network. The system automatically restricts access to specific applications in the network for employees who are not authorized to it. Network access control is widely deployed in the banking sector and financial institutions, where money transfers and approvals should be more secure.

3. Verifying the user for Hardware access

Not all employees in an organization work using the computers in the office. Some employees might use laptops, and they might need to carry them to their homes or, say, onsite projects. Data protection in such cases cannot rely on weak passwords. Even if the password is correctly verified, how can the company make sure that it is their employee accessing their data?

It is quite normal for employees to take their office laptops with them to worksite projects. Face recognition and iris recognition technologies can be used in these instances to authenticate the individual before allowing access to company data. Specific drives in the system and peripheral devices such as pen drives and Hard disks can also be secured using biometric verification methods. Even if the devices are lost, the data will stay safe.

As mentioned in the previous section, laptops and other preferable devices can be secured using biometric encryption. But the security is not enough while the data is transmitted through the internet. These days, web applications like email, cloud, and other apps can be secured using biometric encryption. Signing in to your work computer and corporate resources using biometrics improves not only security but also accountability, which is why many companies are looking at biometrics for business network security.

Microsoft Windows Biometric framework

Windows Biometrics Framework offers the platform to the manufacturers of the Fingerprint machines to use their devices with the facility of Fingerprint Management application development (FMA) support and with inbuilt FMA in the latest OS versions. This functionality provisions developers with a compatible accessible driver and allows the developer to communicate with the interface of the client-side of the framework.

The Windows Biometrics Service (WBS) offers users a platform to enrol, store, compare and match the fingerprints on the local machine in an encrypted mannerism without enabling access to raw data, eliminating data theft.

Windows Hello compatibility with external biometric devices

Windows Hello is a biometric framework for Windows 10 users, facilitating biometric authentication for desktops and laptops. The Hello has integrated with the Windows biometric framework. It will work on computer devices that have face recognition cameras and fingerprint sensors. Hello requires Near-IR cameras to take a consistent and accurate image of the user. Most of the existing Windows 10 devices and upcoming budget devices don't support these feature. Only some of the mid-range and high-range devices are compatible with near-IR cameras.

Importance of WHQL in Bio login devices

Windows Hardware Quality Labs (WHQL) certifies a third-party hardware/software that will work satisfactorily in the Windows platform. WHQL certified drivers can use the Windows logo on them. A device with the Windows logo has been thoroughly tested to meet Microsoft's specifications and is thus compatible with any version of Windows.

With or without a WHQL certificate, any hardware device can be used with windows. But biometric devices deal with sensitive data that biometrics of a person, it is strongly advised to use WHQL certified biometric devices. The privacy of the biometric data will be safe with biometric devices that have WHQL certification. A WHQL certified biometric device can be used with any version of Windows starting with Windows 8.1 OS.

Importance of WBF

Earlier, Fingerprint Developers were designing unique sets of drivers, applications and SDK suiting the versions and platforms of OS. Windows, however, curated a single standard platform where all the developers get one common development platform for all the Fingerprint solutions proprietors with an objective for analogues user experience.

Windows introduced this concept with their Windows OS 7 and Windows Server 2008 R2 version, with external supporting FMA leading to the more solid model in its latest OS Windows 10 Hello with inbuilt FMA and more accepting & elaborated management functionalities with WBF.

Role of Fingerprint Management Applications

For Win8.1 or higher OS, FMA facility is inbuilt in the system. Under the Accounts -> Sign-In options, Windows provides access to enrol and remove Fingerprints from the system.

For lower windows OS versions, Fingerprint Management Application (FMA) needs to be downloaded additionally.

Explore Mantra's WHQL biometric devices

Mantra is one of the leading biometric manufacturers from India with a global presence. Mantra offers a wide range of biometric products for different applications, rising from fingerprint, iris, and facial recognition. Besides, Mantra offers biometric safety and security solutions for all types of industry.

Here are the range of WHQL certified biometric login devices from Mantra:

- **MAPRO OX** : The sensor uses optical fingerprint capturing technology for accurate fingerprint reading.
- **MAPRO CX** : Most advanced capacitive sensor in the range. A high-resolution sensor that produces high-quality images.
- **MFS500** : This optical scratch-free sensor offers auto finger detection functionality & auto capture with a built-in quality check

Benefits of Bio login devices

Selective FAP size and liveness detection in the high-end fingerprint scanners eliminate the concept of fingerprint duplication. In case of intrusion in the system, the fingerprint templates will also be in encrypted format in the local database with partial Fingerprint area captures, making it nearly impossible to reconstruct the Fingerprint impressions.

Due to manual labour or old age, fingerprints can be difficult to read when opting for an alternative such as Voice/Face recognition has been proved fruitful. Due to the latest innovations and creative utilization of fingerprint-based identification and verification solutions, fingerprint biometrics has been an undisputed front-runner in biometrics, and Bio log in applications.

Impact of biometric login in future

Cybersecurity experiences new threats every day; with every new and secured technology out there, there is always a new threat approaching its way and challenging its sustainability. To adapt to the increasing threats, continuous improvisation in the security of the system and constant monitoring of the operations and data management is crucial, especially in the field of biometrics. Once the biometrics data is lost, it can't be restored or reset. Utilizing Multi-Factor Authentication (MFA_ has proved to be improving the chances of cybersecurity.

A study conducted by VISA USA claims that consumers are already aware of the biometrics operability & perks and are more than inclined to shift towards biometrics from traditional passwords. Banking and Finance sector BFSI has embraced biometrics authentication in their applications and services. We can expect more growth of the same in industrial and retail applications.

It wouldn't be an understatement if we said that one's laptop/computer is a Pandora's Box with all of the individual's data. Industry leaders like HP, Lenovo, Acer, and Asus have rolled out laptops with inbuilt fingerprint sensors for consumers use. However, the high-end cost of these machines and Microsoft's WBF and FMA support have opened the way for cost-effective alternate external fingerprint device support, helping system integrators and biometrics manufacturers explore a new horizon in Identity Management. The surge in the improvisation of biometrics and data security is an unavoidable and necessary practice in the upcoming future.

MANTRA

Innovation that counts

+91-79-49068001 sales@mantratec.com