Towards Flexible Transparent Authentication System for Mobile Application Security

Abdullah Golam, Mohammed Abuhmoud, Umar Albalawi
College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia

***Abstract*—Undoubtedly, Mobile Application Security (MAS) has made tremendous progress in implementing enhanced security protocols in the past decade. With the recent increase in the usage of mobile applications, concerns of privacy and security are increasing rapidly. Thus, the security measurement must be applied to satisfy security and privacy needs. On the one hand, the developer community works feverishly to develop mobile applications with innovative and usable layers and user-friendly for multigenerational customers. However, the security community, in particular, strives to make those layers secure. Therefore, the main objective of this research is to build a transparent authentication system in a mobile application. There are potentially many ways to implement an authentication mechanism such as the biometrics approach. It has features, which can be used to heightened security for the end-user. In these articles, we experimentally investigate the multigenerational customer base's factors such as age, convenience, easiness, memorizing new passwords, and understanding the precept of frequently changing passwords to enhance security. Additionally, we propose a system that will solve the common problems users face when starting the password resetting process. At the same time, in the MAS sector, we orchestrate the applications for better security encryption for the stored biometrics to ensure it, which makes it even more challenging for an adversary to bypass the system and reset the password. We conclude our research with a comprehensive security solution for MAS that considers user friendliness and data safeguarding.**

***Keywords*—Transparent security; authentication; UX/UI; forgetting password; reset password; biometric systems**

I. Introduction

Considering the tremendous development in the use of mobile applications and the search for hacker-proof programs that are gathering momentum, security problems have become a feature in the developer's mind to the point of obsession. This endeavour goes hand in hand with the need to enhance the user experience through user-friendly products in times of unprecedented demand for programs that combine security with simplicity and fun. To this effect, the duality 'Security' and 'Usability' operate as an interdependent set of elements, which the developer must incorporate with equal measure. The implications of failing this key operational balance between "Security" and "Usability" will most likely lead to a lack of security or to some difficulties in using the application.

For almost two decades, authentication has been a prominent issue in usable security research. The majority of these studies have concentrated on passwords and other similar authentication techniques that rely exclusively on a shared secret between the user and the computer system. Passwords must be strong enough to prevent guessing and must be memorable enough to not need to be written down. They must also be easy to type and lengthy enough to prevent guessing [1].

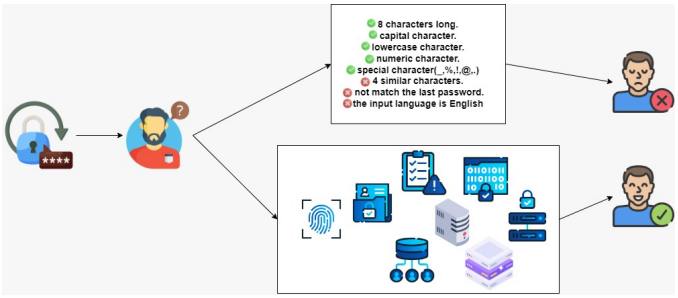

Fig. 1. Password vs. Fingerprint in an Authentication Process.

Transparent security related to mobile authentication can be implemented by physiological biometrics especially using fingerprint. In fact, the fingerprint is rare and difficult to obtain without the consent of the owner. It is also easy to adopt the fingerprint in giving access to the user with authority, as it is considered one of the most popular modern methods, which have been conducted multiple researches measuring the feasibility of this method in terms of ease of use and certainly security [2].

In Fig. 1, it is clear how the traditional method is complicated in resetting the password. For example, the user must not use the same password as the previous and that it is not identical to the name of the user and not to his personal data like date of birth. Also, it must contain symbols, uppercase and lowercase letters, and be at least eight digits long. On the other hand, you only need to pass your finger over the fingerprint sensor and in light of the unique data of the fingerprint. It is safe and has reliable features in its use to give access, Thus, using fingerprint in authentication satisfies the security measurements in a transparent manner. In most cases user do not feel what is happening in the background The system consists of very complex calculation in image processing and fingerprint Features extraction to verify the fingerprint provided by the user to give him access [3].

Although it is not in a user's interest to forget his password, many have done so. The age factor and how it affects the user's memory box, or the need to create as complicated a password as possible to keep the adversary at bay can inadvertently cause a person to forget their password. Either because we may have forgotten our password or due to a security breach, we find ourselves compelled to. As cybersecurity researchers, we must

use all possible means to make this process as secure and user-friendly as possible. Using biometrics that cannot be forgotten or stolen like a security token is one way, the other entails adding another layer of security encryption which must be applied on the stored biometric to ensure it will be even harder to bypass the system and reset the password. As a solution to this ongoing issue, we propose a system that will solve the common problems users face when starting the reset password process.

II. Background and Related Work

A. Transparent Security

Transparent authentication systems for mobile devices can be classified based on whether they use physiological biometrics such as fingerprint scanning or face recognition, or behavioral biometrics such as keystroke touch or walking rhythm. Physiological biometrics are widely regarded useful because they require a lot of computational power and high-quality photos, which are difficult to breach. Iris recognition, for example, requires the user to face the camera, takes longer to authenticate, and requires expensive additional hardware. Furthermore, iris recognition still faces obstacles such as detection, segmentation, coding, and matching [2]. Fingerprint recognition, on the other hand, with the progress of the smart phone industry and the adoption of technologies that provide users with a unique experience for their devices, does not face these obstacles. We find that most modern devices include a fingerprint sensor, and from this comes our focus in this paper on using this sensor to build a password reset system using the fingerprint, which is considered a transparent authentication system.

B. Usability vs. Security

Usually, the security part is sacrificed to complete the user experience part, and vice versa. The proposed idea is a balance between the two, leading us to the term "Transparent Security" intended to complete the security process so that the user does not feel the existence of complex security operations and where some waiting is required for the completion of these processes, usability techniques can be used to make waiting not boring by using usability emotional design. If the system is difficult to use, users will avoid using it. It must be taken into consideration that the effective use of applications and programs requires the programmer to implement usability while designing any program because that will affect efficiency and performance when using the program. The design of effective applications should consider the language, cognition and social interpretations of the user and the community. The word "Usability" also refers to methods for improving ease-of-use during the design process. Usability is defined by five quality components: learnability, efficiency, memorability, error, and satisfaction [4].

Security and usability are acknowledged as working in conjunction. There are examples of security and usability disputes, and these involve: password creation complexity instructions which will be hard to memorize, the enforcement of password masking to save passwords from being compromised, which sacrifices usability [5]. Information security is the defence of individuals, communities, or national interests, along with their information and noninformation-based properties, from the risks associated with their interactions with cyberspace. Users and their communities are among the properties that must be protected. Several security professionals and countries are now recognizing the need for users to be more informed and informed about information security [6].

C. Forgetting Problem

Forgetting is part of contextualization and guides immediate and potential information processing by encouraging environmental exposure and ensuring that knowledge is up to date, enabling timeliness and up-to-date [7]. The problem of forgetfulness cannot be overcome, as it is part of human nature. Therefore, different application developers must consider this human characteristic. As a result of Carnegie Mellon University password security research [8], strong passwords are not easy for users to implement and memorize, the problem is aggravated by users needing to implement and memorize special passwords for all online accounts they use. Joseph Bonneau and his colleagues evaluated 20 years trying to find a password-alternative proposition. They created a collection of 25 criteria that concerned usability, security, and deplorability and used them to assess different authentication methods. They concluded that there are no password alternatives that offer many advantages over conventional passwords. Furthermore, many did not meet a sufficient range of real-world constraints as password alternatives.

D. Password Resetting

Among the things used to reset the password is CAPTCHA [9]. This requirement is meant to ensure that the user is a real person, but the system is greatly affected by the user's experience in terms of clarity and ease of reading and may face challenges in determining the content displayed in front of him/her. These challenges sometimes impede the user from passing the selection point or force them to spend considerable time trying to pass beyond that identification test. Let us not forget, users may be of different ages, may have a low level of education and do not understand English, the preferred language by developers in use by CAPTCHA. The presence of vague characters is also another type of word blindness, which also leads to the character not being specified due to the overlap between the letters, and many of the examples are mentioned in discussing this method. However, the problem in terms of usability refers to the oversight of developers in failing to address the issue of age when designing their systems. The implications indicate neglect of certain age groups. For example, if the user is in an advanced age group, can CAPTCHA be made less challenging than the one designed for younger users? Moreover, there lies a challenge and what if the user is of Arab stock with no knowledge of the English script and is yet expected to answer questions written in English. Here lies a challenge that is too great to overcome. The main problems in this method can be summarized as follows:

1) Distortion issues.
2) Content issues.
3) Presentation issues.
4) Location and position.

The graphic design [10] of the password is used to make it more memorable, user-friendly, and secure. Put simply,

TABLE I. COMPARISON BETWEEN FINGERPRINT AND FACE RECOGNITION

Biometric System	Fingerprint	Face Recognition
Universality	Medium	High
Uniqueness	High	Low
Permanence	Medium	Medium
Collectability	High	High
Performance	Medium	Low
Acceptability	Medium	High
Circumvention	High	Low

the user presses the shape based on which he created the password and then logs into the system. The focus was on usability, and the goal was to test the user experience for the picture password. The questionnaires were used as a tool that covered many users of different categories, including age groups and cognitive achievement. The main argument for graphical passwords is that humans are better at memorizing graphical passwords than alphanumeric character passwords.

III. WHY FINGERPRINTS

There are seven features that determine biometric advantages: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention [11]. The concept of universality states that we can always be successful in finding our desired biometric features in the number of people who will be enrolled in the system. The term uniqueness refers to the number of distinct features a person has among people. Permanence is the evaluation of how far a unique set of characteristics endures or variates over time with maturity level. The concept of collectability refers to measuring how quick and easy it would be to obtain features that can be used to verify identity. Performance refers to a collection of measurements used to evaluate how well a given set performs. Speed, accuracy, and error rate are examples of these measurements. The acceptability of using biometrics evaluates how adequate and satisfiable it is. Circumvention refers to the ease with which a system can be fooled by a forged biometric feature. In mobile devices, the most widely used biometric sensors are fingerprint and facial recognition sensors [12].

The fingerprint is unique even in twins, it will be different and is distinct from one person to another. However, it can be forged like a dummy finger, new technologies have emerged which eliminate this problem by adding some pulse detector and temperature sensor. The fingerprint is a suitable biometric system, as shown in Table I, because it is hard to collect without user cooperation. In face recognition, it has a uniqueness problem due to the similarity between siblings, especially in a twins situation, and that will cause a problem if someone tries to access a system using face recognition like twins. Bad performance depends on many factors, such as the accuracy and speed to analyze. One of the problems of face recognition is that any person may get the face template of someone else from a far distance by using a super-zoom camera that captures long-distance shots, which causes alarming concerns. On the basis of these facts, it is suitable to choose a fingerprint as a biometric system in our proposed system because it will add a security layer and be easy to use and store.

IV. USER EVALUATION OF CLASSIC PASSWORD RESET

Interviews were conducted to evaluate the classic resetting password for various systems as presented in Fig. 2. Each system was developed with different types of password reset methods. The target participants we had interviewed use internet services for various purposes. Most of the usage orbits around browsing to benefit from the services provided on the Internet and to communicate with family and friends through social networking applications. Since social networking sites and other websites store cookies on user devices, the user does not log in by entering his/her username and password, often which means forgetting what they are. Participants in the interviews indicated that they may periodically reset the password, every six or twelve months, and look at the expiration date of the cookies. Therefore, most sites usually leave the configuration for this feature as default, which indicates the period for storing the cookies from six months to a year. Another factor that may cause a password to be forgotten is a different password for different platforms. To avoid the forgotten password, as most of the participants stated that they use the same password on more than one platform and app.

We want to explore the experiences of technical and non-technical Internet users with existing internet services for various uses. The goal is to determine what conditions may require the user to reset their password and what will make this process easier and more secure while saving the user time. The findings of the interviews conducted are as follows:

- The factors that motivate participants to change their password: some participants who may be either technically oriented users or plainly nontechnical change their passwords because they merely memorize their password to keep it safe.
- Degree of satisfaction with the reset password process (0-10): Most participants rated the process of resetting a password below 8 and this tells us that they did not reach their expected level of satisfaction due to the complex methods of resetting password, they feel the operators subject them to.
- The length of time it takes participants to reset a password: The method used in such a process consumes longer time, than the generally expected norm. This depends on the mechanism of resetting passwords, which affects the efficiency even though users understand the importance of the long-time process.

V. THE PROPOSED FLEXIBLE TRANSPARENT AUTHENTICATION SYSTEM

In the proposed system, our goal is to improve the quality of the user experience by using modern techniques such as biometric systems. In the sign-up phase, the system will ask a new user to enter their name, email address, mobile number, password and fingerprints, as shown in Fig. 3 and the Algorithm 1.

In the in-session log-in, it will ask for two things, the email address of the account and the password to gain access to it. If the user has forgotten his/her password, the user will select the forgot password batten. In this phase, there are few fields to complete. First, enter the account email address, then the

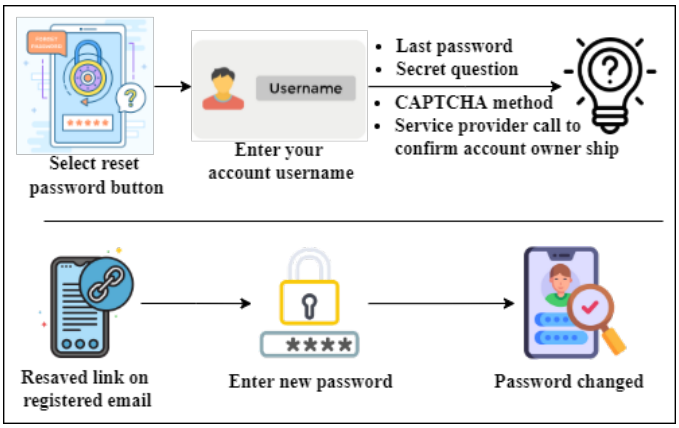

Fig. 2. Classic Password Reset Process.

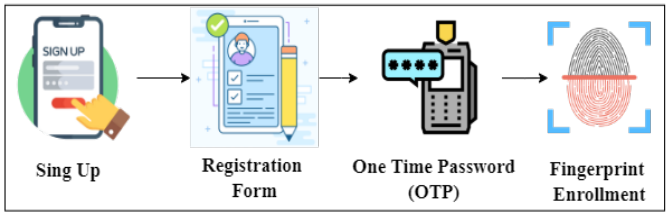

Fig. 3. Sign-Up Process.

user will get an OPT code (a temporary code sent to the user's phone) to confirm that the person trying to reset the password is the owner of that account. After that, the user will have the choice to choose from two methods to reset the password:

1) Fingerprint: if the user chooses to reset the password using the fingerprint method, the user will place it on the scanner, for the system will match the template. If the template matches, then the system will directly open the reset password page, explained in Fig. 4 and Algorithm 2.
2) Email address: if the user chooses the email address, the system will send a link to the user's email to reset the password. For a degree of flexibility that will support both usability and security, the proposed system has two methods for the user to choose from. It eliminates considerable problems by adding security layers and improving usability. Users may suffer from blurred vision, as in entering vague characters during the CAPTCHA test to reset password. Even users who have no blurred vision problem will feel discomfort when trying to enter vague characters during the CAPTCHA phase.

Biometrics, especially fingerprints, are widely used among other biometric systems in authentication tests. Most systems save the user's unique template of minutiae directly in the database as a special template for the user, which can be exposed to a possible attack. This unique and limited information is exposed to danger, as it is possible to reconstruct the fingerprint from the leaked information. To this end, there is a need to urgently enable protection of this information [13].

The hash algorithm is a complex mathematical function that transforms a collection of inputs into an apparently random output string of fixed length, so the same input string will always produce the same output string [14]. However, if the input string has changed even by just a single character, then the output string will be entirely different. Ordinarily, encryption implies incidentally scrambling information until a key is utilized to unscramble it. Hashing is frequently seen as a form of one-way encryption as you cannot go back from a hash to work out the first string; you can only go forward. In our proposed system, we read a fingerprint and then analyze the fingerprint and use base-64 hash to convert it into ciphertext. To avoid storing this ciphertext, we have treated this ciphertext as a password in terms of storing it in the database. Thus, we adopt an extra layer of security to hash the ciphertext using SHA-1 to satisfy the privacy of the user's fingerprint.

We utilize the salts technique to further thwart any rainbow table attack. Salts are short random sets of characters that are appended to the ends of a user password before they are hashed. Salts are automatically added after the user provides the fingerprint. Salts are generally stored in plaintext along with a hashed output, so the system knows which salt to use in regard to verifying a reset password.

Algorithm 1 Sign up using Fingerprint

```
Read User Email
Read Mobile number
Read Password
while not valid password do
    Read password
end while
password hashing(password)
send OTP to mobile
Read sent OTP from user
counter = 0
while is note valid OTP or counter < 3 do
    ** reenter the OTP message **
    Read sent OTP from user
    counter = counter + 1
end while
Read Fingerprint1 as Binary array
match rate = 0
while match rate < 75 do
    Read Fingerprint2 as binary array
    calculate match(Fingerprint1, Fingerprint2)
end while
match rate = 0
while match rate < 75 do
    Read Fingerprint3 as binary array
    calculate match(Fingerprint1, Fingerprint3)
end while
Encoding Fingerprint1 to Base64
Hashing Fingerprint1 SHA-1
Saver(email, mobile, password, Fingerprint)
```

VI. Experiment Results

We evaluate a simulated application of our proposed system so that we can have feedback about it while testing the usability of the system. The simulated application has been tested by eight participants. The average time to reset the password

Algorithm 2 Reset Password using Fingerprint

```
Read User Email
get mobile from storage
send OTP to registered mobile
Read OTP
counter = 0
while is not valid OTP or counter < 3 do
    ** reenter the OTP message **
    Read sent OTP from user
    counter = counter + 1
end while
get fingerprint from storage
is Match = False
while Match = False do
    Read Fingerprint as binary
    Encode Base64(user Fingerprint)
    Hashing Fingerprint1 SHA-1
    Match(user Fingerprint, Fingerprint from storage)
end while
Read New Password from user
hashing new password(new password)
update(password, new password)
```

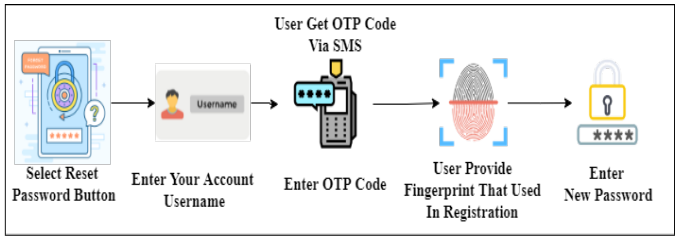

Fig. 4. Reset Password Process.

using the proposed system is 22 seconds that satisfies the user's experience without compromising the security, unlike the classical resetting system, which takes much time due to the challenge response system via email or other system. The evaluation gives us positive results on a lot of usability concerns, as presented in Fig. 5. These concerns included the time spent on the reset password process and the complicated process. 75% of the participants agreed on how easy and fast the password reset process is, while 100% agreed on the simplicity of the password reset process. Table II illustrates samples of participant's feedback.

TABLE II. SAMPLES OF PARTICIPANT FEEDBACK

Questions	Samples of Participant's Feedback
Differences between the classic resetting password and the proposed system.	'Many steps were shortened in the proposed system.'
	"Resetting the password in the proposed system is much easier than the available methods found in most of systems.'
	'In the proposed system, there is no need to leave the system, like email or SMS, and then through a link to do reset password.'
Is the proposed method tedious to reset password	'The proposed method is easy and not tedious'.
	Tow participants show concerns about saving the fingerprint template, whether or not it is safe.
Time	"It took short time".
complexity	"There is no complication".

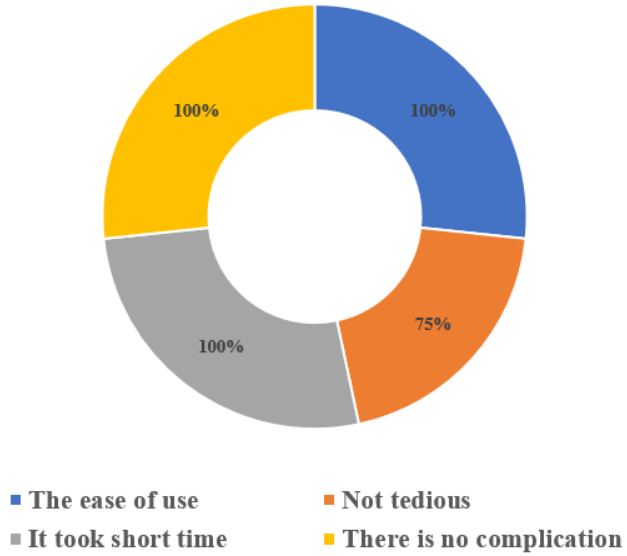

Fig. 5. Satisfaction Level of the Proposed System.

VII. CONCLUSION

Forgetting the password is a problem that exists and continues, it is part of human nature. The traditional method of resetting the password relies on increasing complexity, such as secret questions, which may affect the user experience. We propose a simulation of user authentication and the experiment includes a password-reset process. We use a fingerprint reader to emulate the mobile fingerprint sensor. Based on the simulation and evaluation results, the proposed system has several advantages over the challenge-responding system. The proposed system meets the security needs and at the same time provides usability. The user experience has a very large impact on usability. In the proposed system, to avoid direct saving of the template for the user's fingerprint, we encrypt the fingerprint and then use the Salt algorithm to be immune from decryption using available tools such as john the ripper and rainbow table. The new method of resetting the password gave us positive results in terms of usability and security. In the future, we are going to investigate the impact of biometric features in large scale systems and domains.

REFERENCES

[1] M. Theofanos, S. Garfinkel, and Y.-Y. Choong, "Secure and usable enterprise authentication: Lessons from the field," *IEEE Security & Privacy*, vol. 14, no. 5, pp. 14–21, 2016.

[2] S. Alotaibi, S. Furnell, and N. Clarke, "Transparent authentication systems for mobile device security: A review," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 406–413.

[3] H. Chen and G. Dong, "Fingerprint image enhancement by diffusion processes," in *2006 International Conference on Image Processing*. IEEE, 2006, pp. 297–300.

[4] J. Nielsen, "Usability 101: Introduction to usability (2012)," *URL: http://www. nngroup. com/articles/usability-101-introduction-to-usability/[Accessed November 2016]*, vol. 9, p. 35, 2012.

[5] O. Kulyk, S. Neumann, J. Budurushi, and M. Volkamer, "Nothing comes for free: How much usability can you sacrifice for security?" *IEEE Security & Privacy*, vol. 15, no. 3, pp. 24–29, 2017.

[6] R. Reid and J. Van Niekerk, "From information security to cyber security cultures," in *2014 Information Security for South Africa*. IEEE, 2014, pp. 1–7.

[7] S. Nørby, "Why forget? on the adaptive value of memory loss," *Perspectives on Psychological Science*, vol. 10, no. 5, pp. 551–578, 2015.

[8] L. F. Cranor and N. Buchler, "Better together: Usability and security go hand in hand," *IEEE Security & Privacy*, vol. 12, no. 6, pp. 89–93, 2014.

[9] S. M. R. S. Beheshti and P. Liatsis, "Captcha usability and performance, how to measure the usability level of human interactive applications quantitatively and qualitatively?" in *2015 International Conference on Developments of E-Systems Engineering (DeSE)*. IEEE, 2015, pp. 131–136.

[10] A. M. Eljetlawi, "Graphical password: Existing recognition base graphical password usability," in *INC2010: 6th international conference on networked computing*. IEEE, 2010, pp. 1–5.

[11] S. Pankanti, A. Jain, and L. Hong, "Biometrics: Promising frontiers for emerging identification market," *Comm. ACM*, pp. 91–98, 2000.

[12] J. ANDRESS, "Chapter 2–identification and authentication," *The Basics of Information Security (Second Edition). Se cond Edition. Boston: Syngress*, pp. 69–88, 2014.

[13] S. S. Ali, V. S. Baghel, I. I. Ganapathi, S. Prakash, S. Vu, and N. Werghi, "A novel technique for fingerprint based secure user authentication," *IEEE Transactions on Emerging Topics in Computing*, 2021.

[14] F. E. De Guzman, B. D. Gerardo, and R. P. Medina, "Implementation of enhanced secure hash algorithm towards a secured web portal," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 2019, pp. 189–192.