American Research Journal of Computer Science and Information Technology

Volume 7, Issue 1, 42-46 Pages
Research Article | Open Access
ISSN (Online)- 2572-2921
DOI : 10.21694/2572-2921.24010

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Multi-Factor Authentication Based on Biometric Data

Asha Seshagiri

Software Development Engineer 3 at Expedia, Austin Texas, United States.

ABSTRACT

The article discusses aspects of multi-factor authentication (MFA) using biometric data, which is one of the most effective methods of protecting information systems from unauthorized access. Traditional authentication methods such as passwords are often vulnerable to various types of attacks, including phishing and brute force attacks. The introduction of biometric data, such as fingerprints, and face and voice recognition, significantly increases the level of security due to their uniqueness and complexity of forgery. The article highlights the advantages and challenges associated with the integration of biometrics into MFA systems, including technical and organizational aspects. Examples of successful application of biometric technologies in various fields are also considered and recommendations are given to improve their reliability and ease of use. Special attention is paid to adaptive authentication and password-free methods, which represent the future of cybersecurity.

KEYWORDS: *authentication, biometric data, biometrics, multifactor authentication.*

INTRODUCTION

Recent studies indicate that 92% of enterprises believe the future of security lies in moving away from traditional passwords. The use of biometric security significantly enhances the effectiveness of multi-factor authentication (MFA), as an individual's unique characteristics are extremely difficult to counterfeit. Implementing MFA adds several layers of protection that are exceptionally hard to breach. Hackers face much more complex challenges and often give up when confronted with such barriers. Consequently, the use of MFA significantly reduces security-related risks.

Therefore, integrating biometrics into multi-factor authentication provides organizations with an effective tool for ensuring robust data protection, minimizing the risks associated with traditional authentication methods [1].

This article will thus provide an in-depth examination of multi-factor authentication based on biometric data.

General Characteristics of Authentication Use

Authentication is the process of verifying the identity of a user in information systems, confirmed electronically. Depending on the number of factors used, authentication can be divided into two groups, as shown in Table 1.

Table 1. Authentication factors

Authentication Factor	Description
Single-Factor Authentication	Single-factor authentication involves using one element to verify a user's identity. An example is entering a password to confirm ownership of a user ID. This type of authentication is considered the least secure. If the password is disclosed, either intentionally or accidentally, the account can be compromised, and an unauthorized user may gain access by trying commonly used passwords. Single-factor authentication often employs minimal password complexity, reducing its reliability.
Multi-Factor Authentication	Multi-factor authentication involves using two or more authentication methods based on different factors. This approach significantly enhances security, as the user must provide proof of identity belonging to different categories of factors. Multi-factor authentication is critical in fields requiring a high level of security, such as handling hazardous substances, highly confidential information, or financial transactions. An example of multi-factor authentication is the use of ATMs: to access an account, the user must present a card (possession factor) and enter a PIN (knowledge factor) [2].

Multi-Factor Authentication

Multi-factor authentication (MFA) is an advanced security technology that integrates multiple methods of user identity verification into a single system. This is necessary to confirm the authenticity of a user before granting access to software, products, or executing transactions.

The main components of this technology include passwords, security tokens, and biometric verification. Implementing these elements creates a multi-layered protection system that significantly enhances the security of a product or transaction. A robust MFA structure prevents unauthorized access to targeted systems and technologies and reduces the risks of security breaches, data theft, and online fraud.

MFA is widely used to protect computing devices, databases, networks, and software. Implementing this technology is an essential step in ensuring cybersecurity and protecting confidential information in the modern digital world (see Fig.1) [3].

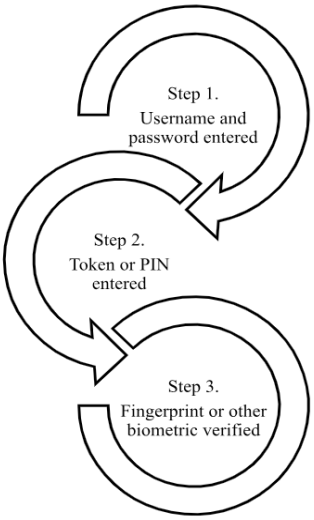

Fig.1. Steps to implement multi-factor authentication [3]

Next, let's examine how multi-factor authentication (MFA) works. Suppose you are logging into a Microsoft account or a work or school account and you enter your username and password. If these are the only credentials required for access, anyone who knows the username and password can log in from anywhere in the world.

However, with MFA enabled, the situation becomes much more secure. When logging into a device or application for the first time, you enter your username and password as usual. Still, then the system requires a second factor to verify your identity.

For example, you can use the Microsoft Authenticator app as the second factor. By opening the app on your smartphone, you will see a unique, dynamically generated 6-digit code that you need to enter on the website to complete the authentication.

If someone else tries to log in with your username and password, they will encounter an additional step—the second factor. Without your smartphone, the intruder cannot obtain the necessary 6-digit code. Moreover, the code in the Microsoft Authenticator app changes every 30 seconds, so even if someone learns the code you used yesterday, they cannot login today.

Thus, multi-factor authentication significantly enhances security by preventing unauthorized access to your accounts [4].

Next, we will examine the existing types of multi-factor authentication systems in Table 2.

Table 2. Types of multifactor authentication systems

Type of Multi-Factor Authentication System	Description
Knowledge Factors	Knowledge factors include passwords, PINs, and answers to security questions. Passwords are most commonly used as the first factor of authentication. However, these factors are vulnerable to phishing attacks, malware installation, and brute force attacks. Attackers can obtain passwords and other knowledge factors through basic social media research or social engineering. Using two factors of the same type, such as a password and a security question, is not true multi-factor authentication. It is rather a two-step verification process that provides some additional security but is not as reliable as a true MFA.

Possession Factors	Possession factors include digital software tokens and physical hardware tokens. Software tokens, such as digital security keys, are stored on the user's devices, like smartphones. They can take the form of digital certificates or one-time passwords (OTP) that change with each login. Some MFA solutions send OTPs to the user's phone via SMS, email, or phone calls. Others use authenticator apps that generate time-limited one-time passwords. Physical tokens can be in the form of USB devices or smart cards. The main advantage of possession factors is that attackers need to physically obtain the user's device to gain account access. However, these tokens can be stolen, lost, or subject to malware attacks.
Inherent Factors	Inherent factors, or biometrics, include fingerprints, facial features, and retina scans. These factors are difficult to hack, but it is possible. For example, researchers have managed to hack fingerprint scanners on some devices by replacing registered users' fingerprints with their own. The problem is that biometric data cannot be quickly changed, making it difficult to regain control over an account after compromise.
Behavioral Factors	Behavioral factors include analyzing user behavior, such as location, typing speed, and typical IP addresses. For instance, logging in from a trusted device may require only one authentication factor. Hackers can spoof their IP addresses or use trusted devices to trick the system.
Adaptive Authentication	Adaptive authentication systems change requirements based on the level of risk. The system uses artificial intelligence to assess user activity and adjust authentication tasks. For example, logging into a low-level application from a trusted device might only require a password, while accessing sensitive information may require additional factors.
Passwordless Authentication	Many organizations aim for passwordless authentication, relying on possession factors and biometric data. Such systems may use fingerprints and physical tokens without the need for password entry. Although most modern MFA systems still use passwords, it is expected that more solutions will eliminate them in the future. Large companies like Google, Apple, IBM, and Microsoft have already started implementing such authentication methods [5].

Multi-Factor Authentication Based on Biometric Data

The core concepts of biometric authentication involve using unique physiological or behavioral characteristics of an individual. This method is convenient for users as it does not require remembering information or possessing an object. However, biometric equipment must be accurate enough to distinguish between people with similar data.

All biometric data are divided into two classes:

- Static: Physiological features that do not change over time, such as fingerprints, iris patterns, retinal patterns, vein patterns, face geometry, hand geometry, and DNA.
- Dynamic: Behavioral characteristics based on human movements, such as handwriting, signature dynamics, voice, speech rhythm, gesture recognition, keystroke dynamics, and gait.

Biometric identification methods, such as fingerprint and voice recognition, are actively being implemented to enhance the reliability of systems. The use of biometric technologies on mobile platforms stimulates the growth of the mobile applications market. Fingerprint recognition is one of the most common biometric technologies. Its usage demonstrates convenience and high reliability. Modern fingerprint scanners are compact and can be integrated into various devices, including smartphones and ATMs. In forensics, fingerprints are used for criminal identification, and in some countries, they are required for obtaining a visa.

Voice recognition is more complex as it includes both physiological and behavioral biometric data. A voice signature is unique, but the accuracy of the method can decrease due to voice changes. Voice identification is effective as an additional method in multi-factor systems.

The proposed biometric system is a client-server mobile application for two-factor authentication. Biometric identification involves comparing the user's biometric data with reference models stored in a database. The system uses encryption algorithms resistant to quantum computing to protect the data.

The server application, written in Java, provides access to biometric data and user authorization. The Android client application offers functions for authorization, adding and deleting biometric data, and authentication in third-party applications.

To enhance the reliability and efficiency of the system, the F-measure is used, combining the precision and recall of recognition algorithms. Calculations based on a sample of 100 users show that the system's accuracy is around 79%.

Using more precise algorithms, such as Mel-Frequency Cepstral Coefficients (MFCC) and Gaussian Mixture Models (GMM), can improve voice recognition accuracy [6]. The essence of the MFCC method is that the Mel-Frequency

Cepstral Coefficients represent a short-term power spectrum of sound, based on a linear cosine transform of a log power spectrum on a nonlinear Mel scale of frequency. MFCC is determined as follows:

1. The audio signal is divided into several frames, each with a short time scale.

2. The power spectrum values are calculated for each frame.

3. The energy sum in each filter is determined by applying a set of Mel filters to the power spectra.

4. The logarithms of all the above block filter energies are taken.

5. A discrete cosine transform (DCT) of the list of logarithmic filter bank energies is generated.

6. The amplitudes of the resulting spectrum are the MFCC [7].

In turn, the Gaussian Mixture Model (GMM) is widely used in many statistical modeling tasks. Theoretically, it can be shown that with a sufficient number of mixtures, a GMM can approximate an arbitrary probability distribution. However, a larger number of mixtures requires more training data to obtain a well-trained model. In practice, the number of mixtures is determined by the volume of training data, the complexity of the actual distribution, and the computational power the system can handle. A GMM represents a weighted sum of M multivariate Gaussian functions. The probability of the presence of a feature vector in the GMM is defined as:

$$p(x|\lambda) = \sum_{i=1}^{M} p_i \quad b_i(x),$$

where x is a D-dimensional feature vector, $\lambda = \{pi, \mu i, \Sigma i\}$ is the model parameter, pi are the mixture weights for the multivariate Gaussian component densities $bi(x)$, and $\mu i, \Sigma i$ is the mean vector and covariance matrix for the multivariate normal distribution. Covariance matrices are usually considered diagonal to significantly reduce the number of parameters that need to be estimated. These parameters can be trained based on data using the maximum likelihood estimation principle, implemented by the Expectation-Maximization (EM) algorithm. Then, a single mixture Gaussian model is split into two mixture Gaussian models, and its parameters are re-evaluated based on training data using the EM algorithm. This process is repeated until the final desired number of mixtures is reached. An important parameter in GMM is the minimum variance level [8].

CONCLUSION

Thus, the implementation of multi-factor authentication based on biometric data can achieve the following results:

1. Reduction of User Disruption: Many MFA methods increase the time and effort required to log into a system, which can be frustrating for users. However, biometric technologies such as facial recognition with passive liveness detection provide high accuracy with minimal effort. Users can simply take a quick selfie, often automatically and seamlessly. Voice biometrics also offer a contactless and easy authentication process, which can be combined with other methods to enhance security or provide users with options based on the situation. Enterprise-level biometrics, unlike those built into mobile devices, are independent of the phone and can be used as an "ownership" factor, ensuring high security and a passwordless user interface.

2. Enhanced Security: Biometric authentication provides a higher level of security compared to traditional methods such as passwords, which are vulnerable to social engineering. According to PCMag, the number of phishing sites increased by 350% during the COVID-19 pandemic. Hackers use personal data found online or on the black market to reset passwords or deceive contact center agents. For instance, information used to answer security questions, such as place of birth or last known address, is easily accessible. Biometrics, being unique to each user, effectively prevents such attacks. Even if a user is locked out of their account or uses a new device, their biometric data remains a reliable factor for re-authentication.

3. Detection of More Fraud Cases: Passwords can be hacked, and personal data used for authentication are easily found online. Fraudsters use SIM card swapping to intercept one-time passwords. Biometric authentication, secured by liveness detection technology, prevents attacks using recorded or synthesized voices, photos, videos, and masks. Passive facial liveness detection eliminates friction in the user experience, making the authentication process both secure and convenient.

4. Increased Security by Combining Biometric Data: Adding a second biometric method to the authentication process significantly enhances security with minimal user effort. The combination of voice biometrics and facial recognition provides 100 times greater security than using just one method. Merging these technologies makes authentication nearly impenetrable. When combined with the user's device factor, this approach meets the criteria for Strong Customer Authentication (SCA). Security experts recommend using MFA, especially for protecting sensitive data [9].

However, the use of biometrics also comes with specific challenges, including the need to protect biometric data from compromise and ensure the high accuracy of biometric systems. It is important to continue improving technologies and algorithms to effectively counter modern threats and provide a high level of security with minimal inconvenience to users.

REFERENCES

1. How multi-factor authentication using biometric data eliminates fraud. [Electronic resource] Access mode: https://www.idmission.com/en/blog/how-multi-factor-authentication-with-biometrics-eliminates-fraud (accessed 06/25/2024).

2. MFA (Multi-Factor Authentication) Using Biometric Data. [Electronic resource] Access mode: https://www.bayometric.com/mfa-multi-factor-authentication-biometrics / (accessed 06/25/2024).
3. What is Multi-factor Authentication (MFA)? [Electronic resource] Access mode: https://www.wallarm.com/what/what-is-multifactor-authentication-mfa (accessed 06/25/2024).
4. What is: Multi-factor authentication. [Electronic resource] Access mode: https://support.microsoft.com/en-gb/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661 (accessed 06/25/2024).
5. What is Multi-factor Authentication (MFA)? Electronic resource] Access mode: https://www.ibm.com/topics/multi-factor-authentication#:~:text=Multi%2Dfactor%20authentication%20(MFA)%20is%20an,web%20site%2C%20application%20or% 20 network (accessed 06/25/2024).
6. Rassokhin D.K. , Lukaschik E.P. Two-factor biometric authentication system // Caspian Journal: Management and High Technologies. 2021. No.4 (56). pp.66-74.
7. User Authentication Based On MPC Algorithm And Multiple Indexed OTP-Generation Methods. [Electronic resource] Access mode: https://www.researchgate.net/publication/303944875_User_Authentication_Based_On_MFCC_Algorithm_And_Multiple_Indexed_OTP-Generation_Methods (accessed 06/25/2024).
8. Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets. [Electronic resource] Access mode: https://onlinelibrary.wiley.com/doi/10.1155/2013/565183 (accessed 06/25/2024).
9. 5 reasons to use biometric data for multi-factor authentication. [Electronic resource] Access mode: https://www.idrnd.ai/5-reasons-to-make-biometrics-part-of-multi-factor-authentication / (accessed 06/25/2024).

Citation: Asha Seshagiri, "Multi-Factor Authentication Based on Biometric Data", American Research Journal of Computer Science and Information Technology, Vol 7, no. 1, 2024, pp. 42-46.