VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2024, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 12, Number 1, January-March 2024 *pp:105-120*

Towards Secure Identification: A Comparative Analysis of Biometric Authentication Techniques

Warda Hassan [1]* **and Nosheen Sabahat** [1]

[1]Department of Computer Science, Forman Christian College University, Lahore Pakistan

Keywords: *biometric, authentication, password, fingerprints, signature verification*

Journal Info:
Submitted:
February 20, 2024
Accepted:
March 25, 2024
Published:
March 31, 2024

Abstract

This paper provides an overview and analysis of existing biometric authentication methods. Biometric authentication enhances the security of traditional authentication methods by utilizing unique biological characteristics of individuals, such as fingerprints, facial features, or iris patterns, to verify identity. However, implementing biometric authentication may involve initial setup costs for service providers due to the need for specialized hardware and software. Additionally, users may experience some initial inconvenience during the enrollment process to register their biometric data. This paper presents a comparative analysis of the usability of biometric authentication techniques. Initially, a survey of existing work is conducted by comparing techniques, algorithms, and metrics used in research. Later the challenges of the distinct types of authentication techniques are discussed, and their problems are discovered. Subsequently, the findings of a quantitative study based on a are presented, aimed at assessing the usability of those techniques. The findings indicate that authentic biometric techniques are perceived as usable.

***Correspondence author email address:** 243041087@formanite.fccollege.edu.pk
DOI: 10.21015/vtse.v12i1.1745

1 Introduction

In this digital age, finding safe and trustworthy identification techniques is more important than ever, where protecting personal data is important. Utilizing distinctive biological characteristics like fingerprints, iris patterns, or facial features, biometric authentication presents a viable way to improve convenience and security in access control systems. But even with the widespread use of biometric technologies, protecting against fraud and unwanted access continues to be a difficult task. Web authentication commonly uses passwords but that compromises security and user experience because vulnerabilities still exist despite initiatives such as password-less methods and federated authentication [1, 2]. A viable way to get around these restrictions is multi-factor authentication, which takes knowledge, possession, and inherence into account. The move to multi-factor authentication is a component of a larger initiative to improve security protocols and overcome the drawbacks of

conventional password-based systems [2].

Strong security protocols need to be implemented if we need to prevent unauthorized access to systems such as access control procedures and authentication requirements like biometric authentication (fingerprints or palm prints) because that provides a higher level of security. The security risks are constantly evolving, which is why we need to ensure that our biometric authentication techniques are continuously improving and enhancing [3].

Passwords, tokens, and verifications rely on comparing an input to a pre-existing saved document to recognize the identity of a person. Biometric authentication, on the other hand, relies on distinctive physiological or behavioral characteristics such as fingerprint patterns or keystroke patterns, which means that the biometrics of a person cannot be borrowed or stolen. The efficacy of biometrics is dependent on application and attack resistance. To assess the effectiveness, advantages, and disadvantages of various biometric authentication techniques and make well-informed decisions about the implementation of strong security measures, a comparative study is essential [4]. Comparative studies such as these are important as they not only compare different biometric authentication techniques but also discuss the problems that they are facing and the reasons behind them.

This paper aims to provide significant insights into the practical effectiveness of biometric authentication methods. This will help inform the system developers and the decision-makers about the advantages, drawbacks, and best practices associated with biometric authentication technologies by discussing and evaluating real implementations across a variety of use cases. The findings of this study will help with security and usability, and it will encourage more people to start using biometric authentication methods in the digital world.

The rest of the paper is structured as follows. The following section describes the literature review. Sections III and IV present the comparison of existing works and the challenges faced by the authentication methods. Section V presents a case study and finally, section VI concludes the paper.

2 Literature Review

Unauthorized access to a machine refers to the action of entering or gaining access to a system or a machine, whether it is physical or electronic, without the explicit consent of the owner or administrator. A. A. Kaur et al. [5] have contributed a lot of work to this field; they say unauthorized access to machines is still an issue despite security provided by authentication methods such as Knowledge-Based Authentication, Object-Based Authentication, and Characteristics-based Authentication.

Knowledge-based authentication is a type of authentication in which only the identified user would know such as user IDs and passwords, passphrases, and PINs [6]. Object-based authentication makes use of any physical personal effects of a person such as identity cards or smart cards that are used in banking or hotels [5]. Characteristic-based Authentication, also known as the Biometric Authentication Technique, can also be further divided into two distinct fields, Physiological Characteristics, and Behavioral Characteristics [4].

A. A. Kaur et al. [5] suggest that these authentication methods are vulnerable to attacks. Password-based authentication faces usability challenges and they struggle to keep up with technical advancements. These issues require to be addressed in a user-centered design approach and intelligence-driven security models. Password security is a primary concern because of weak passwords, memory limitations, and various threats such as database leaks, phishing, and keylogging. Solutions include dynamic password policies, password meters, managers, generators, two-factor authentication, or moving to biometric authentication systems such as keystroke dynamics. Password-based authentication is categorized into User Centric and Machine Centric approaches, with enhancements needed in both areas to improve efficiency and effectiveness. Understanding these protocols is important for enhancing authentication security while overcoming usability challenges [5, 7, 8].

In another paper discussed by K. Papadamou et al. [1], a new web authentication system has also been introduced, that suggests privacy and security

are better than traditional password-based methods. They suggest that a federated device-centric authentication architecture, featuring Identity Consolidator and Behavioral Authentication Authority, improves security, privacy, and user experience. The architecture supports various authentication methods, including biometrics, and prioritizes attribute-based access control. The proposed architecture is user-friendly and privacy-focused, suitable for both end users and service providers.

Two-factor authentication is mostly used for increasing website security and protecting data. Improving the two-factor authentication user experience can motivate visitors to use this authentication method because having more registered users reduces the risk of security breaches. However, it is not given much importance [9]. A lot of research has been done on Two-factor authentication. S. Das et al. [10] discuss that there are a lot of hurdles for older adults when they are trying to adopt two-factor authentication, regardless of its well-known security benefits. Through qualitative research involving ten participants aged sixty and above, the research uncovers various obstacles like design constraints, unclear benefits, and inconsistent guidance. The study proposes a solution for older adults that includes assistance and communication strategies to encourage older adults to start using two-factor authentication. Furthermore, they are trying to make user-friendly security tools to protect older adults from online threats such as phishing and are proposing to add easy-to-follow instructions and guides for these adults to help them effectively embrace and utilize security tools and uphold their digital independence.

The development of authentication techniques, with a significance on multifactor authentication and password-less authentication, has been discussed in another paper by I. Gordin et al. [11]. The usability challenges of multifactor authentication are discussed in detail; however, it is noted that multifactor authentication is acknowledged for its security enhancements. This paper also mentions that eliminating passwords and using biometric identifiers, such as fingerprint authentication and facial recognition, is not only more convenient but also more secure. The paper also suggests that we should explore alternative biometric solutions for future research.

Biometrics are essential in authentication; they could be physiological like fingerprints and facial features or behavioral traits like gait or signature recognition. They are commonly used in network logins and are often combined with smart cards for security purposes. Research conducted by S. Z. Syed Idrus et al. [12] underscores the significance of biometric authentication in addressing hacking threats and proposes enhancing password systems with graphical passwords for improved security measures.

V. Veeraiah et al. [13] discuss the security measures required due to the growing popularity of virtual worlds. Virtual user identification is achieved through behavioral biometric systems; however, their development is impeded by limited collaboration and computational limitations. Traditional passwords can be replaced with biometric systems, which provide secure identification based on distinct physical or behavioral traits. But biometrics have their problems as well. The future of online communication is embodied in the 3D virtual world known as the Meta-verse, which facilitates real-world social and economic interactions. The goal of the study they conducted was to improve security in the Metaverse by using precise and effective biometric systems that provide options and flexibility for practical implementation.

In another paper discussed by S. Abdulrahman et al. [14], it is discussed that biometrics is an identification technique, that makes use of observable behavioral or physiological characteristics. It was first used in antiquity and has two modes of operation: enrolment and authentication. Because of their many uses, biometric systems are widely accepted even though they are not a hundred percent accurate. To increase accuracy and performance, multimodal biometric systems that combine several biometric sources are recommended in the paper. They suggest that more research is necessary for certain techniques and feature extraction methods for better comprehension and implementation.

A person can be recognized and verified using

identifiable, verifiable, specific, and unique data with the use of biometrics [15]. V. Liskin et al. [16] has conducted research in the use of biometrics, and they discuss that biometric data is used to identify and authenticate people by using their unique characteristics. This is done by taking the user's characteristics as input and matching them with the stored data of the user's biometric data to detect similarities. If similarities are found, then the person is identified, otherwise, not. Biometric data is not always uniform as people change, for instance on the face, facial hair could be grown, for eyes, glasses or lenses could be worn, etc. To improve and evaluate the biometric data, certain methods and algorithms are applied on the data to improve the technique. The types of data that we collect depend on the application, for example, web applications, secure facilities, or mobile access.

V. Liskin et al. [16] discuss using biometrics to confirm a person's identity. They divide these traits into two types: biometric traits (like face, fingerprints, and hand shape) and behavioral traits (like how a person types or voice of a person). Each type has its advantages and disadvantages. For instance, face recognition uses pictures, fingerprint recognition looks at patterns, and hand recognition uses how your hand looks. They also study how to make fingerprint recognition better, looking at techniques like ridges and filters. Devices like fingerprint scanners and face scanners are important for logging into networks. They also look at how people type to make sure it is them logging in, using special techniques to check how keys are pressed 4,3,16.

A lot of research has been done in this area, but to the best of our knowledge, a thorough comparison of biometric authentication methods cannot be found. This paper will be helpful for the researchers as it lists all the problems, metrics, pros, and cons of biometric authentication methods.

3 Comparison of Existing Work

In research on Biometric Authentication Methods, it is essential to discuss existing work as it provides context, helps with identifying gaps in the existing literature, and allows for comparison. By reviewing previous studies, areas where further research is needed can be identified and existing methods that may be lacking can be recognized. Comparing findings and methodologies of research with existing studies can evaluate the differences and contributions of work. Building on prior knowledge in the field of biometric authentication methods is also beneficial. Discussing existing work in a research paper provides a foundation for study and identifies gaps and opportunities for further research. Table 1 shows a summary of existing research papers.

A. A. Kaur et al. [5] examined around five hundred research papers to create six research questions that they answered, offering valuable perspectives on the current problems and their potential solutions. The study highlights the significance of addressing both technical and user-centric issues, presents its findings, and suggests future research directions. The results emphasize the necessity of efficient password authentication methods. The advantages of password authentication methods mentioned in the paper are maintaining the memorability of passwords through the use of hash functions to secure passwords against brute force attacks. The paper also indicated that these techniques could help in saving computation time and resources, but they also have some disadvantages. The authors also suggested that passwords require supervision, and it may be difficult to necessitate with the complicated password rules. The paper highlights the difficulty in designing password authentication methods that maintain a balance between security and usability.

E. D. Cristofaro et al. [2] used a qualitative research methodology to understand the point of view of users regarding two-factor authentication. They used social media, mailing lists, and questionnaires to select nine participants. One-on-one interviews were conducted to learn about their preferences, issues, problems, and motivations. Their study indicates that two-factor authentication is a user-friendly solution that can be used on smartphone apps, one-time codes, and PINs. The study aims to look for the advantages of two-factor authentication in terms of usability, trustworthiness, and user experience. Two-factor authentication adds an

extra layer of security, which decreases the possibility of unwanted access and compromising credentials. This can be achieved by requiring users to provide two forms of authentication.

N. Yusuf et al. [3] reviewed passwords and fingerprint authentication methods by prioritizing challenges, strategies, and research findings through a literature review. They worked on improving fingerprint image quality and data encryption while trying to employ fingerprint technology in smartphones, online attendance systems, and mobile apps. They also discussed password authentication methods such as one-time passwords, smart cards, automatic password generation and resolving password leakage issues to prevent unwanted access. They considered that by improving image quality and addressing low-quality fingerprints through graphic password techniques like Hopfield neural network and ridges feature authentication, security against hackers could be increased. However, they also suggested that these techniques come with other problems such as shape memory and usability problems, they also may not be appropriate for large data sets. They discussed that even though fake fingerprints can be very difficult to identify even if complex mechanisms are used, deep neural networks and other fingerprint authentication techniques can have impulse noise and may take a longer time to implement.

F. Ennaama et al. [17] conducted a comparative analysis of various biometric systems, such as fingerprint, iris, face, voice, signature, keystroke dynamics, and retinal recognition. They discussed several factors such as universality, uniqueness, permanence, intrusiveness, effort, cost, and dependability. The performance of each benchmark was compared and the most fascinating and widely used biometric system available was also discussed in the paper. They analyzed that biometric systems have a lot of potential including user acceptance, simplicity, security, and dependability. They conferred that face recognition is non-intrusive, fingerprints are very reliable, iris recognition offers high security and signature recognition is used in transactions. However, there are disadvantages of biometric systems as well, they are very costly, there are a lot of privacy issues and user effort. Even though there are a lot of benefits of biometrics, they suggested that due to privacy concerns and direct physical contact with sensors, we may never switch to biometrics completely.

S. Parusheva [18] discussed the biometric features for online banking authentication systems methodologically using Quantitative research. They evaluated hand geometry, voice, iris, and fingerprint using a two-step evaluation process that involves acceptability, performance, resistance to circumvention, and universality. Scoring systems and numerical metrics were applied to provide a qualitative assessment to identify the best biometric features for online banking system integration. They suggested that biometric authentication offers quantitative assessment, feature selection, and compatibility with two-factor authentication for online banking. They have compared multiple biometric authenticators using a systematic assessment method and the results indicate that face, iris, fingerprints, and DNA are the most appropriate biometric authentication methods in banking, they increase security and dependability.

N. Bawany et al. [19] used interviews, questionnaires and experiments to conduct a study using four age groups, under 20, over 20 and under 30, over 30 and under 40, and over 40 that were split into these categories to separate the results for younger and older adults while discussing the most common biometric authentication techniques. They examined that biometric authentication offers benefits like increased security, less password burden, user comfort, ease of use, and better error recovery and learnability. Users found fingerprint and facial scanning to be less intrusive and time-consuming. The paper also indicated that biometric authentication improves security and reduces the possibility of brute-force attacks for passwords. Nevertheless, they also discussed the problems that older adults have to face when it comes to biometric authentication, the need for complicated passwords, hesitation, and user preference for conventional methods to prevent widespread adoption.

Table 1. Summary of Existing Work

Author	Methodology	Technique	Pros	Cons
A. A. Kaur et al. [5]	Literature Review	Password Authentication Methods	Memorability Resistance to brute force attacks Efficiency and user approach	Usability concerns Guidance Security and Rules
E. D. Cristofaro et al. [2]	Qualitative Research	Two Factor Authentication	Usability Trustworthiness Enhanced Security	Not applicable
N. Yusuf et al. [3]	Literature Review	Password and Fingerprint Authentication	Effective against hackers Better accuracy	Shape-recollection issues Unsuitable for large data sets Not Diverse Time-consuming
F. Ennaama et al. [17]	Comparative analysis	Biometric Systems	Reliability Security Ease of implementation Acceptance by users	Intrusiveness Privacy concerns Cost User effort
S.Parusheva [18]	Quantitative Research	Biometric authentication	Identification of suitable biometric feature Elimination of Unsuitable Biometric Features	Not applicable
N.Bawany et al. [19]	Experiments, questionnaires and interviews	Common Biometric Authentication Techniques	Time-saving Ease of use Reduced password burden Enhanced Security	Hesitation and Fear Age-related challenges Preference for traditional authentication methods

4 Challenges of Authentication Methods

Two main types of authentication techniques are discussed in this section, knowledge-based and characteristic-based authentication techniques. Characteristics-based authentication techniques are further split into two sections, physiological techniques, and behavioral techniques. Physiological biometrics is the study of a person's static physical traits such as face, iris, fingerprint, etc. These traits are generally static because they remain the same after a certain age, but they may change due to some factors. Behavioral patterns on the other hand involve studying the patterns of human activity such as their gait or keystroke pattern [20]. Figure 1 shows various authentication techniques.

Authentication methods are vital in today's modern age for accessing computers, websites, software, or even the Internet of Things. The most widespread solutions used until now are simple usernames and passwords [12], other methods include PIN codes at Automated Teller Machines and Biometric Scans at Government Facilities. Passwords, even though used mostly due to how easy they are, lack security. A good authentication system must balance security, usability, acceptance, and cost. Various knowledge-based and biologically based authentication techniques are discussed in Table II, illustrating where they are deployable, what problems arise in each of the techniques, and the reason for those complications.

1) A **Password** is a collection of characters put together by a user, whether meaningful or not, which is used to prove a person's identity. Figure 2 shows the difference between a meaningful and a non-meaningful password.

Passwords are usually used in websites, computer systems, and software. It can be system generated, which is typically stronger, as they are not meaningful, making them harder to guess for hackers and eavesdroppers to gain access to the system. Some of the challenges faced by passwords are listed below:

- Passwords are vulnerable to guessing attacks [3, 12] because people tend to keep easier passwords so that they can remember them instead of keeping difficult passwords.
- Passwords can easily be revealed by a user to another user because the password policies are usually poor, a person may easily give their credentials to someone else for use without the risk of penalties.
- Most users reuse their passwords [3] because it is easier for a user to memorize one password for multiple websites, rather than multiple passwords.

2) A **Passphrase** is remarkably similar to a password. It is also used to secure software, websites and hardware systems. A passphrase is longer than a password, so it maximizes the key space, providing better security [12]. It consists of a series of strings that are memorized by the user, it could or could not be meaningful, also used to verify a person's identity. The challenges faced by passphrases are listed below:

- Some websites have a character limit, so users can not enter long passphrases.
- Some passphrases may be predictable because patterns in human nature make guessing easier for cybercriminals.

3) A **Personal Identifier Number** (PIN) is a numerical or alphanumeric code, usually four or six digits long, that is a popular authentication method used to unlock smartphones, withdraw money from Automated Teller Machines, activate alarms, and open doors [21]. Figure 3 shows a person entering their PIN code on a keypad of an ATM.

PINs are not secure because of their ease of use and speed. The challenges faced by PINs are listed below:

- PINs are vulnerable to cameras watching when a person is entering it in an ATM.
- Someone could be watching as a person enters their ATM pin into the machine [21].
- A thermal camera could be employed to determine the heat signatures associated with the touch inputs used for entering the PIN code [21].

4) **Fingerprint scanning** is the oldest biometric authentication method and thus one of the most well-established biometric authentication methods for

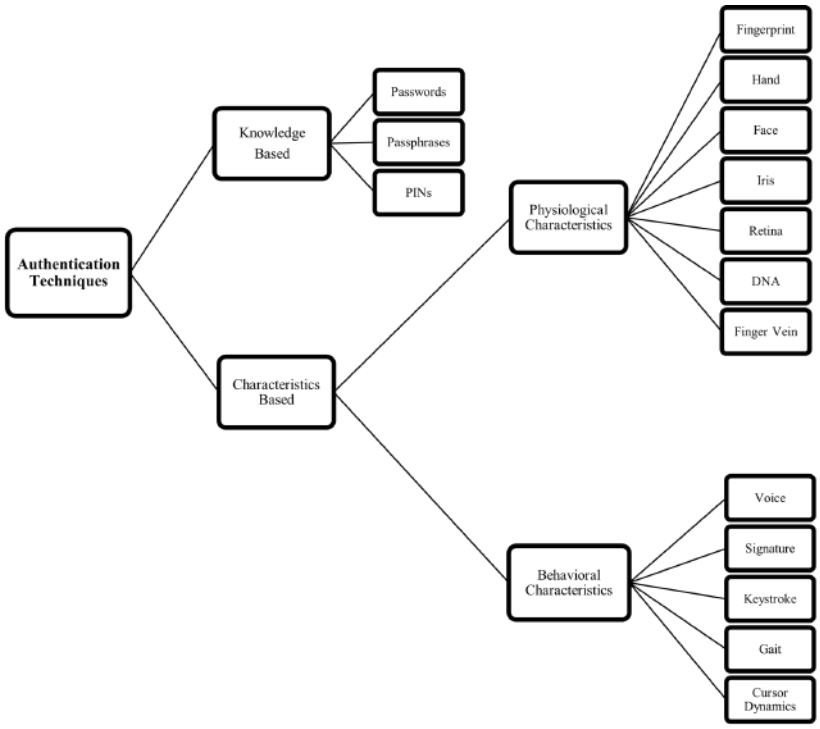

Figure 1. Authentication Techniques

Figure 2. Meaningful and Non-meaningful Password

Figure 3. Keypad of an ATM

Figure 4. Fingerprint Scanner and Fingerprint

identification [22], however, it still requires research and technological advancements in the field. Fingerprints are mostly used in crime detection, access control, attendance systems, and mobile security [3]. Figure 4 shows a fingerprint scanner and a sample of the fingerprint.

Fingerprints are made of loops, arches, and whorl patterns and appear as white lines and dark lines when captured from the device, matching is conducted through minutiae-based methods, which rely on the locations and directions of minutiae points, and pattern matching, where fingerprints are compared to assess similarity [4]. Touch dynamics also make use of fingerprints, they blend touch screen input with behavioral biometrics, and they are employed for authentication by training discriminative classifiers on touch data records [23]. Some of the challenges faced by fingerprints are listed below:

- High elasticity of skin may distort the shape and location of the skin [22] which leads to recognition errors.

- Real-time processing is required [22] to ensure swift identification and access to individuals using collected fingerprint data.
- Wet and wrinkled fingers may cause distortion and non-recognition in biometric profiling [4] as they can conceal or alter the ridges and valleys of the fingerprint.

5) **Hand geometry recognition** method utilizes the distinctive spatial arrangement of a person's hand or fingers such as length, width, thickness, and surface area, using mechanical or optical principles, to profile for biometric authentication. It is used in attendance tracking, personal verification, and physical access. Figure 5 shows a Hand Scanner and a sample of Hand.

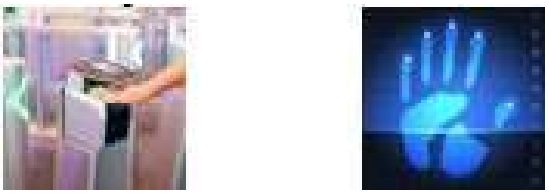

Figure 5. Hand Scanner and Hand

Hand Geometry Recognition method works because each person's hands are unique, after a certain age each person's hands have a distinct geometry that remains unaffected. This method also works with dirty hands, and it is a space-optimized authentication method for storage [4, 22]. Some of the challenges faced by hand geometry are listed below:

- Given its reliance on intricate devices and sensors to accurately capture and process hand geometry data, hand geometry recognition is characterized as a hardware-intensive process.

6) **Facial scanning technology** makes use of the distinct facial features of all human beings. It assists in personal surveillance systems, securing personal devices, and facilitating criminal identification at the governmental level. Figure 6 shows a Facial Scanner and a sample of Face.

Facial scanning technology can be classified into two types, one method is based on specific facial features, for example the position of eyes and the distance from the eyes to the nose, which computes and stores facial metrics in a template, whereas the other method categorizes face based on similarities to a fixed set of faces. Facial recognition systems capture pictures of peoples' faces using high-quality cameras to create matching templates [4, 22]. Some of the challenges faced by facial scanning are listed below:

Figure 6. Facial Scanner and Face

- A person could change the position of their face while having their picture clicked, resulting in differences in the image that is captured.
- The lighting conditions may not always be the same.
- A person could be wearing a cap, glasses, or facial hair one time and then not the other time, which will lead to altered results.
- Different facial expressions could affect the quality of the system, as it will provide inconsistent results.

7) **Iris recognition** capitalizes on the unique features present in everyone's iris to ascertain their identity. Through the scanning of the iris, which constitutes the colored ring encircling the pupil situated between the cornea and the lens of the eye, the system scrutinizes it for the purpose of identification. Figure 7 shows an Iris Scanner and a sample of iris.

Figure 7. IRIS Scanner and Iris

Applications for iris recognition can be found in many domains, such as border control, law enforcement, physical access control, and citizen ID programs. During the recognition process, the system calculates the hamming distance between iris codes and subsequently contrasts them with a predefined security

threshold to authenticate the individual [4, 22]. Some of the challenges faced by Iris Recognition are listed below:

- Wearing eye lenses or eyeglasses could affect the quality of the system.
- Watery eyes or sunlight in the eyes could also affect the system as it would cause reflection in the eyes.

8) **Retina scanning** utilizes low-power infrared lasers and cameras to capture highly detailed images of the retina. These lasers illuminate the retina, allowing the blood vessels to absorb the energy, thereby creating a distinct pattern that serves as a basis for identifying individuals. Figure 8 shows a Retina Scanner and a sample of the retina.

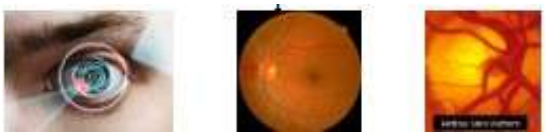

Figure 8. Retina Scanner and Retina

FIGURE 8. RETINA SCANNER AND RETINA

Retinal scanning technology is primarily used in high-end laboratories, nuclear power plants, and military bases. To undergo the scanning procedure, participants are required to remove any eyewear and maintain complete immobility while fixating on the lasers for ten to fifteen seconds. The method's exceptional reliability stems from the near impossibility of duplicating a human retina [4, 22]. The challenges faced by retinal scanning are mentioned below:

- Retinal characteristics are not sustained due to some diseases.
- Many people are afraid to put their eyes this close to a light source.

9) **DNA matching** is a process that sequences the DNA of a person to compare it against the DNA of other people present in a database. DNA matching is used in applications such as forensic science, paternity testing, and medical research. Figure 9 shows a DNA matching machine and DNA strand.

Figure 9. DNA Matching and DNA Strand

DNA matching is a very intrusive approach that is done by gaining access to a sample of a person's saliva, hair, blood, or tissue for the authentication process [4]. The challenges faced by DNA matching are that this is not an automatic approach, and it requires samples that need to be developed.

10) **Finger Vein Recognition** is a biometric authentication method that identifies individuals based on the images of the vessels present in their hands. Figure 10 shows a finger vein scanner.

Figure 10. Finger Vein Scanner

Applications for finger vein patterns include identity verification in high-security settings, biometric authentication for safe banking transactions, and access control systems. Several hand images are collected using near-infrared imaging for different people. All the images are then preprocessed in different models so that samples are generated [22]. Challenges faced by finger vein patterns include:

- It can be difficult to consistently maintain precise finger placement for accurate vein pattern capture.
- Variations in temperature and external lighting can degrade the quality of vein pattern images, resulting in errors.

11) **Voice recognition** is a behavioral biometric technique that relies on speech acoustic and explores

a person's speaking patterns using vocal features such as vocal tract, mouth, and nasal cavities. Voice recognition works because everyone has a unique pitch. It has three input styles, text-dependent, text-prompted, and text-independent. Figure 11 shows Voice recognition and a sample of sound waves.

Figure 11. Voice Recognition and Sound Waves

Voice recognition technology can be found in many industries, including smart speakers, smartphones, cars, customer service, healthcare, and security. It allows for automated phone menus, hands-free device control, smart home features, medical transcription, navigation, and biometric security system authentication. Voiceprints are processed and stored using technologies such as hidden Markov models, pattern-matching algorithms, neural networks, and decision trees. Speech recognition, biometrically profiling people for authentication using voice, can also be done using voice recognition [4, 22]. Some of the challenges faced by the voice recognition systems are mentioned below:

- Noise impedes voice recognition by distorting audio clarity, which makes it more difficult for the system to recognize spoken words.
- Variations in pronunciation, vocabulary, and speech patterns brought about by dialects can occasionally impede the accuracy of the voice recognition system.

12) **Signature Recognition** is dependent upon multiple factors, including but not limited to pressure, direction, acceleration, stroke length, number of strokes, and duration of the signature. Signature Recognition is used in Banking, document authentication and access control. Collecting the data of multiple people signing their names is facilitated by sensors integrated into pens or papers, which capture these dynamics, and then they are processed so that they can be later compared with the original signatures to see if they match or not to identify a person [4, 22]. Figure 12 shows a signature recognition scanner. Problems that occur with signature recognition are lack of accuracy.

Figure 12. Signature Recognition Scanner

13) **Typing recognition system** is a new biometric authentication system and it relies on users inputting text or passwords into a system, it records keystroke timings, speed, and pressure for analysis. Typing recognition is used in authentication systems, personal devices, text entry interfaces and online platforms as shown in Figure 13.

Figure 13. Typing Recognition Technology

A minimum of eight characters are required, attributes include passwords, usernames, and email addresses. The system enhances recognition with modern technologies, with an average error rate of 3% [4, 22]. The major issue associated with typing recognition is that its accuracy needs to be improved.

5 Effectiveness of Biometric Authentication Methods: A Case Study Analysis

Biometric authentication has now become more popular than ever because cyber threats are quite common, and passwords are becoming increasingly prone to

Table 2. Applications of Authentication Techniques

S/N	Techniques	Applicable	Problems	Rationale
1	Password	Websites Computers App	Bruteforce Leakage Reuse	Ease of Use Poor Policies Poor Usability
2	Passphrase	Websites Software Hardware Systems	Character limit Predictable	Space Trendiness
3	Pin	Smart Phones ATMs	Surveillance	Observability
4	Fingerprint	Smartphones Crime detection Attendance Systems Security Industry	Skin Elasticity Processing Moisture Wrinkles	Deformation Prompt verification Obfuscation
5	Hand Geometry Recognition	Attendance Tracking Personal Verification Physical Access	Hardware-intensive	Precision
6	Facial Scan	Device security CCTV Forensics	Movement Lighting item Disguise Variability	Variations Illumination Alteration Inconsistency
7	Iris Recognition	Identity management Border Control	Eyewear Glare	Obstruction Reflection
8	Retina Scan	Military installation Nuclear Facilities	Pathology Phobia	Degradation Lasers
9	DNA Matching	Forensics Paternity Research	Manual	Cultivation
10	Finger Vein pattern	Security Banking	Precision Conditions	Accuracy
11	Voice Recognition	Smartphones Customer service Internet of Things	Noise Dialect	Hindrance Accuracy
12	Signature Recognition	Banking	Inaccuracy	Vulnerability
13	Keystroke Recognition	Gadgets	Inaccuracy	Precision

attacks. Biometric authentications utilize distinct behavioral and physical characteristics for identity verification. However, it is still an ongoing discussion as to which biometric authentication method is the most successful in a practical setting. The objective of this case study is to evaluate the effectiveness of different knowledge-based as well as biologically-based authentication techniques by analyzing how they are applied in various use cases. Physiological or behavioral traits, such as voice, facial features, iris patterns, fingerprints, or keystroke dynamics, can be used in biometric authentication to confirm an individual's identity. In contrast to conventional authentication techniques like PINs or passwords, biometric authentication has built-in benefits like fraud resistance, convenience, and higher security.

The main goal of this case study is to evaluate the effectiveness of various knowledge-based as well as biologically-based authentication techniques in various real-world contexts. The specific objectives of this study are to evaluate the precision and dependability of biometric authentication techniques. And to evaluate how well biometric authentication technologies work in practical applications and how well users accept them. We used a mixed approach in this case study, i.e. combining quantitative analysis with qualitative information that we obtained from questionnaires and interviews.

The study has examined various biometric authentication techniques, including physiological biometrics such as fingerprints, hand geometry recognition, facial scanning, voice recognition, iris recognition, retina scans, DNA matching and finger vein patterns. Behavioral biometrics such as signature recognition, typing recognition and knowledge-based authentication methods such as passwords, passphrases, and pins. Data is collected from Baccalaureate and Post-Graduate students, including qualitative and quantitative information on user experiences, difficulties, and accuracy rates. The statistical analysis and thematic analysis of qualitative data are used to assess the reliability and efficacy of biometric authentication techniques.

The study was conducted by collecting data from two hundred Computer Science students aged seventeen to thirty who use devices and gadgets in a daily routine, so they have multiple accounts across websites and software and have a need to keep their data safe. They were asked which of the above-mentioned physiological biometrics and behavioral biometrics as well as the knowledge-based authentication techniques they have used across their devices and software. The data was then collected and summarized, and each of the two hundred students was then asked how good the authentication method that they had used was, all the data collected was then calculated as a percentage. Each person was also asked to rate the highest authentication technique from all the ones that they had used to select the one that they liked the most and used the most frequently. The data is presented in a tabular form in a bar chart in Figure 14 below.

The data shows that most people have now switched to fingerprints and facial scans, but passwords are still being used by a lot of users. The students were also asked why they were using a particular authentication technique. The most common reason for the switch to fingerprints and facial scans from passwords was the "convenience that the fingerprint offers as there is no need to remember multiple passwords for multiple websites, all we need to do is press our finger or scan our face".

The results also indicate that the precision score is a tie between passwords, PINs, and fingerprints because the users claim that keeping one password for multiple websites is convenient and they never get it wrong. They also suggested that the correct PINs always work because a sequence of numbers is not case-sensitive and usually not that hard to remember either. The results said that fingerprints are precise most of the time because they usually work even if the finger is not very clean, or the fingers are a little wet.

6 Conclusions and Future Work

The paper emphasizes the value of biometric techniques for online security, regardless of all the security that biometric authentication techniques offer, they still must face a lot of issues with the

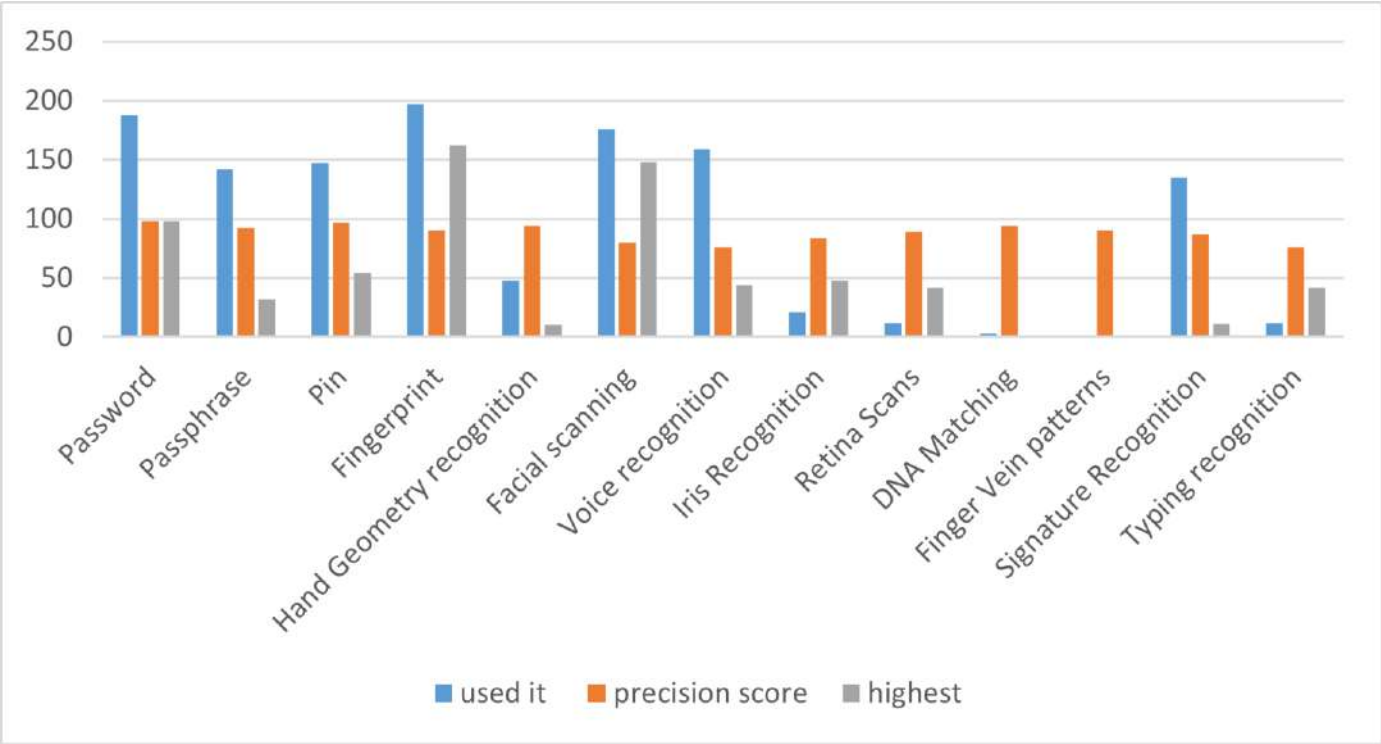

Figure 14. Survey Results of the Authentication Methods

usability, privacy, and user acceptance due to it being a new field and the scope of the field being too big. The study evaluates the user interaction with different knowledge-based and biologically based authentication techniques and how there needs to be a balance between the convenience and the security of the biometric authentication techniques. The results of the case study also suggest that the benefits of biometrics are limitless if only we can start utilizing all the security that they have to offer.

The survey conducted in the paper suggests that even though most people still use passwords and PINs, a lot of people are now moving on to fingerprint and facial recognition systems because of the security it provides. It also suggests that people do not prefer having to remember multiple passwords for multiple accounts, instead, they prefer the convenience of unlocking all of their accounts with a simple fingerprint or facial scan.

Biometric authentication techniques could be worked on in the future on user-centric designs, taking user privacy into account and integrating with all the emerging technologies.

Author Contributions

Warda Hassan: Conceptualization, Methodology, Writing- Original draft preparation **Dr. Nosheen Sabahat**: Supervision, Reviewing and Editing

7 Acknowledgements

I extend my heartfelt gratitude to ALLAH for His benevolence and mercy, which have enabled me to successfully complete this research Endeavor. I also appreciate my supervisor, **D**r. Nosheen Sabahat, for her sincere guidance and unwavering support throughout this journey. Her assistance in providing the necessary resources and fostering a conducive environment has been invaluable in the completion of this assignment. Her support and encouragement have been instrumental in shaping the outcome of this research, and for that, I am deeply thankful.

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest. It is also declared that this article does not

contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] K. Papadamou, S. Zannettou, B. Chifor, S. Teican, G. Gugulea, A. Recupero, A. Caponi, C. Pisa, G. Bianchi, S. Gevers, C. Xenakis and M. Sirivianos, "Killing the Password and Preserving Privacy with Device-Centric and Attribute-based Authentication," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2183 - 2193, 2019.

[2] E. D. Cristofaro, H. Du, J. Freudiger and G. Norcie, "A Comparative Usability Study of Two-Factor Authentication," *arXiv preprint arXiv*, vol. 1309, no. 5344, 2014.

[3] N. Yusuf, K. A. Marafa, K. L. Shehu, H. Mamman and M. Maidawa, "A survey of biometric approaches of authentication," *International Journal of Advanced Computer Research*, vol. 10, no. 47, pp. 96-104, 2020.

[4] S. S. Harakannanavar, P. C. Renukamurthy and K. B. Raja, "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends," *International Journal of Advanced Networking and Applications*, vol. 10, no. 04, pp. 3958-3968, 2019.

[5] A. A. Kaur and K. K. Mustafa, "A Critical appraisal on Password based Authentication," *International Journal of Computer Network and Information Security*, p. 15, 2019.

[6] "types of authentication methods," *Available: https://optimalidm.com/resources/blog/types-of-authentication-methods/*, 2020.

[7] K. B. Anderson, E. Durbin and M. A. Salinger, "Identity Theft," *Journal of Economic Perspectives*, vol. 22, no. 2, pp. 171-192, 2008.

[8] S. Irshad and T. R. Soomro, "Identity Theft and Social Media," *International Journal of Computer Science and Network Security*, vol. 18, no. 1, pp. 43-55, 2018.

[9] "improve-2fa-user-experience," *Available: https://www.wpexplorer.com/improve-2fa-user-experience/*, 7 November 2023. [Online]

[10] S. Das, A. Kim, B. Jelen, L. Huber and L. J. Camp, "Non-Inclusive Online Security: Older Adults' Experience with Two-Factor Authentication," *54th Hawaii International Conference on System Sciences*, Hawaii, 2021.

[11] I. Gordin, A. Graur, S. Vlad and C. I. Adomniței, "Moving forward passwordless authentication: challenges and implementations for the private cloud," *20th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Iasi, Romania, 2021.

[12] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger and J.-J. Schwartzmann, "A review on authentication methods," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 5, pp. 95-107, 2013.

[13] V. Veeraiah, K. R. Kumar, P. L. Kumari, S. Ahamad, R. Bansal and A. Gupta, "Application of Biometric System to Enhance the Security in Virtual World," *2nd International Conference on Advance Computing and Innovative Technologies in Engineering*, Greater Noida, 2022.

[14] S. A. Abdulrahman, B. Alhayani, "A comprehensive survey on the biometric systems based on physiological and behavioural characteristics," *Materials Today: Proceedings*, vol. 80, no. 3, pp. 2642-2646, 2023.

[15] N. Khan, M. Arif, M. Darus, et al., "digital-identity-and-security," *Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics*, Thales group, 20 May 2023. [Online].

[16] V. Liskin, E. Serdobolskiy, I. Sopilko and T. Okhrimenko "Two-factor User Authentication Using Biometrics," *CybHyg*, vol. 2654, pp. 526-535, 2019.

[17] F. Ennaama, K. Benhida and A. Boulahoual, "Comparative and analysis study of biometric systems," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 12, pp. 3466-3476, 2019.

[18] S. Parusheva, "A comparative study on the application of biometric technologies for authentication in online banking," *Egyptian Computer Science Journal*, vol. 39, no. 4, pp. 116-127, 2015.

[19] N. Bawany, R. Ahmed and Q. Zakir, "Common Biometric Authentication Techniques: Comparative Analysis, Usability and Possible Issues Evaluation," *Research Journal of Computer and Information Technology Sciences*, vol. 1, no. 4, pp. 5-14, 2013.

[20] Author, “physiological vs behavioral biometrics difference,” *Available: https://www.iproov.com/blog/physiological-vs-behavioral-biometrics-difference*, iproov, 21 December 2022. [Online].

[21] X. Bultel, J. Dreier, M. Giraud, M. Izaute, T. Kheyrkhah, P. Lafourcade, D. Lakhzoum, V. Marlin and L. Mota “Security analysis and psychological study of authentication methods with PIN codes,” *12th International Conference on Research Challenges in Information Science*, Nantes, 2018.

[22] S. R. Kodituwakku, “Biometric Authentication - A Review,” *International Journal of Trend in Research and Development*, vol. 2, no. 4, pp. 113-123, 2015.

[23] V. M. Patel, C. Rama, C. Deepak and B. Brandon, “Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges,” *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 49-61, 2016.