Usability Testing of Memorable Word in Security Enhancing in e-Government and e-Financial Systems

Hanan Alotaibi, Dania Aljeaid, Amal Alharbi
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia

***Abstract*—Most applications increase their security by adding an extra layer to the login process using two-factor authentication (2FA). In Saudi Arabia, One-Time Password (OTP), which is 2FA, is the most common method used as users log in to their accounts. However, some issues have emerged with using OTP as 2FA; these issues from previous research were investigated in the study. Also, the study proposed a new method of account authentication, which is a Memorable Word (MW). MW is the second and short password in which the user enters a certain number of characters instead of the whole password. The study conducted usability testing to compare two 2FA methods, OTP and MW. The study included 60 participants logged into a simulated website using both authentication methods. Then, all participants have to complete the questionnaire. The collected data analyses showed a favourable opinion of the MW method.**

Keywords*—Security; usability testing; two factor authentication; one time password; memorable word

I. Introduction

The digital world is a rapidly evolving landscape, and using e-Systems is becoming increasingly commonplace. e-Systems are electronic systems that allow users to access, store, and share information and data. These systems are used in various ways, from e-government and online banking to social media, and they are becoming an integral part of our lives. e-Government has the potential to modernise the way governments interact with citizens and provide services. It can give citizens access to government services and information more efficiently and cost-effectively [1]. It can also help governments to manage their resources better and improve the delivery of services. e-Government can help reduce the administrative burden on government employees and improve the transparency and accountability of government services [2, 3, 4]. For instance, the government of Saudi Arabia has taken a proactive approach to ensure the security of its e-government systems. The Saudi e-government security policy is designed to protect data resources from a wide range of risks, including malicious attacks, unauthorised access, and data loss, by implementing aspects of the data security [5].

Similarly, e-financial services in Saudi Arabia have seen a significant shift in recent years as banks have offered more innovative services through online banking. This shift has enabled banks to maintain their market share and gain customers as online banking has become increasingly popular [6]. However, this digital transformation to systems poses several challenges and security threats. For example, it can be difficult to ensure that systems are reliable and resilient in the face of cyber-attacks and other threats.

However, with the increased use of systems comes an increased risk of security threats. Cybercriminals are constantly looking for ways to exploit weaknesses in these systems and expose sensitive information such as social security numbers or verification numbers sent to e-mail addresses or contact numbers [7, 8]. Cybercriminals use a variety of methods to accomplish successful cyberattacks, which include phishing, malware, and ransomware attacks, as well as data breaches. To protect against these threats, it is essential to implement strong security measures in place within systems. This includes keeping software and systems up to date, which can help prevent vulnerabilities from being exploited. It is essential to be aware of the latest security threats and to take steps to protect against them. Moreover, using strong passwords, multifactor authentication, and encryption are essential fields [9]. An authentication system is deployed to ensure that both parties involved in the communication are authentic ones. The dominant form used in various authentication systems is based on username and password. Nevertheless, passwords can be easily guessed if it is weak or stolen, so it is significant to use additional security measures. One of the most common methods used to increase the security of authentication is to adopt two-factor authentication (2FA). Implementing 2FA for end users can provide organisations with several benefits, including increased security and improved user experience. Recent studies found that 2FA can help protect user accounts from unauthorised access and malicious actors and reduce the risk of data breaches [10, 11]. However, it can also pose some challenges and complications. For example, implementing 2FA can be difficult and costly, as organisations need to invest in the necessary infrastructure and technologies to support the authentication process. Additionally, users may find entering their 2FA code tedious and time-consuming [10, 12]. Thus, this research studies the implementation of Memorable Word (MW) as a 2FA and evaluates its security efficiency and usability.

The main contribution of this paper is to investigate the users' perspective when accessing Saudi systems, such as government and bank websites, using MW instead of the current authentication method, SMS One-Time Password (OTP).

The rest of the paper is organised as follows: Sections II describes the common methods used in authentication while Section III highlights recent works related to usability testing

in authentication, followed by methodology in Section IV. In Section V, exhaustive experiments are conducted to validate the MW. In Section VI, the results of the experiments are discussed. Lastly, the paper is concluded along with the limitations and future work in Sections VI and VIII, respectively.

II. Authentication Methods

Due to the increasing number of cybercrimes, traditional username and password authentication methods are no longer enough to protect sensitive information from malicious actors. Businesses and individuals must take additional steps to secure their data. Multi-factor authentication (MFA) is one of the most effective methods for protecting sensitive information. MFA requires users to provide two or more pieces of evidence to prove their identity. This could include a combination of something the user knows (such as a password), something the user has (such as a physical token or smartphone), and something the user is (such as a biometric scan) [13]. 2FA is one of the most common authentication methods. It is a security measure that requires two different authentication factors to verify a user's identity. It is used to protect sensitive information from unauthorised access and is becoming increasingly popular as a way to protect against data breaches. The two factors used in 2FA are typically something the user knows (e.g., a password or PIN) and something the user has (e.g., an OTP, token, or digital certificate). This combination of factors makes it much more difficult for an attacker to gain access to a user's account, as they would need to know both the password and have access to the physical device or token. 2FA is a great way to protect against phishing, brute force attacks, keylogging, and credential theft attacks. It is also a great way to protect against data breaches, requiring two different authentication factors to verify a user's identity. There are several different types of 2FA, such as OTP-based and Biometrics-based. OTP-based 2FA requires users to enter an OTP valid for a single login session. Biometrics-based 2FA requires a user to provide a biometric factor such as a fingerprint or iris scan [6]. Several different 2FA methods exist, such as SMS, Time-Based One-Time Password, Pre-generated Codes, Push, and Universal Second Factor Security Keys. Each method has advantages and disadvantages, as discussed in the following subsections.

A. SMS Token / SMS-based Authentication

SMS-based authentication is one of the most common methods of 2FA, and many organisations use it to protect their users' accounts and systems. In SMS-based, a one-time verification code is sent to the user via a text message to their mobile phone. This code is usually six digits long and is used to verify the user's identity. The user then enters the code into the system to gain access. This code is only valid for a short period of time, usually a few minutes, and it must be used within that time frame, or it will expire. It is easy to use and requires minimal effort from the user [6, 14]. However, SMS-based 2FA is not without its drawbacks. It is vulnerable to SIM-swapping attacks, where an attacker can access the user's phone number and intercept the verification code. It is also vulnerable to phishing attacks, where an attacker can send a fake text message with a malicious link that leads to a fake website. SMS messages can take a long time to arrive, and they can be blocked or delayed by network congestion because they are delivered over cellular network standard SMS. This can be a problem if users need to access their accounts quickly [15, 14]

B. Time-Based One-Time Password

Time-based one-time password (TOTP) is an alternative to SMS-based 2FA that provides an additional layer of security for online accounts. It generates a unique, valid code for a limited time, usually 30 seconds. This code then authenticates the user's identity [6, 16]. Yet, there are some drawbacks to using it. One of the main drawbacks is that it can be challenging to use. The user must have access to the device generating the code, such as a smartphone or a hardware token. This can be inconvenient for users who do not have access to the device or who do not have the time to wait for the code to be generated. Another drawback is that TOTP codes can be vulnerable to replay attacks. This is when an attacker captures the code and uses it to gain access to the account. To mitigate these attacks, it is essential to use a secure connection when generating the code and ensure that it is not stored in plain text. Finally, TOTP codes can be challenging to remember. This can be a problem for users not using 2FA [17].

C. Pre-Generated Codes

Pre-generated tokens are an effective backup 2FA method if the user cannot access the primary 2FA method. This method is relatively straightforward to implement, as the service provider simply creates a list of verification codes and asks the user to print or write down the codes. The list length is variable; the codes are usually about eight digits long. Tokens can be used in any order and must be kept secure by both the server and the user to prevent theft. Since these codes are usually longer than codes sent via SMS or generated using TOTP, there is additional room for user error when entering codes. Moreover, the user must be careful not to lose the broker on which they registered the codes, and they will be vulnerable to an offline brute force attack [6].

D. Push

Push authentication requires the user to receive a push notification on their smartphone to approve or deny a login attempt. This method is advantageous because it eliminates the need for users to type in numbers, as required by other 2FA methods, making it both faster and more user-friendly [18]. Additionally, push authentication requires Internet access, which is necessary to keep communication between the user's device and the server secure, such as through TLS. However, the most prominent push-based authentication methods are proprietary, making it difficult to verify the exact security measures in place and require implicitly trusting a third party [6]. Furthermore, push-based authentication has not yet been well-studied by the security community, making it difficult to assess the security of this method.

E. Universal Second Factor Security Keys

Universal Second Factor (U2F) Security Keys are an open standard for authentication through a USB device. The user must connect the device to the computer to authenticate with a security key and activate the device when the website requests.

U2F Security Keys are designed to be more secure than traditional 2FA methods, such as SMS or email-based authentication. One of the main drawbacks of U2F security keys is that they can be challenging to set up and use. U2F security keys require users to install a particular driver on their computer or mobile device to use them. This can be a time-consuming process, and it can be difficult for users who need to be tech-savvy. Additionally, U2F security keys are incompatible with all devices and can be expensive. Besides, U2F security keys can be lost or stolen, which can be a significant inconvenience for users who need to replace them [19].

F. Memorable Word Technique

The Memorable Word (MW) is a short password (usually assumed to consist of one word) and is one of the layers of authentication, where the MW differs from the password in how it is used; instead of entering the whole MW, the user enters a certain number of MW's characters, usually, three letters and the letters to be entered vary each time the user is asked to enter it. Initially, the client and the server know a short password of length m characters that has been shared before. During authentication, the server sends unique numbers between 1 and m to the client. The client responds with the letter in each corresponding position in the password. If all these characters are correct, the authentication succeeds; otherwise, it fails [20]. It has been recognised that transaction systems must include authentication and data encryption. To complete these requirements, MW has been proposed to contain mutual authentication and data encryption using the symmetric algorithm that improves the security of existing transactions. Symmetric encryption is employed in transactions to prevent identity theft of clients or banks—additionally, user authentication and authorisation to protect against cyber-attacks [21, 22].

III. Related Work

Usability testing can help identify areas for improvement in the system, such as user experience and security, which can help improve the system's overall performance. Furthermore, usability testing can help to identify any areas of confusion or difficulty that users may need help with when using the 2FA system. This can help improve the user experience by making the system easier and more convenient. Usability testing is one of the preferred methods for assessing user experience with 2FA due to its ability to provide direct feedback from users [11]. Das et al. [23] suggest that usability testing can be used to evaluate the effectiveness of 2FA systems and identify potential usability issues. This type of testing often includes a series of tasks to measure user performance and satisfaction with the 2FA process. Other evaluation methods, such as surveys, interviews, and focus groups, provide additional insight into user experience with 2FA [11]. Gunson et al. [24] found that usability testing was the most effective way to evaluate 2FA due to the complexity of the task and the need to ensure that users understand and follow the authentication process correctly. However, they also identified several challenges in implementing usability testing. These include finding a representative sample of users, developing suitable test scenarios, and ensuring that the test results are valid and reliable. According to a study by Golla et al. [24], implementing 2FA for end users can provide organisations with several benefits, including increased security and improved user experience. The study found that 2FA can help protect user accounts from unauthorised access and malicious actors and reduce the risk of data breaches. Additionally, 2FA can provide users with an improved experience when logging into their accounts, as they can be quickly and easily authenticated. However, while 2FA can provide organisations and end users many benefits, it can pose some challenges. The study found that implementing 2FA can be difficult and costly, as organisations need to invest in the necessary infrastructure and technologies to support the authentication process. Additionally, users may find entering their 2FA code tedious and time-consuming [24]. As such, organisations must be aware of these challenges and take steps to ensure that their implementations of 2FA are secure, efficient and user-friendly. Abbott and Patil [12] explored the potential for improving user experience through 2FA. They found that 2FA can enhance security, provide users with greater confidence in the service, and provide a better overall user experience. Through their study, the authors found that users are more likely to remain engaged with services that use 2FA as they feel more secure and trust the service provider. Furthermore, they noted that 2FA can be tailored to the individual user's needs, which can help to improve user experience by providing them with a more tailored experience.

The usability dimensions of ISO 9241-11 form the basis for measuring user experience based on the three usability dimensions, which are efficiency, effectiveness, and satisfaction. Efficiency focuses on the amount of time taken to complete a task, effectiveness is the ability to complete a task, and satisfaction is the user's opinion of the convenience and acceptability of the system, which is measured by the System Usability Scale (SUS) [25]. Factors impacting each usability dimension can be documented, such as the time it takes to complete a task or user demographic information. Collecting this information can help developers and designers create and improve the 2FA MW systems [26]. SUS is a tool that has become increasingly popular in the field of usability testing. Developed by John Brooke in 1986, SUS is an efficient and cost-effective way to measure the usability of a system. The tool has been used in a wide range of studies and has consistently produced reliable results. Additionally, SUS is a popular option for usability testing because it is efficient and cost-effective. It is a straightforward tool that can be administered quickly and easily.

Weir et al. [27] compared the usability of three two-factor authentications: push-button tokens, card-activated tokens, and PIN-activated tokens. The study aimed to measure the time required for authentication and user satisfaction. Their findings were that user prefers authentication methods which are easy to use rather than security; however, quality and usability decreased when additional levels of security were required.

An exploratory comparative investigation study conducted by [28] into the usability of 2FA. The study assessed and compared the usability of three widely used 2F solutions: security token-generated codes, OTP delivered through email or SMS, and dedicated smartphone apps like Google

Authenticator. Also, they investigated motivations behind users' choices and examined how these factors influence their perception of usability. The finding from the study indicates that 2FA are widely accepted and highly usable. This means that users are embracing the user of additional layer of security beyond just password. The study also highlights that user opinions of 2F usability are frequently connected with individual attributes. This suggests that different users may have varying levels of comfort or experience with using 2FA, which can influence their perception of its usability. Moreover, the study reveals that the trustworthiness of 2F is positively correlated with ease of use.

In a study conducted by Reese et al. [29] the usability of five 2FA methods was examined. The study aimed to compare the usability of Pre-generated Codes, Push, SMS, OTP, and U2F Security Keys. The sample consisted of 72 participants who logged into a simulated banking website using 2FA. The objective was to gain insights into users' perspectives on 2FA and assess their experiences with different authentication methods. The findings showed that the majority of participants expressed a desire to use 2FA as a means to enhance the security of their sensitive online accounts. However, it was noted that some participants encountered difficulties when utilizing these methods such as spending longer time at login phase, particularly with the OTP and U2F methods.

Our research is different from the previous studies as it focuses on the implementation of a new two-factor authentication (2FA) method, specifically the Memorable Word (MW), in Saudi Arabia's e-government and banking systems. The aim of our study was to examine the user perspective on utilizing MW as a 2FA method. To achieve this objective, a survey was conducted to compare the currently employed 2FA method in Saudi Arabia, which is One-Time Password (OTP), with the proposed 2FA MW method.

IV. Methodology

The study's first phase, as described in Sections II and III, involved conducting a literature review on authentication methods and usability. By thoroughly examining existing literature, gaps in knowledge were identified, highlighting areas that required further research. In the second phase, a website was developed to support both OTP-2FA and MW methods. To gain a deeper understanding of MW authentication, a questionnaire was conducted through a simulated webpage. Additionally, three expert reviews were obtained to ensure that the usability testing aligned with the study's objectives. The purpose of these interviews was to assist the authors in confirming the usability testing process. Afterward, a comprehensive questionnaire was constructed and administered to collect data on users' perspectives towards both OTP and MW methods. The research methodology, including the various phases and steps undertaken, is presented in Fig. 1.

The participants were assigned various tasks to perform on a simulated website and subsequently completed a survey. To ensure a smooth process, participants were initially scheduled for an appointment with a study coordinator. During this meeting, the coordinator provided necessary guidance and assistance to the participants in creating an account as the following steps:

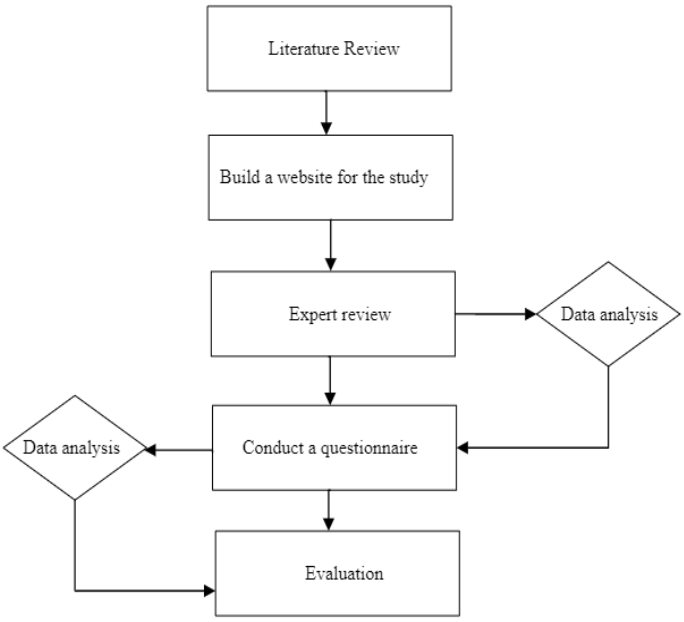

Fig. 1. Research methodology.

1) User registration: This step involved user registration, where the participants were required to provide their details, such as their name, phone number, and email address. Once registered, the participants were able to create their unique username and password. In addition, they were required to set up an MW with the following considerations:

- Six to eight characters long without spaces.
- Contains only letters (A to Z), excluding any numbers or special characters.
- It cannot be the user's first and last name.
- It should not include alphabetic sequences such as "QWERT" keyboard.

The participants were informed that they would need to remember three random characters from their MW, which they would be prompted to enter after providing their login credentials. Fig. 2 shows the creation MW page.

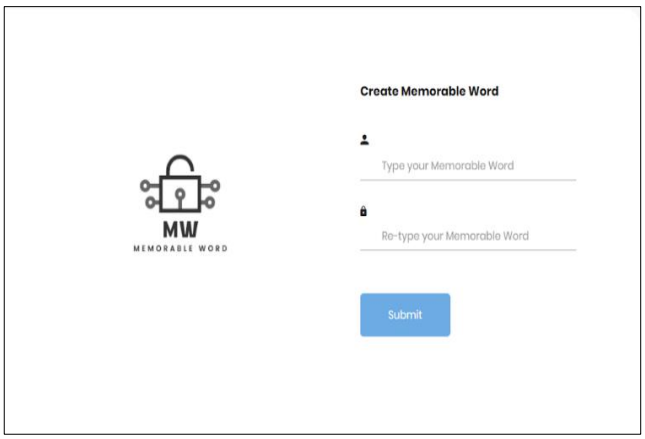

Fig. 2. Create MW page.

2) User log-in: The participants were prompted to log in to the website after successfully registering. To ensure that the participants were familiar with both authentication methods, they were instructed to initially select the OTP method and then log out and re-login using the MW method. This step was deemed necessary as it allowed the users to experience and become comfortable with both methods before proceeding to the next stage. Fig. 3 shows the login page, where the user can select the authentication methods. Fig. 4 shows the MW authentication page.

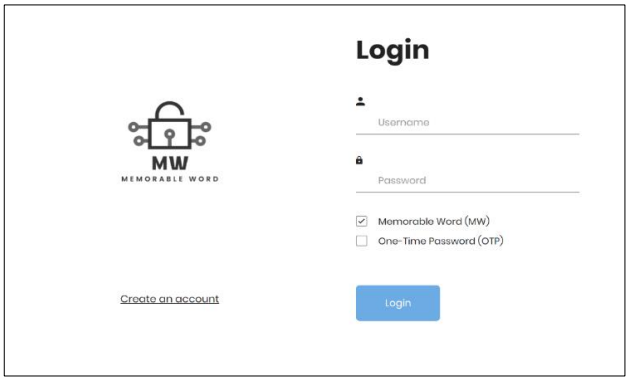

Fig. 3. Login page.

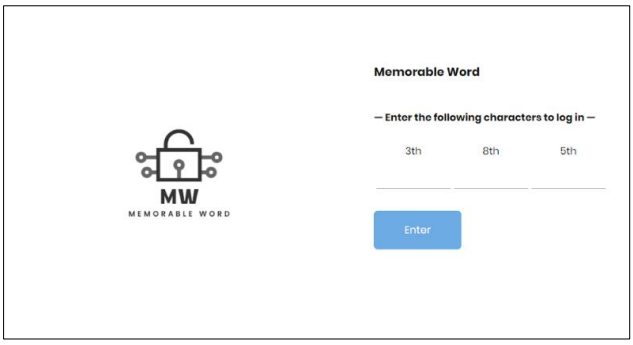

Fig. 4. The MW authentication page.

3) Survey questionnaire: Once the participants had completed the registration and login process, they were directed to answer a questionnaire. A total of 60 participants were recruited for this purpose, and they were randomly selected to ensure unbiased results. After two weeks, the collected data from the questionnaire was meticulously analysed, providing valuable insights and conclusions for further evaluation.

V. Results Analysis

The data was collected from 60 participants in a span of two-week. In this study, participants were asked to answer eight parts of a survey, each consisting of questions with different objectives.

A. Demographics/ Participants

The demographic data collected from the participants revealed a slightly higher number of female participants than male participants, with 62.5% and 37.5%, respectively. Additionally, the study showed that most participants were young adults, with 65.5% being between the ages of 18-29 years, 23.6% between 30-49 years, and only 10.9% between 50-69 years. The data also indicated that most participants had a bachelor's degree, accounting for around two-thirds of the participants (63.6%). Interestingly, all participants were familiar with using e-government and online bank systems, indicating their technological proficiency. However, it was also found that 100% of the participants had no prior knowledge of the MW method. To ensure that participants clearly understood the MW method, a brief description was given to them during the registration process through the simulated website.

Table I summarises the participant's demographics. As can be seen from the table, although the sample size is small (total = 60), overall, the study showed that the participants were diverse in gender, age, and education level, but their technological proficiency was high.

TABLE I. Participants' Demographics (Total = 60)

Gender	
Male	37.5%
Female	62.5%
Age	
18-29 years	65.5%
30-49 years	23.6%
50-69 years	10.9%
Qualification	
Secondary School	20%
Diploma	7.3%
Bachelor	63.6%
Postgraduate	9.1%
Familiar with using E-government and online bank systems?	
Yes	100%
No	0%
Familiar with Memorable Word?	
Yes	0%
No	100%

B. Timing Data

Login timing is an essential element in analysing user experience regarding systems. The study analysed the timing data of two authentication methods used for logging into a system: OTP and MW. The login time for two different methods was measured, counting the time from when the login page initially loaded to when the user submitted a password. To obtain reliable data, users were asked to repeat the login process ten times, five times for each method. Once all the data was collected and analysed, the findings revealed that users spent more time in the OTP method due to the delay in receiving the verification code. Fig. 5 presents the time spent in second to login to the system using both methods. Table II shows the mean time in seconds for both methods.

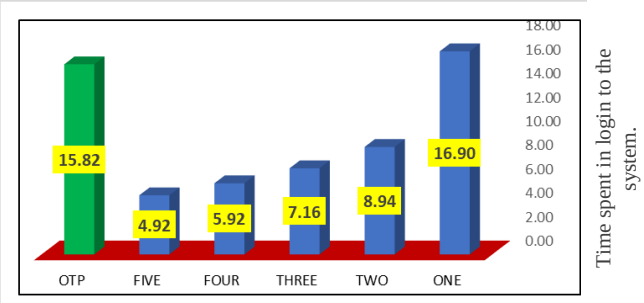

Fig. 5. The time spent to login to the system using both methods.

TABLE II. THE MEAN TIME IN SECONDS FOR THE TWO AUTHENTICATION METHODS

Method	Mean Time
MW	9.3
OTP	15.81

C. Individual Learnability

One of the objectives of the survey was to explore individual learnability. The hypothesis in this part of the experiment was that participants would become faster at validating their accounts with specific authentication methods as they become more familiar with them. To test this hypothesis, we computed a correlation between the time an individual spent in the session and the amount of time it took to validate their account using different authentication methods. The results showed a statistically significant difference between the two authentication methods (P-value ¡0.01). The MW method was found to be faster than the OTP method. This suggests that individuals can learn and become faster at validating their accounts with MW authentication methods over time.

D. System Usability Scale

The main goal of SUS is to evaluate a user's perception of a system's ease of use and overall usability. The SUS survey consists of nine tool questions with five-point Likert-scale answers. The survey is designed to gather feedback from users about how easy it is to use an MW authentication. To increase the reliability of the survey, four of the questions are phrased positively, while the other five are phrased negatively. This approach helps to reduce response bias and provides more accurate results. The results indicated that 98.18% of participants found the MW method easy to use for login, demonstrating high usability. Additionally, 94.91% of participants preferred the MW method to the OTP method. These results were all statistically significant and supported the hypothesis that the MW method was easy to use and preferred by users (P-value = 0.00 ¡0.05). Table III and Fig. 6 show the findings from each question.

E. Previous Experiences with Account Compromise and Worth Inconvenience

Participants were asked if they had ever faced difficulty logging in to their accounts regarding compromised online accounts. 12.7% of participants have an experience with remote attackers taking over their online accounts. Also, 52.7% know someone had an experience with remote attackers taking over their online accounts. Participants with previous experience and who know someone with an account compromised would be more likely to feel that an MW method was worth using. For worth inconvenience, the participants were asked to use MW as a second authentication is worth an extra step of login. 87.27% of participants felt using MW is worth an additional inconvenience.

F. Security and Inconvenience

The security and inconvenience factor was also investigated. Participants were asked if the MW authentication method made them feel more efficient and convenient to access their accounts than the OTP method. Most participants thought that the MW method was secure and convenient. The study showed that 92.36% of participants felt that MW was secure when logging into their accounts. Furthermore, 89.45% of participants found MW more convenient than OTP.

TABLE III. SYSTEM USABILITY SCALE ANALYSIS OF THE NINE STATEMENTS

		Statement	Mean	Standard Deviation	P-value
Statement Number	1	I find the various functions in this MW were well integrated.	4.95	0.23	.000
	2	I think the MW was easy to use.	4.91	0.55	.000
	3	I would like to use this MW frequently.	4.75	0.48	.000
	4	I think most users would learn to use this MW very quickly.	4.69	0.96	.000
	5	I find the MW is complex.	1.51	0.84	.000
	6	I find the MW is hard to use.	1.51	0.84	.000
	7	I think I need support to use MW.	1.45	0.54	.000
	8	I need time to learn how to use MW	1.38	0.97	.000
	9	I think there is inconsistency in using MW.	1.11	0.57	.000

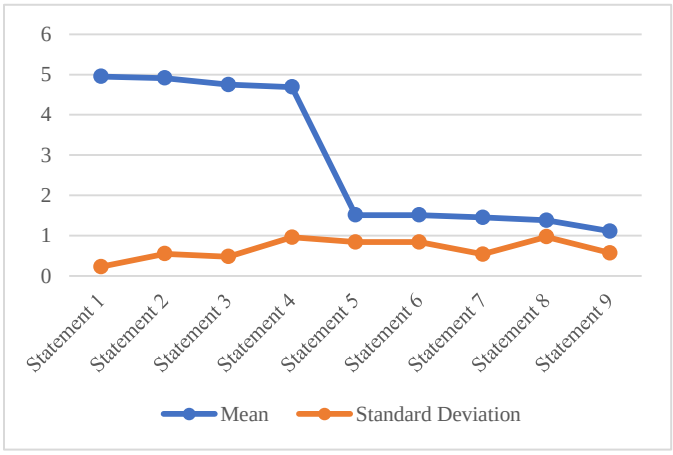

Fig. 6. System usability scale analysis of the nine statements.

G. Perception of Likelihood for Account Compromise

Participants were asked how much value they placed on their online accounts, such as bank and government accounts, to investigate whether they felt the need to protect their information and data. The results showed that 92.5% of participants expressed that they needed to secure their accounts from others, while 7.5% felt that there was nothing essential to protect.

H. MW Timeout

After a week of creating an account on the simulated website, the participants were asked to log in to their account using MW as an authentication factor to test their experience using the proposed method if they needed help entering randomly selected letters. The result is that 94.91% of participants logged into their accounts without any mistakes; before time out; also, 97.82% found MW easy to use. 96.36% of participants agreed with the statement, "I did not struggle in using MW as much as struggling in OTP".

VI. Discussion

The main contribution of this study is to investigate the users' perspective when accessing Saudi electronic systems, such as government and bank websites, using MW instead of the current authentication method, SMS OTP. The study found a favourable opinion and feedback toward MW, where the participants reported faster login times than the OTP method. An overwhelming majority of participants (97.82%) logged into their accounts without any mistakes or forgetting their memorable words, indicating that MW was convenient, learnable, and easy to use.

Comparing the study results with similar study results [29], we found that timing data in MW authentication method is the faster way for users to log in to their accounts. At the same time, U2F is the quickest method in the [29]. Moreover, our study tested MW timeout to check if participants needed help entering MW letters. The result was that 94.91% of participants logged into their accounts without any mistakes before it timed out. Another study tested OTP timeout and found that 65% of participants had problems entering the six-digit verification code before it timed out. Both studies conducted SUS to evaluate a user's perception of a system's ease of use and overall usability. Our study found that the median score of the MW method was 96.22. Regarding Reese et al. study [29], the finding of evaluating five methods was passwords had the highest median SUS score, with a median score of 95, followed by TOTP, which had a median SUS score of 88.75.

In today's fast-paced world, users have increasingly high expectations for carrying out their tasks promptly on various digital platforms. Any delay or inconvenience in the login process can lead to frustration, negative user experiences, and potential cyberattacks. Our study highlighted a critical finding regarding the OTP method, which showed a delay in receiving the verification code. Eliminating the need for users to wait for OTPs can enhance the efficiency of authentication systems and provide a seamless login experience for users. OTP can be less secure when a user's mobile device or token generator is compromised or intercepted maliciously. One of the significant vulnerabilities associated with SMS OTP is SIM swapping [30, 31]. This occurs when an attacker convinces a mobile network provider to transfer a victim's phone number to a new SIM card under their control. Once the attacker controls the victim's phone number, they can intercept any SMS OTPs sent to that number, effectively gaining access to the victim's accounts. Another common attack vector for OTP is the phishing attack [32, 33]. Phishing involves tricking and deceiving the victim into revealing their login credentials or multi-factor authentication (MFA) code by posing as a legitimate entity. In the case of OTP, the attacker could send a phishing message to the victim's phone, making it appear as if it is coming from a trusted source such as a bank or other known service providers. Once the victim falls for the scam, the attacker can use that code to authenticate themselves and gain unauthorised access to the victim's account.

On the other hand, using the MW technique can help prevent certain types of attacks, such as MITM attacks [34, 35], where malicious attackers redirect users to a fake website before forwarding them to the legitimate one. Since users are only required to type random letters from the memorable word instead of their entire secret token, it becomes more difficult for attackers to capture the complete word in one go. While the MW technique may provide some protection against MITM attacks, unfortunately, it does not entirely prevent them. In the event of a MITM attack, an attacker could still prompt the user for the same letters they are being prompted for, thereby gaining access. Thus, it is recommended that the MW be changed frequently.

It is important to consider that while MW may provide some level of security at the user's end, it may be less secure at the server or organisation's end. One potential vulnerability exists in storing memorable words as a single field within the system. This means that if there were to be a database leak or breach, the MW authentication system would be susceptible to the same risks as other forms of 2FA.

In conclusion, using MW as a security solution offers few advantages over OTP methods. It provides a better level of security than just relying on a password alone by preventing the transmission of the complete word and protecting against certain types of attacks. However, it may be less secure in specific scenarios and should ideally be implemented as an additional layer of security alongside other authentication methods.

VII. Limitation

The main limitation of this research was the time needed to spend with the participants, which reduced the sample size. Thus, this may prevent generalising the findings to the general population.

VIII. Conclusion and Future Work

The study investigated and compared the usability of two authentication methods, MW and OTP, in e-government and e-bank systems in Saudi Arabia. A usability testing survey was conducted to gain insights into users' perspectives on the proposed MW method and compare it with OTP. Overall, the participants expressed a positive opinion about MW, finding it easy to use and highly convenient. In contrast, OTP presented several challenges, including delays in receiving verification

codes and ineffective authentication when the signal was interrupted. The study revealed that many users struggled with OTP and required an alternative authentication method. Through analysis and simulation, it was determined that the proposed MW method offers comparable security control to existing OTP authorisation while minimising the dynamic risk of theft and eliminating the need for additional hardware. As this method eliminates the possibility of crucial theft, it can be used on private and public computers. Notably, this method is cost-effective and poses no significant hurdles.

The proposed method holds potential for further research on security attacks, particularly in addressing replay attacks, man-in-the-middle attacks, reflection attacks, and parallel session attacks.

ACKNOWLEDGMENT

The authors are grateful to Afrah Almalki and Retal Mehdawi for their work during projects.

REFERENCES

[1] A. S. Alharbi, . G. Halikias, M. Rajarajan and . M. Yamin, “A review of effectiveness of Saudi E-government data security management,” International Journal of Information Technology, vol. 13, p. 573–579, 2021.

[2] H. P. Singh and T. S. Alshammari, “An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia,” Beijing Law Review,, vol. 11, no. 3, pp. 637-650, 2020.

[3] G. P. Dias, “Global e-government development: besides the relative wealth of countries, do policies matter?,” Transforming Government: People, Process and Policy, vol. 14, no. 3, pp. 381-400, 2020.

[4] Y.-C. Yan and S.-J. Lyu, “Can e-government reduce local governments' financial deficits?——Analysis based on county-level data from China,” Government Information Quarterly, vol. 40, no. 3, 2023.

[5] A. Alrubaiq and T. Alharbi, “Developing a Cybersecurity Framework for e-Government Project in the Kingdom of Saudi Arabia,” Journal of Cybersecurity and Privacy, vol. 1, no. 2, p. 302–318, 2021.

[6] R. A. Abdulhadi and S. Ahmad, “IInternet Banking In Saudi Arabia,” Palarch’s Journal Of Archaeology Of Egypt/Egyptology , vol. 18, no. 13, pp. 673-684, 2021.

[7] F. Mabrouk, “Statistics of Cybercrime from 2016 to the First Half of 2020,” International Journal of Computer Science and Network, vol. 9, no. 5, pp. 252-261, 2020.

[8] M. Bada and J. R. C. Nurse , “Exploring Cybercriminal Activities, Behaviors, and Profiles,” in Applied Cognitive Science and Technology, Singapore, Springer, 2023, p. 109–120.

[9] R. Dhanalakshmi, N. Vijayaraghavan, S. Narasimhan and S. Basha, “Password Manager with Multi-Factor Authentication,” in International Conference on Networking and Communications (ICNWC), Chennai, 2023.

[10] M. Golla, G. Ho, M. Lohmus, . M. Pulluri and E. . M. Redmiles, “Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns,” in 30th USENIX Security Symposium, 2021.

[11] K. Reese, “Evaluating the Usability of Two-Factor Authentication,” 2018.

[12] J. Abbott and S. Patil, “How Mandatory Second Factor Affects the Authentication User Experience,” in CHI Conference on Human Factors in Computing Systems, honolulu, 2020.

[13] E. T. Alharbi and D. Alghazzawi, “Two Factor Authentication Framework Using OTP-SMS Based on Blockchain,” Transactions on Machine Learning and Artificial Intelligence, vol. 7, no. 3, pp. 17-27, 2019.

[14] R. P. Jover, “Security Analysis of SMS as a Second Factor of Authentication: The challenges of multifactor authentication based on SMS, including cellular security deficiencies, SS7 exploits, and SIM swapping,” acmqueue, vol. 18, no. 4, p. 37–60, 2020.

[15] V. K. Anand and D. Tirfe, “A Survey on Trends of Two-Factor Authentication,” in Contemporary Issues in Communication, Cloud and Big Data Analytics, Singapore, 2022.

[16] M. Hassan, Z. Shukur and M. K. Has, “An Improved Time-Based One Time Password Authentication Framework for Electronic Payments,” International Journal of Advanced Computer Science and Applications , vol. 11, no. 11, pp. 359-366, 2020.

[17] A. A. Ali Abdullah S. Alqahtani, “0E2FA: Zero Effort Two-Factor Authentication,” 2020.

[18] A. Mohammed, R. Dziyauddin and L. Abdul Latiff, “Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges,” Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges, vol. 14, no. 1, pp. 166-178, 2023.

[19] S. Das and A. Dingman, “Why Johnny Doesn’t Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key,” in Financial Cryptography and Data Security: 22nd International Conference, Nieuwpoort, 2018.

[20] D. Tirfe and V. K. Anand, “A Survey on Trends of Two-Factor Authentication,” in Contemporary Issues in Communication, Cloud and Big Data Analytics, Singapore, 2021.

[21] S. Istyaq, “Hybrid Authentication System Using QR Code with OTP,” International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 10, no. 6, pp. 1194-1197, 2016.

[22] S. P. Boraiah, “Secure Cardless Transaction Android Application using ECC algorithm and QR code,” Masters thesis, Dublin, National College of Ireland, 2019.

[23] S. Das, B. Wang, Z. Tingle and L. J. Camp, “Evaluating User Perception of Multi-Factor Authentication: A Systematic Review,” in the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), Nicosia, 2019.

[24] N. Gunson, D. Marshall, H. Morton and M. Jack, “User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking,” Computers and Security, vol. 30, no. 4, pp. 208-220 , 2011.

[25] J. Brooke, “SUS—A Quick and Dirty Usability Scale,” Usability Evaluation in Industry, pp. 189-194, 1986.

[26] A. S. Alharbi, G. Halikias, M. Rajarajan and M. Yamin, “A review of effectiveness of Saudi E-government data security management,” nternational Journal of Information Technology, vol. 13, no. 2, pp. 573-579, 2021.

[27] C. Weir, G. Douglas, . M. Carruthers and M. Jack, “User perceptions of security, convenience and usability for ebanking authentication tokens,” Computers & Security, vol. 28, no. 1-2, pp. 47-62, 2009.

[28] E. D. Cristofaro, . H. Du and J. Freudige, “A Comparative Usability Study of Two-Factor Authentication,” in Workshop on Usable Security and Privacy (USEC’14), 2014.

[29] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron and K. Seamon, “A usability study of five {two-factor} authentication methods.,” in Fifteenth Symposium on Usable Privacy and Security, Santa Clara, CA, USA, 2019.

[30] M. Kim, J. Suh and H. Kwon, “A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures,” in 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), Vietnam, 2022.

[31] R. P. Jover, “Security analysis of SMS as a second factor of authentication,” Communications of the ACM, vol. 63, no. 12, pp. 46-52, 2020.

[32] R. A. Grimes, “One-Time Password Attacks,” in Hacking Multifactor Authentication, Wiley, 2020.

[33] E. Ulqinaku, D. Lain and S. Capkun, "2FA-PP: 2nd factor phishing prevention," in Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, Florida, 2019.

[34] O. Umoren and H. Marco-Gisbert, "A Study on the Security of Authentication Systems," in The Fourteenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2021.

[35] S. Maaz, G. Sinha and D. K. Sinha, "Examination of Different Network Security Monitoring Tools," in Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, Singapore, 2023.