International Journal of Research in Engineering, Science and Management
Volume-2, Issue-10, October-2019
www.ijresm.com | ISSN (Online): 2581-5792

User Authentication in DBMS

Saurabh Yadav
Student, Department of Comuter Science, Thakur College of science and commerce, Mumbai, India

***Abstract*: Authentication is the process of recognizing a user's identification. The credentials provided are compared to those on a file in a database of the authorized user's information on local operating system or within an authentication server. It is important because it enables users to keep their identity and data secured. There are several types of authentication techniques such as password, two-factor authentication, biometrics, etc.**

***Keywords*: Biometric, Data Authentication, DBA, DBMS, Distributed DBMS.**

1. Introduction

Data is raw facts of information which should be translated into a form that is more convenient to process. Database is the collection of related data, which is organized in such a way that it can be easily managed. A Database Management System (DBMS) is a software which manages the data, it can perform operations like creation, insertion, modification, and deletion of data to manage it in a systematic way. Database system are designed to manage large amount of data by providing security from accidental crash of system and unauthorized access.

As organizations increase their reliance on, presumably distributed, distributed systems for daily business, they become additional at risk of security breaches when they gain productivity and potency blessings. The variety of techniques, like coding and electronic signatures, square measure presently accessible to shield knowledge once transmitted across sites, a very comprehensive approach for knowledge protection should conjointly embody mechanisms for imposing access management policies supported knowledge contents, subject qualifications and characteristics, and alternative relevant discourse info, like time. it's well understood these days that the linguistics of information should be taken into consideration so as to specify effective access management policies. Also, techniques for knowledge integrity and accessibility specifically tailored to information systems should be adopted. during this respect, over the years the information security community has developed variety of various techniques and approaches to assure knowledge confidentiality, integrity, and accessibility.

2. Authentication

Database authentication is that the method or act of confirming that a user UN agency is trying to log in to info is permitted to try and do therefore, and is barely accorded the rights to perform activities that he or she has been licensed to try and do. The construct of authentication is acquainted to nearly everybody. as an example, a mobile performs authentication by posing for a PIN. Similarly, a laptop authenticates a username by posing for the corresponding arcanum. In the context of databases, however, authentication acquires another dimension as a result of it should happen at completely different levels. it should be performed by the info itself, or the setup is also modified to permit either the software system, or another external methodology, to demonstrate users.

For example, whereas making a info in Microsoft's SQL Server, a user is needed to outline whether or not to use info authentication, software system authentication, or each (the alleged mixed-mode authentication). different databases within which security is predominant use near-foolproof authentication modes like fingerprint recognition and retinal scans.

A username may be a word, phrase, variety or combination of characters that unambiguously identifies a user on package, a website, a laptop or any computer or connected service that needs user authentication. A username may be a distinctive alphabetical and numerical set of characters won't to establish and gain access to an automatic data processing system. A username is additionally referred to as a login ID.

An arcanum may be a basic security mechanism that consists of a secret pass phrase created mistreatment alphabetic, numeric, character set and symbolic characters, or a mix. An arcanum is employed to limit access to a system, application or service to solely those users UN agency have memorized or hold on and/or area unit licensed to use it. An arcanum may additionally be referred to as Associate in Nursing access code, PIN or cryptograph.

A. Multi factor authentication

Multi-factor authentication (MFA) is an authentication methodology during which a somebody is granted access solely when with success presenting 2 or additional items of proof (or factors) to an authentication mechanism: information (something the user and solely the user knows), possession (something the user and solely the user has), and immanency (something the user and solely the user is).

Two-factor authentication (also called 2FA) may be a kind, or subset, of multi-factor authentication. it's a technique of confirming users' claimed identities by employing a combination of 2 completely different factors: 1) one thing they understand, 2) one thing they need, or 3) one thing they're. A good example of two-factor authentication is that the

withdrawing of cash from an ATM; solely the right combination of a charge card (something the user possesses) and a PIN (something the user knows) permits the dealing to be dole out. 2 alternative examples area unit to supplement a user-controlled positive identification with a one-time positive identification (OTP) or code generated or received by an critic (e.g. a security token or smartphone) that solely the user possesses.

Two-step verification or ballroom dance authentication may be a methodology of confirming a user's claimed ide they understand (password) and a second issue aside from one thing they need or one thing they're. Associate in Nursing example of a second step is that the user continuance back one thing that was sent to them through Associate in Nursing out-of-band mechanism. Or, the second step may well be a six-digit range generated by Associate in Nursing app that's common to the user and therefore the authentication system.

3. Biometric authentication

Biometric authentication may be a security method that depends on the distinctive biological characteristics of a private to verify that he's United Nations agency is says he's. Identity verification systems compare a biometric knowledge capture to hold on, confirmed authentic knowledge in a very info. If each samples of the biometric knowledge match, authentication is employed to manage access to physical and digital resources like buildings, rooms and computing devices.

In addition to the protection provided by hard-to-fake individual biological traits, the acceptance of biometric verification has conjointly been driven by convenience: One can't simply forget or lose one's biometry. The oldest well-known use of biometric verification is process. Thumbprints created on clay seals were used as a way of distinctive identification as way back as ancient China. trendy biometric verification has become virtually instant, and is more and more correct with the arrival of computerized knowledge bases and also the conversion of analog data. There are various types of Biometric Authentication Technologies are in used some of the are as follows.

A. Retina scan

Retina scanning may be a biometric verification technology that uses a picture of an individual's retinal vessel pattern as a singular characteristic attribute for access to secure installations.

Biometric verification technologies square measure supported ways that within which people are often uniquely known through one or a lot of distinctive biological traits. distinctive identifiers embody fingerprints, hand pure mathematics, lobe pure mathematics, membrane and iris patterns, voice waves, deoxyribonucleic acid and signatures.

Retina scanners square measure in use in several military bases, nuclear reactors and different high-security locations because of their strength as a security live. membrane scans square measure nearly not possible to faux. what is more, as a result of the membrane decays therefore quickly once death, a scan will solely be accessed from a living human membrane scanning goes back as way as 1935 in conception, by Doctors Carleton Simon and Isadore Goldstein. commercialized use goes back to 1984 with the corporate Identity, that pioneered the primary devices that used membrane scanning technology.

Fig. 1. Retina Scan

B. Facial Recognition

Facial recognition may be a class of biometric computer code that maps a person's countenance mathematically and stores the data as a faceprint. The computer code uses deep learning algorithms to match a live capture or digital image to the keep faceprint so as to verify a person's identity.

The computer code identifies eighty nodal points on an individual's face. during this context, nodal points endpoints accustomed measure variables of a person's face, like the length or dimension of the nose, the depth of the attention sockets and therefore the form of the cheekbones. The system works by capturing data for nodal points on a digital image of an individual's face and storing the ensuing information as a faceprint. The faceprint is then used as a basis for comparison with data captured from faces in a picture or video. biometric authentication system solely uses eighty nodal points, it will quickly and accurately establish target people once the conditions are favourable. However, if the subject's face is part obscured or in profile instead of facing forward, this kind of computer code is a smaller amount reliable. per the National Institute of Standards and Technology (NIST), the incidence of false positives in biometric authentication systems has been halved each 2 years since 1993.

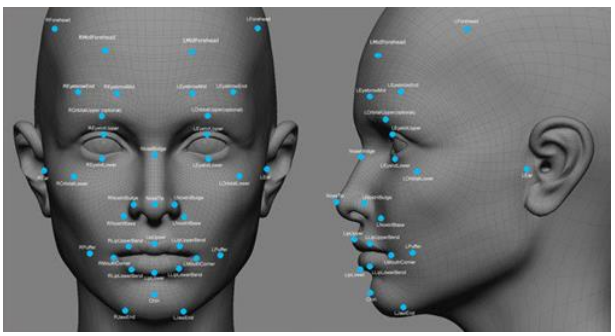

Fig. 2. Facial Recognition

High-quality cameras in mobile devices have created facial recognition a viable option for authentication in addition as identification. Facebook uses biometric authentication computer code to tag people in images. Other samples of biometric authentication embody Amazon, MasterCard and Alibaba, UN agency have unrolled biometric authentication payment strategies unremarkably noted as selfie pay. The Google Arts & Culture app uses biometric authentication to spot deposit doppelgangers by matching a true person's face print with a portrait's face print.

C. Fingerprint Scanning

A fingerprint scanner may be a kind of technology that identifies and authenticates the fingerprints of a private so as to grant or deny access to a computing system or a physical facility.

It is a sort of biometric security technology that utilizes the mix of hardware and computer code techniques to spot the fingerprint scans of a private.

Fig. 3. Fingerprint Scanning

A fingerprint scanner generally works by 1st recording fingerprint scans of all licensed people for a selected system or facility. These scans square measure saved inside a info. The user requiring access puts their finger on a hardware scanner, that scans and copies the input from the individual and appears for any similarity inside the already-stored scans. If there's a positive match, the individual is granted access. Fingerprint scanners most ordinarily use a person's fingerprint as identification.

4. Biometric authentication working

Biometric authentication works by examination 2 sets of data: the primary one is preset by the owner of the device, whereas the other belongs to a tool traveler. If the 2 knowledge square measure nearly identical, the device is aware of that "visitor" and "owner" square measure one and therefore the same, and offers access to the person.

The vital factor to notice is that the match between the 2 knowledge sets should be nearly identical however not precisely identical. this can be as a result of it's on the brink of not possible for two biometric knowledge to match 100 percent. for example, you would possibly have a rather sweating finger or a small, small scar that changes the print pattern.

Designing the method so it doesn't need an explicit match greatly diminishes the possibility of a false negative (the device doesn't acknowledge your fingerprint) however conjointly will increase the chances that a faux fingerprint may be thought-about real.

5. Biometric authentication vs. Password protection

Unless you don't connect to the internet – that clearly isn't true – there's no way to avoid passwords: it's the foremost common and widespread method of acting any on-line activity in a secure setting. That additionally implies that several users can get swamped by the abundance of passwords, associated security queries and protocols that require to be remembered. And this is often just for on-line accounts, too, therefore unless the all-important notebook during which the watchwords square measure unbroken is with you otherwise you use a similar password everyplace, the requirement for a watchword manager arises. memory each complicated watchword created for the numerous on-line accounts we have a tendency to all have is Associate in Nursing not possible mission for the common user.

Even with the ballroom dance verification or two-factor authentication demand there's no guarantee that the data you unlock is safe from the prying eyes of hackers, thieves or the likes of, WHO will use 'digital signature' patterns to interrupt into people's accounts and steal sensitive info or build fallacious transactions.

Biometrics could be a potential answer to combat this downside, that dramatically strengthens the protection level of the authentication processes too. firms adopt identity verification as a result of, in theory, this sort of identification – a fingerprint, face, or voice – ensures a high degree of certainty of a user's identity. In alternative words, by victimisation bioscience – in Apple's case, bit ID or Face ID – a corporation will be additional sure that the user unlocking their phone is that the rightful owner of that specific device. This creates a considerably safer setting and is way easier to use since it doesn't need memorizing a group of characters. It's additionally price noting that biometrics are a lot of harder to govern than passwords and/or alternative two-step identification and two-factor authentication processes. however that doesn't mean they're unbreakable: bioscience simply creates a safer setting, and has so become the bottom of a replacement system that could be a safer various to passwords.

And finally, a reminder: biometric identification is additionally liable to hacking – and not solely passwords – however with a big twist. If your biometric identity is taken, it equates to your identity being taken since it can't be modified or changed as a result of that's distinctive to each single person. If a watchword is taken it will be modified, however you can't (easily) amendment your fingerprints or your face. As always, use a watchword manager to form robust and distinctive passwords to shield your on-line identity. watchword managers

can cue you once it's time (to amendment to vary to alter) the watchword – it's extremely suggested that you simply change them often – adding another layer of security. Biometrics? It's convenient and quick, however if not guarded safely it, too, will create even as serious a risk to your personal life and not simply your digital life.

6. Advantages of password protection

- Easy Implementation. Password authentication systems exist in software.
- Low Cost. Because software handles password authentication, the only cost comes from the minor effort required for programming.
- Easy to Change.
- Widely Used.
- Reliable.

7. Disadvantages of password protection

As a result, they are doing not pay comfortable attention to showing wisdom selecting passwords nor protective them. There are many ways that within which AN persona non grata will attack password-protected systems. the foremost common kind of attack is countersign idea.

8. Advantages of biometric authentication

A. Accurate Identification and Accountability

Biometric systems offer a lot of correct identification, lowering your risk of unwanted breaches. With this kind of security system, access is granted not by passwords or good cards however by biological characteristics like iris scans or fingerprints that ar troublesome to duplicate or forge.

This a lot of correct info helps with security likewise as answerability. work activity through a biometric security system helps connect personnel with specific actions or events which will be observed within the unfortunate case of a security breach.

B. Efficient

Incorporating bioscience into your business security can prevent time and cash. Biometric security systems are designed with easy use in mind and provides you correct results with negligible effort. With the correct security system supplier, installation of a biometric security system straightforward} and manageable with simple, easy coaching.

C. Scalable

As your business develops and grows, it's vital to possess systems in situ which will scale with the expansion of your business. Biometric security systems are versatile and simply ascendable. whether or not you would like to secure a lot of areas of your facility or simply add a lot of information for added workers, biometric security systems can grow aboard your business for ease and security.

9. Drawbacks of biometric authentication

A. Cost

Despite being cheaper than ever, biometric systems will still be big-ticket to implement for the precise use cases or smaller outfits. attributable to this reality, biometric system might not best the most effective plan for applications wherever range of individuals to spot is incredibly less and may be managed with manual strategies. Regular maintenance of biometric systems is additionally vital to make sure optimum performance, however, it additionally ensure extra value.

B. Technical complexity

While most a part of preparation and implementation of a biometric system is taken care by its merchandiser, biometric systems might need the administrator to possess a particular level of tech-friendliness to use, maintain and perform day-after-day back-end operations. Some organizations might not be snug therewith half and will realize biometric systems too advanced.

10. Conclusion

User authentication is well required for any DBMS, without this data of user can be at huge risk. User authentication keeps the integrity of data. This different technique helps the users to keep data safe. Database are a favorite target for the attackers because of the large volume of data available of different users. Database security mechanism should not irritate the user, so biometric authentication helps the user to get authenticate easily.

References

[1] https://www.computer.org/csdl/journal/tq/2005/01/q0002/13rRUx0xPol
[2] https://www.techopedia.com/definition/27388/database-authentication
[3] https://www.techopedia.com/definition/4153/username
[4] https://en.wikipedia.org/wiki/Multi-factor_authentication
[5] https://whatis.techtarget.com/definition/retina-scan
[6] https://searchsecurity.techtarget.com/definition/biometric-authenticatio
[7] https://searchenterpriseai.techtarget.com/definition/facial-recognition
[8] https://www.techopedia.com/definition/29808/fingerprint-scanner
[9] https://heimdalsecurity.com/blog/biometric-authentication/#WhatIs
[10] https://password-managers.bestreviews.net/biometrics-vs-passwords-biometrics-secure/
[11] https://www.veridin.com/blog/5-advantages-of-biometric-security-systems/
[12] https://www.bayometric.com/advantages-disadvantages-biometric-identification/