Fingerprint Sequencing: An Authentication Mechanism that Integrates Fingerprints and a Knowledge-based Methodology to Promote Security and Usability

Mohammad H. Algarni
Department of Computer Science, Al-Baha University, Saudi Arabia
malgarni@bu.edu.sa (corresponding author)

Received: 13 March 2024 | Revised: 31 March 2024 and 7 April 2024 | Accepted: 9 April 2024

 DOI: https://doi.org/10.48084/etasr.7250

ABSTRACT

Biometric authentication stands at the forefront of modern security measures, offering a highly sophisticated and reliable method for identity verification. Biometrics aims to identify an individual's identity by comparing specific characteristics against a stored template. Unlike traditional passwords or PINs, which can be forgotten, shared, or stolen, biometric authentication relies on unique biological or behavioral traits that are inherent to each individual. The current article introduces the innovative concept of multi-fingerprint sequence authentication process to verify users. In contrast to the traditional, single fingerprint methods, this multifactor technique combines the use of multiple fingerprints along with a sequence pattern for enhanced usability and security. Furthermore, this study presents a comprehensive evaluation of an innovative authentication system utilizing a multiple fingerprint sequence pattern as an alternative to biometric usernames and textual passwords, named BioPass. By leveraging an established framework, the research focuses on assessing the proposed system's usability and security aspects, as well as its potential benefits.

Keywords-authentication; biometrics; security; usability; privacy; multi fingerprints; fingerprint sequencing

I. INTRODUCTION

A. The Importance of Security

In modern technological societies, the security landscape is constantly changing. With the increasing number of devices and advancement of tactics, new threats constantly arise. Every day individuals face a range of risks, including malware infections, phishing attempts, and sophisticated hacking methods. To protect their information and digital possessions effectively, they must remain vigilant, and constantly adapt to this ever-evolving environment. To safeguard and maintain the privacy of data, identity verification processes for individuals who wish to access those data have been introduced. Only when an individual's identity has been accurately verified and approved they are given permission to use or access the data [1]. This effort includes approaches, such as implementing encryption protocols and incorporating artificial intelligence and machine learning technologies to detect and remove potential threats [2]. The proposed method combines multiple fingerprints in a specific order to ensure user verification security. This innovative method adds a layer of protection that is not only compelling, but also highly resistant to unauthorized access attempts.

B. The Distinct Advantages of Biometric Authentication

There is an urgent need to revolutionize the field of user authentication. While the traditional, password-based, systems are widely used, they have been found to possess vulnerabilities that can lead to breaches and unauthorized access [3]. As a result, there is a shift towards more reliable methods like biometric authentication. Biometric authentication systems have been proven to be more effective and secure compared to the existing technologies [4]. By utilizing behavioral traits, like fingerprints, facial features, or voice patterns, biometric schemes can provide a higher level of security and accuracy compared to the traditional methods [6]. Biometrics can recognize an individual's characteristics by matching features against a pre-existing template, either possession-based (using tokens like security tags or cards) or knowledge-based (codes or passwords). Reliable validation systems often employ samples for verification by incorporating various characteristics and dimensions [6]. Biometrics is defined as the unique (personal) physical/logical characteristics or traits of the human body [8]. These characteristics and traits can be deployed to identify a human being. Any details of the human body which differ from one person to another, such as: retina, iris, fingerprints, palm print, and DNA can be used as unique biometric data that reflect that person's unique identification (ID) [8]. Biometric features, unlike passwords,

are inherent to everyone while being extremely difficult to duplicate [7]. As technology advances, biometric authentication is no longer primarily a choice but, in fact, essential for strengthening digital security [6]. The adoption of biometric technologies is motivated by their efficacy, ease, and capacity to offer an unsurpassed degree of security [8]. With the ongoing advancement of biometric technology like facial recognition and fingerprint authentication, these methods are increasingly being recognized as the most reliable means of verifying users' identity [9]. The future of authentication hinges on the smooth incorporation of biometric characteristics and other authentication factors to provide a secure, user-friendly experience across many digital platforms [10]. Biometric technology has been implemented at airports to provide faster and more secure processes and hence reduce waiting time. Around 63% of airports and 43% of airlines intended to allocate funds towards the implementation of biometric processing systems by 2020 [11]. Biometric authentication is increasingly being acknowledged by various businesses and organizations for its potential and advantages, thus positioning it as a fundamental aspect of digital security measures [12].

C. The Cornerstone: A Fingerprint Authentication System

A fingerprint authentication system utilizes distinct patterns present on our fingertips. These patterns, such as ridges, loops, and whorls, develop in the womb, and remain relatively constant, without significant alterations, throughout our lives [13]. When a finger is placed on a sensor, the system records and analyzes these patterns, before transforming them into a representation. Subsequently, this representation can be matched with pre-existing templates for authentication [14]. The distinguishing feature of fingerprint authentication lies in its exceptional accuracy. The distinctive nature of each person's fingerprint, even between twins, makes it an exceptionally reliable method for identifying individuals. Furthermore, the system's capacity to identify specific characteristics, known as minutiae points, guarantees the verification of the identification [15]. The combination of a high degree of accuracy with the simple, effective nature of the process positions fingerprint authentication as one of the foremost technologies in use today.

D. The Concept of the Multi-fingerprint Sequence Authentication Process

The core of this new technique is the incorporation of several fingerprint patterns, which function as a multifactor authentication scheme by combining biometric identification (fingerprints) with knowledge-based authentication (a sequence). Modern systems commonly utilize a form of authentication that depends on "something you know", such as a password, and a sequence of fingerprints to be presented to a scanner, as the initial method for confirming an individual's identification. Common secondary authentication methods include SMS/phone verification, physical tokens, biometric identity, One Time Password (OTP), and push notifications [3]. The variety of additional identification verifications provided in this context exhibits diversity, within the scope of authentication procedures [16]. The main purpose of establishing such a system is to make stolen account credentials useless to fraudsters who lack the information required to complete the secondary authentication step. Fingerprint recognition, known for its accuracy and dependability, is the fundamental basis of the biometric authentication technique [17]. Nevertheless, what distinguishes it is the necessity for users to provide not just one but a consecutive series of fingerprints, in a predetermined order. This factor adds an extra level of complexity, significantly making it more difficult for unauthorized users to circumvent the authentication procedure. The sequential nature of this knowledge-based component enhances the authentication process, rendering it unimodal. Users need a clear understanding of the precise sequence in which these fingerprints must be provided.

II. RELATED WORK

Authors in [18] proposed FingerPIN, a novel authentication technique that integrates fingerprints with Personal Identification Numbers (PINs) to augment security. The authors propose a factor approach that combines the characteristics of knowledge-based and biometric-based authentication factors in order to solve concerns about the permanence of fingerprints. To address this concern, FingerPIN implements a method whereby users must submit a series of fingerprints that correspond to their selected PIN digits. This is determined by a correlation between the numbers and digits. The authors also performed a vulnerability analysis of the proposed technique, showcasing its robustness in scenarios where a fraudster compromises one or several fingerprints. The report emphasizes the crucial need for strong authentication techniques to protect data and apps against the ever-evolving cybersecurity threats. The experimental results confirm that FingerPIN is highly effective in preventing brute force assaults, therefore demonstrating its superiority over authentication methods that are based on PIN or fingerprints. Nevertheless, it is essential to acknowledge that the significant memory burden placed on users could potentially reduce its attractiveness with regard to widespread use. Furthermore, there has been an absence of usability research or user acceptance piloting regarding this technique. Authors in [19] proposed a method of authentication that enhances the security of fingerprint biometrics. They suggest a solution that fills a gap in the research by recommending the use of securely stored fingerprints, each of which is associated with a unique password. By combining fingerprint and extended password authentication, they aim to elevate the security level. This study explores the distinct nature of fingerprint identification while also highlighting the risks associated with the existing fingerprint systems. The authors suggested an approach in which multiple fingerprints are stored alongside passwords for security. These passwords are generated based on the position of each finger and combined with a chosen password by the user, offering both flexibility and enhanced security. This method effectively merges the benefits of biometrics with the traditional security protocols, resulting in an adaptable, dependable authentication solution. The method proposed in this article, nevertheless, is less user-convenient, since they must remember each number associated with the finger that will be added to the passwords that they provided during the registration phase. Another factor is that the extra prefix added to the passwords for each finger is fixed, making it vulnerable to attacks, since it is difficult to replace.

III. MOTIVATION

In the field of user authentication, the potential for reforming the standard methods is both attractive and essential. The traditional password-based systems, while commonly used, have demonstrated vulnerabilities to breaches and unauthorized access [4]. This has prompted a paradigm shift towards more secure, dependable methods, led by biometric authentication, which has been shown to be more efficient and secure than the standard technologies [5]. By capitalizing on distinctive physiological or behavioral traits, such as fingerprints, facial features, or voice patterns, biometric systems offer a level of security and accuracy that exceeds that offered by the traditional methods [6]. In the modern world, people find themselves relying heavily on digital platforms and interfaces in almost every aspect of their lives. Whether one is making transactions or engaging in personal communication, the importance of having secure measures in place cannot be overstated. The traditional methods, that were once considered sufficient for authentication, now face challenges due to the evolving cyber threats and sophisticated attack techniques. Considering these challenges, a groundbreaking approach that combines the strengths of authentication with sequential knowledge-based verification has emerged. Passwords, which were once considered to safeguard individuals' security, have proven to be vulnerable to breaches arising from phishing attacks, brute force attempts, and credential stuffing. As technology has advanced, so has the capability of cybercriminals, necessitating a leap forward in the authentication methods that will be adopted. By integrating biometric data, which are extremely difficult to replicate, with a requirement for specific sequence knowledge, this innovative approach directly tackles this pressing need. Not only does this method represent a breakthrough, but it also demonstrates a strategic response to the ever-changing threat landscape.

IV. METHODOLOGY

Three fingerprints are provided in a specific sequence. These fingerprints, biometrics, and the chosen sequence, as knowledge-based information, are fused together to provide a secure, usable, multifactor authentication methodology. In the example shown in Figure 1, the chosen fingerprints during the registration phase are the left index finger, right thumb, and right index finger, consecutively. Following successful registration, users can confirm their identities by presenting their fingerprints in the same sequence as they did when registering on the system. It is apparent that the selection and sequence of the fingerprints are both provided by the user, a fact which provides both a level of security as well as usability to the proposed scheme. Once users have entered the three fingerprints, the system compares this input against the stored data. Since each fingerprint is mapped to a sequence number (1st, 2nd, 3rd) during the registration phase and is stored in the database, the proposed system compares it to the sequence in the database when all fingerprints are matched, as observed in Figure 2. The main goal in verifying each feature separately is to ensure that it returns usable feedback to the users if they fail to successfully authenticate themselves.

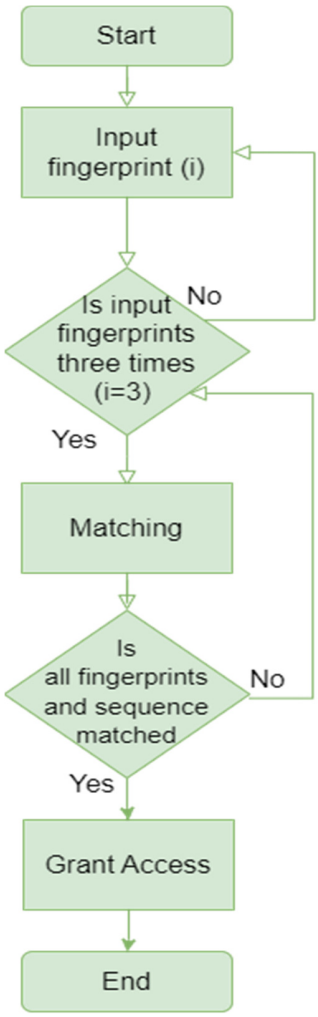

Fig. 1. System flowchart.

Further research in this area led to the discovery that the researchers from the University of Cambridge Computer Laboratory had found a solution to the problem of evaluating authentication systems. The new proposed authentication system needs to be evaluated from different perspectives to confirm its superiority to the legacy authentication system, that uses biometrics as a username combined with a textual password. The following section will refer to the legacy authentication system as BioPass. The next section also presents the benchmarks and metrics that can be applied to the proposed system in order to measure its strength regarding security and usability.

A. Evaluation Framework

Authors in [1] presented an unbiased evaluation framework of the proposed password replacement schemes. The framework was developed because these schemes have been facing several problems. On the journey to providing a reliable evaluation mechanism, authors in [1] provided a standard scale and framework that can evaluate any user authentication system. In the evaluation framework, a set of benefits, termed as Security, Usability, and Deployability, are presented.

However, this research focuses on usability and security rather than deployability since both systems are similar in terms of their authentication type as employing biometrics and being knowledge-based. This framework makes it possible to judge whether any authentication system which is proposed as a replacement for a similar existing system will be proved to be beneficial. The current research employed this framework to analyze the proposed system. Schemes like, password, proxy, federated, graphical, biometric, hardware-based, managers etc. are examined and evaluated using the framework of benefits. The authors in [1] conclude that no system is close to providing all the benefits that an ideal authentication system would offer.

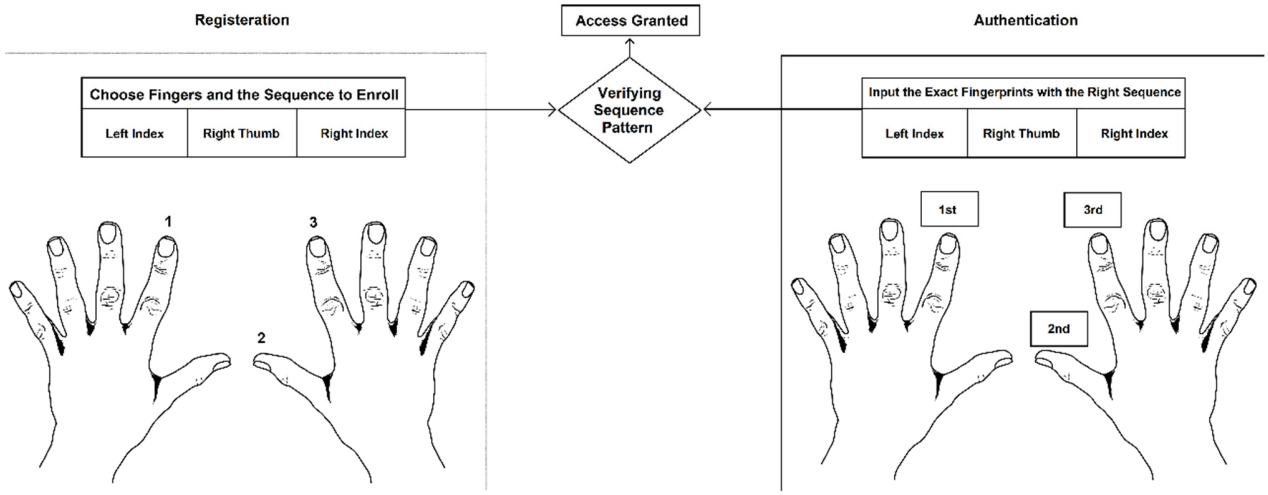

Fig. 2. Registration and authentication after user chooses fingers in a sequence. In this case, left index, right thumb, and right index in order.

B. Relevance of the Framework to the Proposed System

Authors in [1] compared the idea of using fingerprints with utilizing textual characters as passwords. Their conclusion, based on various criteria, was that using fingerprints as passwords performed worse than employing textual passwords in terms of efficiency, recovery from loss, frequent errors, deployability, etc. A further important factor in authentication systems is the username field. In this research, the idea of using a sequence pattern of fingerprints as a password is respected but, regarding usernames, it proposes the use of multiple fingerprints. As fingerprints, or biometrics in general, represent who you are, it is essential that they are used as usernames.

C. Application of the Framework to the Proposal

The framework presented in [1] can be directly applied to the research presented in this paper, which focuses on a password replacement scheme. The framework presents detailed criteria, based on which an authentication system can be evaluated. The criteria presented are divided into the categories of security and usability. In this section, an analysis of the BioPass system and the proposed system will be performed for each criterion presented in the framework.

1) Usability

- Memorywise-Effortless: In the case of the BioPass authentication system, a user must remember a password that usually has a minimum length requirement to ensure security, while in the proposed system the user needs to remember only the sequence in which the fingerprints must be presented. Hence, the proposed system places fewer burdens on the user's memory compared to the BioPass system.
- Scalable-for-Users: The BioPass authentication systems and passwords are not scalable, since a cognitive load is placed on the user to keep the passwords separate for every account. Some users prefer to deploy different passwords for different accounts, but the proposed system minimizes the load because no password is required. The sequence pattern of fingerprints can be the same for multiple accounts and the user does not need to remember anything.
- Nothing-to-Carry: With the adoption of smartphones and embedded fingerprint sensors, nothing needs to be carried in both systems.
- Physically-Effortless: The proposed system requires only the correct sequence of fingerprints to be presented, whereas the BioPass system demands a relatively long password.
- Easy-to-Learn: BioPass authentication systems are easier to learn than the proposed system, as not all users may have been trained to handle a sequence pattern.
- Efficient-to-Use: The existing devices for fingerprint scanning are efficient for both systems.
- Infrequent-Errors: With the BioPass authentication systems that exist today, there is an increased chance that errors will occur when typing the password compared to presenting fingerprints in a particular sequence.
- Easy-Recovery-from-Loss: Both the password in the BioPass authentication system and the sequence pattern in the proposed system are easy to change in the event of forgetfulness or account compromise. Nevertheless, the proposed system boasts a lower likelihood of compromise.

2) Security

- Resilient-to-Physical-Observation: Neither the BioPass authentication system nor the proposed system are resilient to physical observation.
- Resilient-to-Targeted-Impersonation: Due to the carelessness of the users in choosing a password that is easy to guess and/or writing it down on paper, the BioPass system is quasi-resilient to targeted impersonation. The sequence pattern in the proposed system can be targeted more, so the system is not resilient to targeted impersonation.
- Resilient-to-Throttled-Guessing: Weak passwords are not resilient to throttled guessing. The proposed system is easier to guess, and hence also not resilient to throttled guessing.
- Resilient-to-Unthrottled-Guessing: The BioPass authentication system is not resilient to unthrottled guessing (brute force) because weak passwords can be targeted. The proposed system is resilient, however, because the sequence cannot be easily targeted using Unthrottled-Guessing.
- Resilient-to-Internal-Observation: Neither textual passwords nor the proposed system are resilient to internal observation.
- Resilient-to-Leaks-by-other-Verifiers: Like the BioPass authentication system, the proposed system is not resistant to leaks by other verifiers.
- Resilient-to-Phishing: Passwords are not resilient to phishing attacks. The resilience of the proposed system towards phishing attacks would depend on the implementation rather than the design. For example, if the sequence pattern template never leaves the device, then it would be resilient to phishing attacks.
- Resilient-to-Theft: Neither the BioPass authentication system nor the proposed system require any external device or hardware for authentication, and so are resilient to theft.
- Non-Trusted-Third-Party: Neither the BioPass authentication system nor the proposed system require a third party to be trusted for the authentication, so the benefit is maintained.
- Requiring-Explicit-Consent: In the case of textual passwords, one needs to type them in, which requires explicit consent. Similarly, one needs to provide fingerprints in a specific order to authenticate them and so the proposed system requires explicit consent as well.
- Unlinkable: Both the BioPass authentication system and the proposed system are linkable due to the use of physical biometrics in both systems.

Table I displays the scores received by both systems for each criterion. The label "Y" indicates that a system offers the benefit stated by the criterion, "N" that it does not, and label "Q" that a system improves the situation partially. Quantifying the scores received by each method helps to the establishment of a mathematical base for comparison. Scoring the systems on the same set of numbers helps in deciding which of the systems performs better in comparison with the other. For this purpose, the labels "N", "Q" and "Y" are mapped to a set of numerical values. Label "N" is assigned a score of 0. As the label "Q" indicates better performance compared to "N", is assigned to a score of 0.5, and the label "Y" indicates that the system offers the benefit stated by a particular criterion, so is assigned a score of 1. The cumulative score for the usability of the BioPass system is 3 points, whereas the proposed system scores 4.5 points. Similarly, for the legacy system, the cumulative score for the security of the BioPass system is 2.5, and 3 for the proposed system. From Table I, it can be inferred that, regarding security and usability, the proposed system achieves a higher cumulative score compared to the BioPass system. It is safe, then, to argue that the proposed system outperforms the BioPass system as per the detailed criteria related to the aspects of security and usability.

TABLE I. SCORES RECEIVED BY BOTH SYSTEMS

Usability		
	BioPass	**Proposed system**
Memory Wise Effortless	N	Q
Scalable for Users	N	Q
Nothing to Carry	Y	Y
Physically Effortless	N	Q
Easy to Learn	Y	Q
Efficient to Use	Y	Y
Infrequent Error	N	Q
Easy Recovery from Loss	N	N
Security		
Resilient to:	**BioPass**	**Proposed System**
Physical Observation	N	N
Targeted Impersonation	Q	N
Throttled Guessing	N	N
Unthrottled Guessing	N	Q
Internal Observation	N	N
Leaks from Other Verifiers	N	N
Phishing	N	Q
Theft	Y	Y
No Trusted Third Party	Y	Y
Requiring Explicit Consent	N	N
Unlinkable	N	N

V. SUMMARIZED METRIC RESULTS

Measurement is the first step towards controlling something and may eventually lead to an improvement. It was necessary to measure the usability and security associated with the proposed system to understand its advantages and drawbacks.

A. Usability and Security

To calculate the various attributes or characteristics of the usability and security of any system, the measurement can be represented in the form of metrics. Based on [14], the results of the metrics can be added to a plot. Some of the metrics represent the usability and others the security of the system. There are 8 Usability Metrics (UM) and 1 Security Metric (SM). All the UM were created with a maximum score of 8 points. An ideal result will be a vector running from (0x) to (8x). Supposing that I = (8x).

All the security metrics were created with a maximum score of 11 points. An ideal result will be a vector running from (0y) to (11y). Supposing that K = (11y).

The Euclidean distance of U from I was calculated and the results for the BioPass system and the proposed system were noted.

The distance between I and U is equivalent to the Usability for BioPass):

$$d = \sqrt{(Ix - UM)^2} \Rightarrow d = \sqrt{(8 - 3)^2} \Rightarrow d = 5$$

Likewise, the Usability for the proposed system is:

$$d = \sqrt{(Ix - UM)^2} \Rightarrow d = \sqrt{(8 - 4.5)^2} \Rightarrow d = 3.5$$

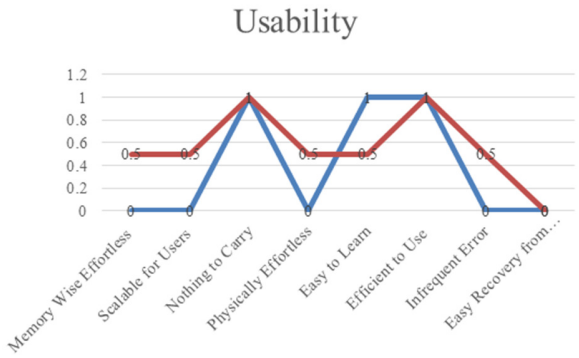

Fig. 3. Results of the comparison of the Usability of the BioPass system and the proposed system.

Distance between K and S (Security for BioPass):

$$d = \sqrt{(Ky - SM)^2} \Rightarrow d = \sqrt{(11 - 2.5)^2} \Rightarrow d = 8.5$$

Distance between K and S (Security for the proposed system):

$$d = \sqrt{(Ky - SM)^2} \Rightarrow d = \sqrt{(11 - 3)^2} \Rightarrow d = 8$$

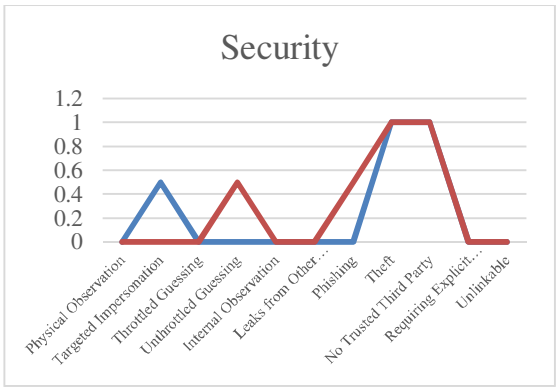

Fig. 4. Results of the comparison of Security in the BioPass system and the proposed system.

TABLE II. USABILITY METRIC SCORES AND THE CALCULATED EUCLIDEAN DISTANCE

System	UM	Euclidean distance from I
BioPass	3	5
Proposed	4.5	3.5

TABLE III. SECURITY METRIC SCORES AND THE CALCULATED EUCLIDEAN DISTANCE

System	SM	Euclidean distance from I
BioPass	2.5	8.5
Proposed	3	8

Based on the calculated Euclidean distance, it is clear that the proposed system is closer to the ideal system than the BioPass system, because it performs better in both aspects of Usability and Security.

B. Registration and Authentication Time

An experiment was conducted in Matlab to implement the concept suggested in this article and the BioPass system. Ten reads were acquired for both systems. The registration and verification times were documented for each read, and the average time of every stage was computed in ms for both systems as shown in Table IV.

TABLE IV. REGISTRATION AND VERIFICATION TIME (ms)

System	Registration time (ms)	Authentication time (ms)
BioPass	151, 147, 143, 137, 149, 143, 142, 138, 144,147 Average: 143.8	121, 125, 132, 137, 127, 141, 126, 138, 127,132 Average: 124.3
Proposed	109, 97, 106, 94, 98, 106, 94, 112, 97, 115 Average: 102.8	87, 96, 80, 76, 94, 85, 83, 74, 93, 81 Average: 84.9

The enhanced performance of the proposed system was proven by the results. Remarkably, the proposed system scores an average registration time of 102.8 ms and an average authentication time of 84.9 ms compared to an average of 143.8 ms and an average of 124.3 ms for the BioPass system, respectively. By comparing the registration and authentication times of both systems, Figure 5 clearly illustrates the efficiency improvements the proposed system provides. It is worth noting that the BioPass system often needs passwords with strict requirements like minimum length of 8 characters including at least one capital letter, numbers, and special characters for security purposes. This complexity is one of the reasons why the proposed system provides a more intuitive user registration and authentication process without the need for complicated password creation or memorization while still maintaining strong security measures.

The proposed system, not only improves user experience by reducing authentication time, but also offers security upgrades with a precise and quicker authentication method. However it is crucial to recognize constraints, like how the system may perform when altering the authentication algorithm. Nevertheless, the positive results from this study suggest that the proposed system should be considered as effective in providing an enhanced authentication process.

VI. CONCLUSION

Biometrics have the strong characteristic that one cannot forget easily or lose their biometrics. Also, as biometrics is hard to fake, unique to all, and enhances convenience, it is a strong candidate for enhancing the authentication systems. Some manufacturers fail to consider security threats while

making particular devices, hence, it is essential to strengthen these devices with security measures, such as biometrics, to protect them from unauthorized access [20]. It is worth noting that one of the main limitations to the fingerprint authentication that is employed by several mobile operating systems is the root access that permits users to access the operating system. Consequently, it allows users to control or avoid the security processes that have been built into the system. If any breach occurs in the root access, the fingerprints stored on the device can be compromised [21].

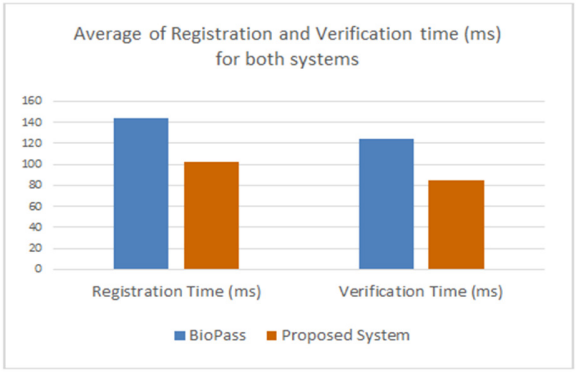

Fig. 5. Registration and authentication times comparison.

Biometric technologies, like Fingerprint identification, Hand Geometry, Iris scan, Face Recognition, etc. [22], are methods for verifying the identity of a living person based on physiological or, in some cases, behavioral characteristics. Currently, authentication systems involve authenticating a user's account using biometrics along with a textual password, BioPass system in this research suffers from drawbacks. Thus, it is necessary to focus not on developing a password replacement scheme, but on other aspects of the authentication process. In this research, to reinforce the security and usability of the authentication systems, a system that does not challenge the concept of passwords (something one knows) but instead focuses on enhancing the way this method will be merged with other authentication methods; in this case, biometrics (fingerprints) are used in a sequence pattern.

REFERENCES

[1] S. Muramoto, T. P. Forbes, A. C. van Asten, and G. Gillen, "Test Sample for the Spatially Resolved Quantification of Illicit Drugs on Fingerprints Using Imaging Mass Spectrometry," *Analytical Chemistry*, vol. 87, no. 10, pp. 5444–5450, May 2015, https://doi.org/10.1021/acs.analchem.5b01060.

[2] S. Zaman *et al.*, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 94668–94690, Jun. 2021, https://doi.org/10.1109/ACCESS.2021.3089681.

[3] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, Sep. 2003, https://doi.org/10.1109/JPROC.2003.819611.

[4] B. Ammour, T. Bouden, and L. Boubchir, "Face–iris multi-modal biometric system using multi-resolution Log-Gabor filter with spectral regression kernel discriminant analysis," *IET Biometrics*, vol. 7, no. 5, pp. 482–489, 2018, https://doi.org/10.1049/iet-bmt.2017.0251.

[5] A. K. Jain, P. Flynn, and A. A. Ross, Eds., *Handbook of Biometrics*. New York, NY, USA: Springer, 2007.

[6] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Professional*, vol. 3, no. 1, pp. 27–32, Jan. 2001, https://doi.org/10.1109/6294.899930.

[7] P. V. L. Suvarchala and S. S. Kumar, "Feature Set Fusion for Spoof Iris Detection," *Engineering, Technology & Applied Science Research*, vol. 8, no. 2, pp. 2859–2863, Apr. 2018, https://doi.org/10.48084/etasr.1859.

[8] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part II: Multiple Use Case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 140–151, Dec. 2010, https://doi.org/10.1109/TIFS.2010.2098873.

[9] A. K. Jain and A. Kumar, "Biometric Recognition: An Overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras, Eds. Dordrecht, The Netherlands: Springer Netherlands, 2012, pp. 49–79.

[10] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, Mar. 2018, Art. no. 1, https://doi.org/10.3390/cryptography2010001.

[11] N. A. R. Negri, G. M. R. Borille, and V. A. Falcão, "Acceptance of biometric technology in airport check-in," *Journal of Air Transport Management*, vol. 81, Oct. 2019, Art. no. 101720, https://doi.org/10.1016/j.jairtraman.2019.101720.

[12] C. Unal and V. Tecim, "The Use of Biometric Technology for Effective Personnel Management System in Organization," *KnE Social Sciences*, pp. 221–232, Nov. 2018, https://doi.org/10.18502/kss.v3i10.3540.

[13] H. Swofford, C. Champod, A. Koertner, H. Eldridge, and M. Salyards, "A method for measuring the quality of friction skin impression evidence: Method development and validation," *Forensic Science International*, vol. 320, Mar. 2021, Art. no. 110703, https://doi.org/10.1016/j.forsciint.2021.110703.

[14] V. M. Praseetha, S. Bayezeed, and S. Vadivel, "Secure Fingerprint Authentication Using Deep Learning and Minutiae Verification," *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1379–1387, Jan. 2020, https://doi.org/10.1515/jisys-2018-0289.

[15] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 43, no. 2, pp. 90–98, Oct. 2000, https://doi.org/10.1145/328236.328110.

[16] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *2012 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, May 2012, pp. 553–567, https://doi.org/10.1109/SP.2012.44.

[17] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. London, UK: Springer, 2009.

[18] E. Marasco and M. Albanese, "FingerPIN: An Authentication Mechanism Integrating Fingerprints and Personal Identification Numbers," in *Computer Vision and Image Processing*, vol. 1376, S. K. Singh, P. Roy, B. Raman, and P. Nagabhushan, Eds. Singapore: Springer Singapore, 2021, pp. 500–511.

[19] A. Q. M. S. U. Pathan, A. Chakraborty, M. Kabir, and K. Thakur, "Fingerprint Authentication Security: An Improved 2-Step Authentication Method with Flexibility," *International Journal of Scientific and Engineering Research*, vol. 10, no. 1, pp. 438–442, Jan. 2019.

[20] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[21] M. Algarni, "An Extra Security Measurement for Android Mobile Applications Using the Fingerprint Authentication Methodology," *Journal of Information Security and Cybercrimes Research*, vol. 6, no. 2, pp. 139–149, Dec. 2023, https://doi.org/10.26735/EPZF6556.

[22] D. Virmani, P. Girdhar, P. Jain, and P. Bamdev, "FDREnet: Face Detection and Recognition Pipeline," *Engineering, Technology & Applied Science Research*, vol. 9, no. 2, pp. 3933–3938, Apr. 2019, https://doi.org/10.48084/etasr.2492.