International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 290-293, October-2023
https://doi.org/10.47001/IRJIET/2023.710037

Biometric Authentication & It's Security Purposes

[1]Prof. S.B.Bele, [2]Sakshi R. Bherde, [3]Atharva U. Wadalkar, [4]Sakshi R. Deshmukh

[1]Assistant Professor, Department of MCA, Vidya Bharati Mahavidyalaya, Amaravati, India
[2,3,4]Student, Department of MCA, Vidya Bharati Mahavidyalaya, Amaravati, India

***Abstract* - Trusted user authentication is becoming an increasingly important function in a web-enabled world. The effect of an unsecure authentication system in a corporate or enterprise environment can be prosperous and can include dropping of confidential information, rejection of service, and compromise of data integrity. The value of trusted user authentication is not limited to computer or network access. Many other applications in daily life also require user authentication, such as banking, e-commerce, and can benefit from physical access control and enhanced security to computer resources.**

Keywords: Biometric, Pattern, Iris, Authentication, Security, Sensors.

1. Introduction

Password less authentication plays an important role in improving this situation. By leveraging the unique physical characteristics of individuals to establish their identity, it provides unparalleled security. It locks sensitive, critical information behind the scenes of your fingerprints, iris patterns, facial features, voice patterns, and behavioral patterns like keystroke dynamics. Biometric systems can be deployed in applications ranging from physical authorization and time attendance systems to mobile devices and online transactions. This compatibility enables organizations to apply tighter security measures across multiple touch points, protecting sensitive data and assets.

2. Applications of Biometric Authentication

A) Lawful Applications

Justice and Law Enforcement: Biometric technology and law enforcement have a long history, and many important variations in identity management have arrives from this beneficial relationship. Biometrics implemented by the police force today is truly multimodal. Fingerprint, face and voice recognition play a unique role in improving public safety and tracking the people we are looking for.

B) Government Applications

Border Control and Airports: A major area of application for biometric technology is at the boundary. Biometric technology helps automate the boundary crossing process. Reliable and automated passenger screening initiatives and automated SAS help simplify the international passenger travel experience while improving the efficiency of government agencies and keeping borders more secure than ever.

C) Health Care Applications

In the healthcare sector, biometrics presents an enhanced model. Medical records are one of the most valuable personal documents; Doctors need to access them quickly and accurately. Lack of privacy and good computing can make the difference between timely and error free detection and health fraud.

D) Commercial Applications

Privacy:

As connectivity spreads across the globe, it's clear that old security methods aren't strong enough to protect what matters most. Fortunately, biometric technology is more accessible than ever, poised to provide added security and convenience for everything from car doors to phone PINs that need to be protected.

Finance:

Biometric technology is widely used in finance to enhance security and convenience. By using unique biometric characteristics like fingerprints, iris, voice, and face, customers can securely access their financial data. These biometric modalities, used alone or in combination, help protect against fraud and ensure that the person accessing the account is the authorized user.

Eyes Movement Applications:

Eye movement tracking applications have various uses in different industries. In the automotive industry, tracking a driver's eye movements can help measure sleepiness or drowsiness. Screen navigation applications use eye tracking to assist people with disabilities in scrolling web pages or performing actions on computers or mobile devices. In aviation, eye and head movement tracking in flight simulators can analyze pilot behavior and serve as a training tool for new pilots.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 290-293, October-2023

https://doi.org/10.47001/IRJIET/2023.710037

E) Screen Navigation

Screen navigation applications that track eye movements are indeed crucial for people with disabilities. By using cameras, these applications enable individuals to scroll web pages, write text, and perform actions on computers or mobile devices simply by clicking on buttons. This technology has been gaining significant attention due to the rapid development and the increasing demand for new methods of screen navigation, particularly on mobile devices platforms. It's exciting to see how this innovation is improving accessibility for individuals with disabilities.

F) Aviation

Flight simulators track the pilot's eye and head movement to analyze their behavior in realistic scenarios. This helps evaluate their performance based on eye movements and other information. It's also a valuable training tool for new pilots, encouraging them to regularly monitor airplane indicators on the primary flight display (PFD). It's fascinating how technology aids in pilot training and enhances aviation safety.

3. Security Needs for Biometric Authentication

According to research papers, security is crucial for biometric authentication due to the following reasons: Non-repudiation: Biometric authentication provides a unique and personal identifier for individuals, making it difficult to deny their actions or presence. Difficult to replicate: Biometric traits, such as fingerprints or iris patterns, are difficult to replicate, making it challenging for unauthorized individuals to gain access. Enhanced protection: Biometric data is stored in encrypted form, adding an extra layer of protection against unauthorized access. Reduced reliance on passwords: Biometric authentication reduces the reliance on traditional passwords, which can be easily forgotten, guessed, or stole.

Continuous authentication: Biometric authentication can provide continuous authentication, ensuring that the authorized user remains present throughout the session. Overall, research emphasizes the importance of security in biometric authentication to protect sensitive data and ensure the integrity of the authentication process.

4. Simple Biometric System Architecture

A) Sensor

The sensor is the first block of the biometric system which gathered all the crucial data for biometrics. It is the interface between the system and the natural world. Basically, it is an image acquisition system, but it also depends on the peculiarity or characteristics required that it has to be restore or not.

B) Pre-Processing

The second block in a biometric system performs pre-processing tasks. Its function is to increase the input and cancel artifacts from the sensor, background noise, etc. It also performs some kind of normalization to prepare the data for further analysis. It is the second block that executes all the pre-rectifying. Its function is to increase the input and to cancel artifacts from the sensor, background noise, etc. It performs some kind of normalization.

C) Feature Extractor

The third step in a biometric system is indeed the most important one. It involves extracting features to identify them later on. The goal of a characteristic extractor is to characterize an object using calculation for recognition.

D) Template Generation

The template generator plays a crucial role in the biometric system. It generates templates using the extracted features for authentication. These templates can be in the form of a vector of numbers or an image with distinct characteristics. They are stored in the database for differentiates and serve as input for similar.

E) Matcher

The matching phase involves using a matcher to compare the acquired template with the stored templates. Various algorithms like Hamming distance are used for this comparison. Once the inputs are matched, the results are generated.

F) Application Device

An application device is a device that utilizes the results of a biometric system. Examples of such devices include the Iris recognition system and facial recognition system. They make use of biometric data for identification and authentication purposes.

5. Research

In biometric authentication, research methodology involves conducting studies to understand and improve the accuracy and reliability of biometric systems. Researchers start by selecting a specific biometric modality, such as fingerprint, iris, or face recognition. They collect a large dataset of biometric samples from individuals to create a training set. Next, researchers develop algorithms and models to extract unique features from the biometric samples. These features are then used to create templates or reference points

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 290-293, October-2023

https://doi.org/10.47001/IRJIET/2023.710037

for each individual. The templates are stored securely in a database.

A) Data overload & accuracy

Data overload and accuracy are important considerations in biometric authentication. When it comes to data overload, it refers to the situation where a large amount of biometric data is collected and processed. This can pose challenges in terms of storage, processing power, and efficiency. It's crucial to strike a balance between collecting enough data for accurate identification and authentication, while also considering the limitations of the system.

In terms of accuracy, biometric authentication systems strive to achieve high levels of precision and reliability. However, it's important to note that no system is perfect and there can be instances of false positives or false negatives. Factors such as environmental conditions, variations in biometric traits, and quality of sensors can impact accuracy. Continuous research and advancements in algorithms and technologies aim to improve the accuracy of biometric authentication systems.

B) How Biometric authentication help in Security purposes

- Biometric authentication enhances security by using unique physical or behavioral traits for identification.
- These traits, such as fingerprints, iris patterns, or facial features, are difficult to replicate, making it harder for unauthorized individuals to gain access.
- Biometric data is more secure than traditional methods like passwords, as it is inherently tied to the individual and cannot be easily forgotten or stolen.

C) Biometric System Architecture

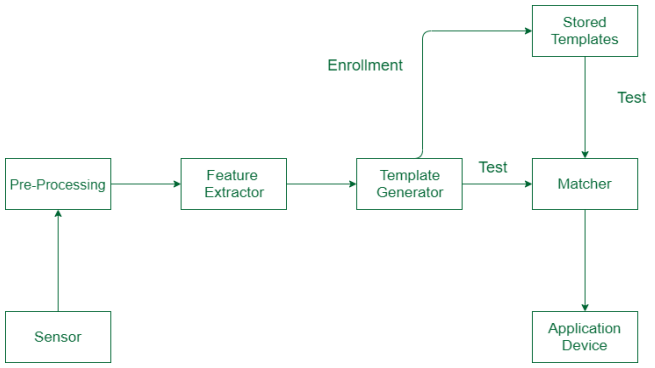

Figure 1: Biometric System Architecture

D) Research Methodology

In biometric authentication, researchers follow a systematic research methodology. They start by selecting a specific biometric modality, like fingerprint or face recognition. Then, they collect a dataset of biometric samples and develop algorithms to extract unique features. These features are used to create templates for each individual. Researchers evaluate the system's performance using testing protocols and metrics like False Acceptance Rate and False Rejection Rate. Statistical analysis is done to analyze the results and improve the system.

E) Discussion

Biometric authentication is a fascinating field that offers secure and convenient ways to verify one's identity. It utilizes unique physical or behavioral characteristics, such as fingerprints, iris patterns, or facial features, to authenticate individuals. This technology has numerous applications, from unlocking smartphones to accessing secure facilities. It provides a higher level of security compared to traditional methods like passwords or PINs, as biometric traits are difficult to forge or replicate. However, it's important to address privacy concerns and ensure that biometric data is securely stored and used ethically. Overall, biometric authentication is an exciting field with promising advancements in enhancing security and user experience.

F) Future Scope

The future scope of biometric authentication looks promising. Advancements in technology will likely lead to more accurate and reliable biometric systems. We can expect improvements in areas such as multi-modal biometrics, where multiple biometric traits are combined for enhanced security. Additionally, research and development will focus on addressing challenges like spoofing attacks and ensuring the privacy and security of biometric data. Biometric authentication will continue to find applications in various industries, such as banking, healthcare, and travel, providing convenient and secure ways to verify identity it's an exciting field with ongoing innovation and potential for widespread adoption.

6. Result

Biometric authentication provides secure and convenient identity verification using unique physical or behavioral characteristics. It offers a higher level of security differentiated to traditional methods like passwords. Advancements in technology continue to improve biometric systems, making them more accurate and reliable. It has various applications in industries such as banking, healthcare, and travel. Overall, biometric authentication has proven to be a successful and effective method of ensuring secure access.

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 290-293, October-2023
https://doi.org/10.47001/IRJIET/2023.710037

7. Conclusion

Biometric authentication is a secure and convenient method of verifying one's identity using unique physical or behavioral characteristics. It offers a higher level of security differentiated to traditional methods like passwords. Advancements in technology continue to improve biometric systems, making them more accurate and reliable. Biometric authentication has found applications in various industries, providing secure access to sensitive information and facilities. It is a promising field with ongoing innovation and potential for widespread adoption.

REFERENCES

[1] https://www.seminarsonly.com/computer%20science/Biometrics%20Based%20Authentication%20Problem.php
[2] https://www.intechopen.com/chapters/65920
[3] https://www.geeksforgeeks.org/what-is-biometrics/
[4] https://www.researchgate.net/publication/46189709_Biometric_Authentication_A_Review
[5] https://link.springer.com/chapter/10.1007/1-84628-064-8_1
[6] https://www.mastercard.com/news/perspectives/2022/brazil-biometric-verification/?cmp=202
[7] https://www.ijert.org/review-paper-on-biometric-authentication
[8] https://www.javatpoint.com/iot-healthcare

Citation of this Article:

Prof. S.B.Bele, Sakshi R. Bherde, Atharva U. Wadalkar, Sakshi R. Deshmukh, "Biometric Authentication & It's Security Purposes" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 10, pp 290-293, October 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.710037

****

