Volume 9, Issue 7, July – 2024
ISSN No:-2456-2165
International Journal of Innovative Science and Research Technology
https://doi.org/10.38124/ijisrt/IJISRT24JUL541

Biometrics and Password Less Authentication: The Future of Digital Security

Rajesh Kumar
Cyber Security Professional, USA

Abstract:- Passwords and other old authentication mechanisms are becoming less secure as cybersecurity threats continue to change. By utilizing distinctive physical or behavioral characteristics to confirm the identification of anyone gaining access to sensitive data or systems, biometric authentication is a viable alternative (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). The purpose of this article is to investigate how biometric authentication might improve cybersecurity. It emphasizes the benefits of biometrics, such as their better user experience, multi-factor authentication capabilities, and uniqueness and non-replicability (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). Concerns and restrictions, including possible vulnerabilities and privacy issues, are also covered in the article. It also covers important factors to consider while implementing biometric authentication, such as safe processing and storage of biometric data (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). Biometrics are essential for bolstering cybersecurity and reducing the dangers connected with password-related issues since they offer a dependable and secure means of user verification.

All things considered, biometric authentication provides a reliable and practical way to confirm user identities, strengthening an organization's security posture and shielding confidential data from unwanted access.

Keywords:- *Password, Authentication Mechanisms, Cyber Security Threats, Biometric Authentication, Vulnerability.*

I. INTRODUCTION

Strong and dependable authentication techniques are now essential in the digital era, as cybersecurity threats are ever-changing (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). There are several intrinsic problems with traditional password-based authentication techniques, including weak passwords, forgotten credentials, and vulnerability to hackers. Password less authentication techniques and biometric authentication have come to light as viable solutions to these problems (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). The measurement and examination of an individual's distinctive physical or behavioral traits is referred to as biometrics. These characteristics—including fingerprints, facial features, iris patterns, voice patterns, or even behavioral patterns like typing rhythm—are difficult to mimic or counterfeit due to their uniqueness (Weaver, 2006). Businesses can highly accurately confirm users' identities by using biometric authentication.

The idea of password less authentication is to completely do away with the need for passwords. Rather than committing complicated passwords to memory, users can verify themselves via hardware tokens, biometrics, or one-time codes, among other validating criteria (Weaver, 2006). In addition to increasing security, password less authentication makes user authentication easier, which boosts usability all around (Weaver, 2006). The great degree of precision and security that biometric authentication offers is its main advantage. Because biometric characteristics are exclusive to each person, it is very difficult for someone not permitted to access (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). Furthermore, by removing the need to memorize and enter passwords, biometric authentication techniques improve user experience and lower the possibility of weak or reused credentials.

Biometric authentication can provide multi-factor authentication in addition to bettering the user experience. The security of the authentication process is further enhanced by integrating biometrics with additional authentication elements like hardware tokens or cryptographic keys (Weaver, 2006) (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). Because an attacker would have to compromise many factors to get past the authentication barriers, the danger of unauthorized access is greatly decreased by using a multi-factor authentication system.

In conclusion, biometric authentication, and password less authentication offer significant improvements over traditional password-based methods. By combining convenience, strong security, and usability, these authentication approaches pave the way for a more efficient and reliable digital authentication landscape.

II. DIFFERENT BIOMETRIC TECHNIQUES AND TECHNOLOGIES

As we've already mentioned, there are two types of biometric traits. Thus, based on these traits, biometric authentication mechanisms have been devised.

Below is a discussion of the specifics of some methods.

- *Fingerprint Technology:*

The ridges and valleys left on the finger's surface are what make up a fingerprint. The conventional technique imprints a fingerprint on paper using ink. After then, a

conventional scanner is used to scan this piece of paper. Live fingers print readers are being employed in recent approaches (Gayathri, Malathy, & Prabhakaran, 2020). These are founded on concepts related to optics, heat, silicon, or ultrasonics. Among all the biometric procedures, it is the most ancient. Currently, the most often used type is an optical fingerprint reader (Gayathri, Malathy, & Prabhakaran, 2020) (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). They are predicated on variations in reflection at the locations where the reader surface is touched by finger papillary lines. Every optical fingerprint reader is made up of a light source, a light sensor, and a unique reflection surface that modifies the reflection.

An optical finger measures around 10*10*15 (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). Reducing them further is challenging since the reader must consider the light sensor and light-reflecting surface.

Fig 1: Fingerprint Template (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009).

The finger's capacitance serves as the basis for the optical silicon fingerprint sensor. A silicon chip with rectangular arrays of capacitors on it makes up the DC-capacitive fingerprint sensor. The fingerprint on one capacitor plate resembles a finger, while the other plate has a small region of metallization on the chip surfaces (Gayathri, Malathy, & Prabhakaran, 2020). When the finger is pressed against a chip's surface, the fingerprint ridges are adjacent to the neighboring pixels and have a high capacitance to them. Because the valleys are farther away from the closest pixels, their capacitance is smaller.

The newest and least prevalent fingerprint type is ultrasound. When a user lays their finger on a piece of glass, an ultrasonic sensor moves and scans the whole fingerprint (Gayathri, Malathy, & Prabhakaran, 2020). This technique is used to monitor the surfaces of the figures. It takes a moment or two to do this.

Techniques for matching fingerprints fall into two groups. One relies on minutiae, while the other relies on correlation. Techniques based on minutiae first identify the minutiae points, after which they map their relative locations on the finger (Gayathri, Malathy, & Prabhakaran, 2020). The exact placement of a registration point is necessary for correlation-based approaches, which are impacted by picture translation and rotation.

➢ *Face Recognition Technology:*

Unique facial characteristics, such as the relative locations of the lips, nose, and eyes, are used by facial biometrics to identify people. It is used in user authentication on mobile devices, security systems, and surveillance (Li, 2020) (Gayathri, Malathy, & Prabhakaran, 2020). The first method is the Facial metric method. Facial metric technology is dependent on the production of facial characteristics, as seen in figure 2. Typically, the system looks for the positions of the mouth, nose, and eyes as well as the separations between these features. The area of the face is resized to a predetermined set size (e.g. 149-99 points) (Li, 2020). The canonical picture is this facial image that has been standardized. Following that, a face template is created, and the facial metrics are calculated. These templates typically range in size from 3 to 5 KB, while some systems have templates as little as 96 bytes (Li, 2020).

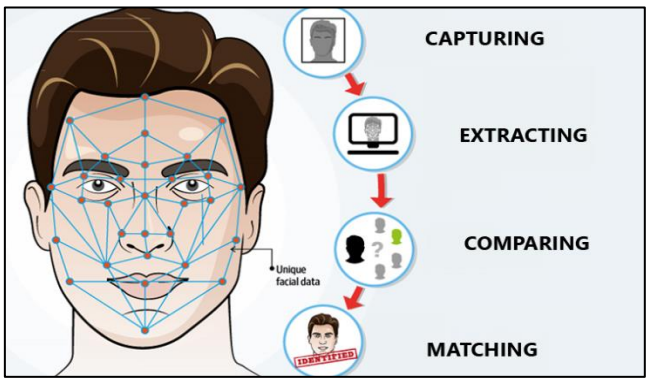

Fig 2 Recognition of Facial Characteristics (Starlink, 2023)

The second method is the Eigen face approach. The Eigen face approach is based on representation learning, in which a face image is represented as a linear combination of fundamental images called eigenfaces (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). Eigenfaces are the statistical distribution of face images in a dataset represented by the eigenvectors of a covariance matrix.

➢ *IRIS Technology:*

The iris, or colored region surrounding the pupil's eye, is used in this identifying technique. Iris patterns are distinct and may be captured using an image acquisition technology that is based on video (Patel, Trivedi, & Patel, 2012). Every iris structure has an intricate pattern. A mix of distinct features including corona, crypts, filaments, freckles, pits, furrows, striations, and rings may be present. Figure 3 shows an IRIS image. A specialized grayscale camera is used to capture the iris pattern at 10–40 cm from the camera (Patel, Trivedi, & Patel, 2012). The program looks for the iris in the grayscale picture of the eye after it has been collected. The program covers the iris with a net of curves if an iris is detected. The program generates iris code based on point-to-line darkness (Patel, Trivedi, & Patel, 2012). Two influences need to be considered in this situation. First, since the lighting situation affects the total darkness of the image, the darkness threshold—which determines whether a specific location is bright or dark—must be dynamically calculated based on the overall darkness of the picture (Patel, Trivedi, & Patel, 2012).

In the decision process, the matching software takes two iris codes and computes the hamming distance based on the number of different bits. The hamming distance score is calculated and compared with a security threshold to determine if the iris codes are the same (Patel, Trivedi, & Patel, 2012). Computing hamming distance of iris codes is quick, just counting exclusive OR bits.

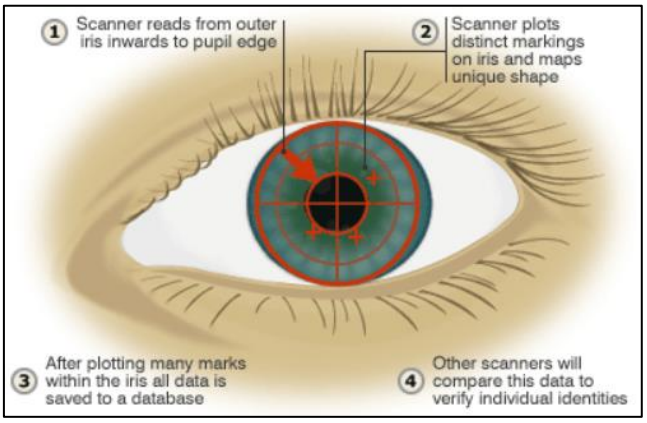

Fig 3 Image of IRIS (Vks, (n.d))

We can also apply the concept of template matching in this technique, which involves comparing a stored iris template with a produced one using statistical calculations (Patel et al., 2012).

➢ *Technologies Related to Hand Geometry:*

The estimate of the hand's length, breadth, thickness, and surface area is one of these procedures. There are several ways to measure hands, including mechanical and optical principles (Boreki & Zimmer, 2005). The optical scanners are divided into two subcategories. Devices in the first category produce a bitmap picture of the hand in black and white. A black and white camera and a light source could be used to do this with ease. The computer program processes the bitmap picture. In this instance, only 2D hand characteristics are applicable. Systems of hand geometry in other categories are more intricate (Boreki & Zimmer, 2005). They feature two (vertical and horizontal) sensors for measuring the contour of the hand and employ certain guiding markings to section the hand more effectively. Thus, all 3D feature data is handled by sensors in this category (Boreki & Zimmer, 2005). In Figures 4, the hand geometry system is displayed.

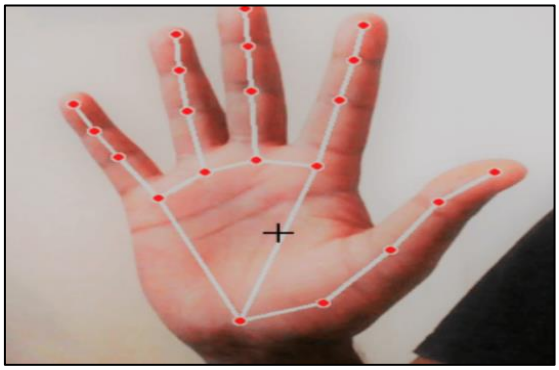
Fig 4 Taking Image of the hand (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009).

A few hand geometry scanners solely generate a video signal that shows the form of the hand. The necessary video or picture of the hand is subsequently obtained by digitalizing and processing those signals in the computer.

➢ *Behavioral Biometrics:*

The study and assessment of a person's distinctive behavioral characteristics to confirm their identification or spot questionable activities is known as behavioral biometrics (Alsaadi, 2021). A variety of behaviors, including keystroke patterns, mouse movements, touchscreen gestures, voice patterns, and even walking or gait analysis, can be included in behavioral biometrics. These actions are thought to be particular to each person and can serve as biometric markers. Organizations can develop a thorough profile of a person's behavior over time by consistently observing and evaluating these behavioral patterns (Alsaadi, 2021). When the user interacts with a system or device, this profile can be utilized to authenticate them in real time.

Behavioral biometrics has several benefits, such as continuous authentication, which makes the user experience more secure and seamless, and non-intrusiveness due to its reliance on non-physical attributes (Alsaadi, 2021). It can be used to strengthen security protocols and expedite user identification and verification procedures in a variety of industries, such as banking, cybersecurity, and fraud prevention.

III. OTHER TECHNIQUES

Some different techniques for biometric authentication that are used vaguely are listed below.

➢ *DNA:*

Currently, DNA sampling is somewhat invasive and needs a sample of tissue, blood, or another bodily fluid. This capturing technique still needs to be improved. Currently, DNA analysis lacks the necessary automation to be classified as a biometric technology (Dharavath, 2013). It is now feasible to analyze human DNA in ten minutes. It might become increasingly important as soon as technology develops to the point where DNA can be matched automatically in real time (Dharavath, 2013). Since biometric systems DNA are already widely used in crime detection, they will continue to be used in law enforcement for the foreseeable future.

➢ *Thermal imaging:*

The vein geometry of the hand is comparable to this technology. Moreover, it creates an image of the vein pattern in the wrist or face using a camera and an infrared light source (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009).

➢ *Ear Shape:*

When earmarks are discovered at crime scenes, law enforcement uses the ear shape to identify individuals (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). It remains to be seen if this technology will advance to access control applications. The Octophone is an ear shape verifier

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL541

made by ART Techniques, a French firm. It's a phone-style device with two cameras that take pictures of the ear and a lighting unit within.

- *Body Odor:*

The idea behind body odor biometrics is that almost every human scent is distinct. Sensors that can detect odors from non-intrusive body parts, like the back of the hand, are used to detect the scent. Mastiff Electronic Systems is investigating ways to record a person's scent. Volatiles are molecules that give each human scent its unique composition (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). The system pulls them out and turns them into a template. Because body odor contains a great deal of sensitive personal data, using body odor sensors raises privacy concerns. By examining the body odor, certain illnesses, or behaviors from the previous few hours (such as sex, for example) might be identified.

- *Identification of Veins:*

Using near-infrared light to scan and analyze the vein patterns in a person's fingers or palms, vein recognition technology verifies an individual's identity (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). It is used in financial transactions and access control.

IV. BIOMETRIC SYSTEM PERFORMANCE

Numerous measures are used to evaluate a biometric system's performance in terms of how well it can reliably identify or verify persons. The following are some essential performance indicators for assessing biometric systems.

- *Rate of False Acceptance (FAR):*

The false acceptance rate (FAR) is the likelihood that a biometric system may mistakenly accept an unauthorized person or imposter. Higher security is indicated by a lower FAR (Wayman, 2005).

FAR = (False Accepts / Total Imposter Attempts) × 100%

- *Rate of False Rejection (FRR):*

FRR calculates the likelihood that a biometric system may mistakenly deny access to a legitimate or authorized person (Wayman, 2005). Usability is higher when the FRR is lower.

FRR = (False Rejects / Total Genuine Attempts) × 100%

- *EER, or equal error rate:*

When the FAR and FRR are equal, there is an equal chance of false acceptance and rejection, which is known as the EER (Wayman, 2005). A system that is more accurate and balanced has a lower EER.

- *The Curve of Receiver Operating Characteristic (ROC):*

A graphical representation of the relationship between the FAR and FRR at various threshold levels is called a ROC curve. It aids in evaluating the trade-off between a biometric system's usability and security (Wayman, 2005).

- *True Acceptance Rate (TAR), also known as Genuine Acceptance Rate (GAR):*

The system's capacity to accurately accept legitimate or authorized users is indicated by GAR or TAR (Wayman, 2005). A system with a higher GAR/TAR is more accurate.

- *Failure to Enroll (FTE):*

The term FTE describes the system's incapacity to accurately register or enroll legitimate users (Wayman, 2005). A higher FTE suggests that the system is having trouble gathering precise biometric information.

FTE = (Failed Enrollments / Total Enrollments) × 100%

- *FTC, or Failure to Capture:*

FTC indicates that the biometric data needed for recognition or verification cannot be captured by the system. An increased FTC indicates usability issues or technical constraints (Wayman, 2005).

FTC = (Failed Captures / Total Authentication Attempts) × 100%

- *Template protection:*

The greatest quantity of data sets that may be entered into the system is its definition (Wayman, 2005).

V. CONSIDERATIONS FOR ADOPTING BIOMETRIC AUTHENTICATION

Before adopting biometric or password less authentication, organizations should assess their security and compliance requirements (Pooe & Labuschagne, 2011). Ensure that the chosen authentication methods meet industry standards and regulatory guidelines. Conduct a thorough risk assessment to identify potential security risks and vulnerabilities associated with biometric or password less authentication (Pooe & Labuschagne, 2011). Develop mitigation strategies to address these risks effectively. Pilot testing should be done to confirm the functionality and efficacy of biometric or password less authentication techniques in real-world scenarios prior to full-scale deployment. To address any problems or concerns, get user input (Pooe & Labuschagne, 2011). To increase security even further, think about combining biometric or password less techniques with multi-factor authentication (MFA) (Pooe & Labuschagne, 2011). MFA gives consumers flexibility while also enhancing security.

By addressing concerns, overcoming challenges, and following best practices, organizations can successfully adopt and implement biometric and password less authentication.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL541

VI. FUTURE OF BIOMETRIC AUTHENTICATION

In the USA, biometric authentication has a bright future in cybersecurity as long as improved security protocols are prioritized and widely implemented. Because of their accuracy and practicality, biometric authentication techniques like fingerprint, face, and iris scanning are being used more and more in a variety of industries (Dharavath, 2013). One important aspect of the future of biometric authentication in the USA is the emphasis on privacy and data protection. As biometric data involves sensitive personal information, there is a growing need to ensure the secure storage, handling, and transmission of this data (Dharavath, 2013). The development of robust encryption methods and secure storage practices will be crucial to safeguarding biometric information. Moreover, biometric authentication is expected to play a significant role in securing critical infrastructures and government systems in the USA (Dharavath, 2013). Biometrics can provide a strong and reliable means of verifying identities and protecting against unauthorized access in sensitive environments (Dharavath, 2013). Additionally, the continued advancement of machine learning and artificial intelligence technologies will enhance the efficiency and accuracy of biometric authentication systems in the USA. These technologies enable continuous learning and adaptation to different user behaviors and environmental changes, improving overall system performance (Dharavath, 2013).

In conclusion, the future of biometric authentication in cybersecurity in the USA involves the integration of biometrics into existing security frameworks, a focus on privacy and data protection, the use of biometrics in critical infrastructures and government systems, and advancements in machine learning and artificial intelligence technologies.

VII. CONCLUSION

Biometric authentication is far from a flawless solution, even if it can provide a high level of security. Rather than relying solely on the incorporation of biometrics in one form or another, strong system engineering principles are still necessary to guarantee a high degree of security.

The distributed database of biometrics used in security applications is highly vulnerable to compromise, especially when it comes to individual privacy and, consequently, non-repudiation and irrevocability. With proper implementation of biometric infrastructure, it is possible to eliminate the requirement for such remote databases without sacrificing security.

Legislation will be needed to mitigate the effects of biometric technology on society, as well as the threats to identity and privacy. For most of the brief history of biometrics, technological advancements have surpassed moral or legal ones. A broader and more thorough examination of the significance of biometric data and the legal protections that should be in place for it is now necessary.

REFERENCES

[1]. Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

[2]. Weaver, A. C. (2006). Biometric authentication. Computer, 39(2), 96-97.

[3]. Gayathri, M., Malathy, C., & Prabhakaran, M. (2020). A review of various biometric techniques, their features, methods, security issues and application areas. Computational Vision and Bio-Inspired Computing: ICCVBIC 2019, 931-941.

[4]. Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. IEEE access, 8, 139110-139120.

[5]. Patel, C. D., Trivedi, S., & Patel, S. (2012). Biometrics in IRIS technology: A survey. International Journal of Scientific and Research Publications, 2(1), 1-5.

[6]. Boreki, G., & Zimmer, A. (2005, October). Hand geometry: a new approach for feature extraction. In Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05) (pp. 149-154). IEEE.

[7]. Alsaadi, I. M. (2021). Study on most popular behavioral biometrics, advantages, disadvantages, and recent applications: A review. Int. J. Sci. Technol. Res, 10(1).

[8]. Dharavath, K., Talukdar, F. A., & Laskar, R. H. (2013, December). Study on biometric authentication systems, challenges, and future trends: A review. In 2013 IEEE international conference on computational intelligence and computing research (pp. 1-7). IEEE.

[9]. Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2005). Biometric systems: Technology, design, and performance evaluation. Springer Science & Business Media.

[10]. Pooe, A., & Labuschagne, L. (2011). Factors impacting on the adoption of biometric technology by South African banks: An empirical investigation. Southern African Business Review, 15(1).

[11]. Starlink, & Starlink. (2023, November 7). Biometric Face Recognition System: Benefits, Uses, & How does it Work? - StarLink India. *StarLink India* -. https://www.starlinkindia.com/blog/biometrics-face-recognition/

[12]. Vks, S. A. (n.d.). An introduction to retinal scanning and iris scanning. https://www.divilabs.com/2013/04/an-introduction-to-retinal-scanning-and.html