International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

Useable Authentication Mechanisms for Secure Online Banking in Saudi Arabia

Ali Alzahrani
Department Computer Science, Islamic University of Madinah, Madinah, Saudi Arabia

ABSTRACT

Two-factor identity authentication offers the most effective login security, and online and mobile banking users now use multi-factor identity authentication as the simplest and most innovative login security measure available for guaranteeing the privacy and safety of personal data. This system allows banks to recognize a client, while simultaneously verifying for the client whether he/she has accessed the correct bank's website or application prior to password entry. All internet and mobile banking authentication techniques may be categorized as preventing two common types of attack: offline credential theft and online channel-breaking attacks. It has therefore been recommended by security experts worldwide that a multi-factor authentication method be used for Internet and mobile banking authentication to ensure the safety of users' confidential data without undermining the ease of secure and simple authentication. Multi-factor internet and mobile banking authentication seems, therefore, to offer a solution through which the trade-off between safety and usability may be successfully negotiated. This study's primary objective is to propose various practical technological security mechanisms that will enable online banking customers in Saudi Arabia to select their preferred method of signing into online banking websites that are reliant on one-time password (OTP) techniques. The study included a survey aimed at ascertaining the various techniques used and which of these techniques were preferred. The experiment replicated an actual online banking setting utilizing the proposed methods; subsequently, the usability and safety of three different techniques for generating and communicating OTPs were assessed (SMS, e-mail, and soft and hard tokens).

Keywords : Password Authentication, One-Time Password (OTP), Two-factor Authentication

I. INTRODUCTION

The Internet plays a significant role in our lives, and the number of individuals who wish to avail of the convenience of online banking, available regardless of time and place, is steadily increasing. Internet and mobile banking have emerged as a key element of financial companies' multichannel policies. Owing to the extreme sensitivity of information concerning financial institutions, their clients and their operations, the use of public networks can contribute new complexities to the process concerning issues of security and reliability. The problems of verification, privacy, honesty and non-repudiation must be resolved by any internet and mobile banking system; that is, they must ensure that internet and mobile banking accounts are used exclusively by genuine clients, that all data remain secure and tamper-proof, and that any transactions performed are perceptible and confirmable. No single method for addressing both authentication and non-repudiation has hitherto been proposed, while Secure Sockets Layer/Transport Layer Security (SSL/TLS) remains the primary internet banking protocol for privacy and reliability.

Prior to availing of services, users must be verified by internet and mobile banking systems. Specifically, the banking system should request some direct or indirect evidence of knowledge regarding confidential information or credentials so that it may verify whether the user is indeed who he or she claims to be. On the assumption that such questions can only be answered correctly by a valid user, successful verification ultimately permits customers to access their confidential information. Two-way identity authentication offers the most effective sign-in security. Internet and mobile banking users now use multi-factor identity authentication, as the simplest and most innovative login security measure available for guaranteeing the privacy and safety of personal data. This system allows banks to recognize a client, while simultaneously confirming for the client whether he/she has accessed the correct bank's website or application prior to password entry.

All internet and mobile banking authentication techniques are categorized as preventing two common types of attack i.e. offline credential theft and online channel-breaking attacks. It has, therefore, been recommended by security experts worldwide that multi-factor authentication methods should be used for internet and mobile banking authentication to ensure the safety of users' confidential data without undermining the ease of secure and simple authentication [1]. In comparison with single-password based authentication, multi-factor authentication techniques are associated with inferior usability, and this probably accounts for the lower adoption rates [2 –7]. Multi-factor internet and mobile banking authentication seems, therefore, to offer a solution through which the trade-off between safety and usability might be successfully negotiated.
This paper will describe existing authentication techniques and offer a comparative usability study concerning internet and mobile banking verification in Saudi Arabia. An easy-to-use multi-factor identity authentication technique is employed in the research through which users are permitted to freely select strong passwords. This technique is simple and easy to use, and can help to prevent numerous standard offline credential-stealing attacks and online channel-breaking attacks that are associated with internet and mobile banking authentication systems. First, a pilot study is conducted to determine the most popular multi-factor technologies used by international banks. Subsequently, the plan and outcomes of the quantitative research project (comprising a survey of 100 users) are offered, through which the usability of some two-factor solutions are determined: one-time codes generated through security tokens, and one-time pins gained through SMS, e-mail, and hard and soft tokens SMS.

II. LITERATURE REVIEW

Two types of authentication technique, i.e., single-factor and two-factor, will be discussed in this study.

A. Authentication Methods:

Authentication is the process via which a user's authenticity is verified as they attempt to access information [2]. Several factors affect the successful identification of the user. Authentication may comprise various stages, including:

- Password Authentication
- Biometric Authentication
- Two-factor Authentication
- Phase Authentication
- Identity Based Authentication
- Identifying and Puzzle-Solving Based Authentication

1) Single-Factor Authentication:

For Single-Factor Authentication (SFA), only one factor is required to verify users before they are granted access to the website. The mostly commonly employed mechanisms include knowledge-based

factors, such as passwords, passphrases, and PINs, although these are perceived as the least secure authentication methods. Most consumers are concerned about the usability of SFA methods. Ma and Feng [13], also concerned with SFA methods, assessed the usability of three password types: customary text passwords, mnemonic passwords and graphical passwords.

Ma and Feng's study revealed that traditional and mnemonic passwords consumed less user authentication time than did graphical passwords [13]. Graphical passwords required longer to verify users because of two factors: the additional time needed to download the images and the time taken by the user to process the 30 images presented on the page [13]. Moreover, it became clear that both graphical and text passwords are equally memorable [13]. The usability of three password managers (i.e. a phone manager, a USB manager and an online manager) was examined by Karole et al. [12]. Users' views regarding the security and usability of the three password types were examined by researchers who discovered that portable and standalone managers were more frequently employed by users than were online managers [12]. It was also revealed, however, that the usability of online managers is superior to that of other managers [12 and that phone managers were more frequently used by non-technical users [12]. Comprehensive research on graphical password techniques was conducted by Hafiz et al. [8], who examined the usability and security characteristics of graphical password techniques. The findings revealed that graphical passwords can deal with attacks more effectively [8]. Some participants claimed that they found traditional passwords more difficult to remember than graphical ones [8]. This research was aimed at fulfilling users' needs [8], and, ultimately, the need to strike a balance between usability and security was highlighted [8]. Human computer interaction security is examined by Nilsson [19]. He compared two verification procedures and to comprehend users' views regarding trust in online banking. The survey and in-depth interviews with a sample of 86 users revealed that permanent passwords are considered less reliable than security boxes [19].

2) Multi-Factor Authentication:

The most frequently employed authentication technique is that comprising a username and password, which is unfortunately considered to be the least secure system. Three main factors characterize authentication techniques:

- Knowledge: something that is known to the user (e.g., a PIN or a password)
- Possession: something owned or possessed by the user (e.g. a USB token or smart card)
- Characteristic: something intrinsic to the user (e.g. biometric features such as fingerprints or eye patterns).

Authentication methods may be categorized as single- or two-factor authentication on the basis of these three factors. Just one factor is involved in single-factor authentication. For example, basic username or password authentication is reliant on information known to the user. Two or more factors are involved in two-factor authentication which may be facilitated by software (e.g. a software certificate), hardware (e.g. smart card or USB token) or any out-of-band techniques for generating one-time passwords (OTP) (e.g., SMS, e-mail, soft or hard tokens).

Two-factor authentication in the online banking context signifies the need for various login names, passwords, or other modes of verification, or knowledge required to access highly confidential information or transactions that are associated with high threat levels. This technique may involve extra security-related questions or supplementary passwords when users seek to perform transactions that involve higher risk levels. In two-factor

authentication systems, users are required to answer an additional security related question if they wish to transfer finances outside the institution, or a call-back policy may also be applied.

B. Usability of Online Banking:

Online banking enables clients to access their account information online and to avail of several services. Website usability should be considered to facilitate a positive online experience. Two vital issues affect online banking: safety and usability. However, security measures are frequently inadequate or entirely lacking [16].

To ensure that clients may avail of online services without any risk of scam, modern security techniques are often used by the banks in their online banking websites, making the usability of online banking systems a significant issue. Several studies have examined the usability of online banking interfaces [7-10].

Usability is regarded as an important component of present-day interactive systems. According to the International Standards Organization (ISO 1999), usability is 'the extent to which users are allowed by a computer system, in a particular setting, to achieve a particular objective successfully and proficiently while offering contentment' [1, 2]. Usability assessment plays a significant role in interface design along with interactive sequences of design, prototype, and assessment [3]. The evaluation process includes capture, examination, and review. Capture is the stage during which usability data are gathered (e.g. time taken to complete the task, number of mistakes made, and subjective rating of the user's satisfaction level). During the analysis phase, the collected usability data are analyzed according to appropriate data analysis tests and usability scoring methods to determine issues associated with interface usability. Various recommendations, strategies, or improvements are then offered [3, 4].

The design of usable interfaces is promoted by the field of human-computer interaction (HCI). The software industry also makes use of several development models in this field [5, 6], with key emphasis placed on establishing and enhancing the efficiency, usability, security, and utility of interactive computer-based products [5, 7]. This technique boasts multi-disciplinary applicability since it entails theory, research techniques, user and setting, statistics and examination, and planning and application [8]. Controlled experiments, usability research, observation, interviews, focus groups, field researches and surveys are the most frequently used examination techniques [9, 10].

Rogers *et al.* [5] offered a definition of interaction design, with priority given to enhanced user experience. Techniques incorporating ideas from HCI and Software Engineering (SE) are still required to some extent, however. Usability Engineering (UE) emerged in response to this requirement [5]. At present, usability is a chief concern for HCI. The planner attempts to ensure that the interface element of the software can be utilized successfully and proficiently by future users. For example, users should know how to progress from one phase to the next, if possible, without needing to refer to documentation [11]. Furthermore, designers aim to reduce the number of steps and mouse clicks required, as well as the time within which users can complete a task. In interface assessment, the user engaging with software is often closely monitored. The number of mistakes made, presence of pre-existing medical conditions, reaction and achievement times, and inability to complete an activity, are considered and reported along with the conditions in which these tasks were performed. The findings are then examined and applied to enhance the interface and the procedure is repeated until the software is deemed adequately usable [11, 12].

Usability assessment facilitates the development of interfaces that are usable, efficient, and gratifying for the user [13]. Through an effective interface, users can accomplish tasks with few errors and within a shorter time. The lowest error rates are observed when tasks are accomplished using an effective interface. User behavior contributes to the user's level of fulfillment with respect to the system [5, 8, 14]. Final versions of these systems frequently undergo a validation test as the last stage of assessment.

Qualitative surveys concerning the user identification techniques implemented in Anglophone online banking settings have been conducted [22,23]. Through examination of the online banking interfaces of several popular banks operating in seven countries, various reports and requests for the standardization of user documents in these settings were produced.

The study was aimed at verifying user identity in an online banking system. Users were required to undergo verification using digital techniques and, more significantly, attempts were made to prevent illegal access. Several suggestions were offered by the author to help ensure a more secure online banking environment; moreover, he examined how personal information can be gathered. The study's findings revealed that authentication techniques customarily require only a username and password, with the username replacing the account number, and that security questions concerning private information such as date and place of birth also serve as verification techniques for online banking systems. The author proposed a more secure technique: tokens, which are small tools via which codes can be delivered to users, allowing them to access the system. Not all banking systems have embraced this method, however, as it is regarded by some as too complex to work efficiently; clients are not usually willing to use additional devices to access the system.

Moreover, 100 online banking clients were observed in a simulated banking setting [16-21] and the usability and safety of three different techniques (token, card reader, and fingerprint) were evaluated. Initial findings showed that the system model was suitable for evaluating ease of use, while the results indicate that, according to users, the fingerprint is the safest and preferred technique.

The proposed technique entailing comprehensible authentication steps aims to offer hands-on experience in the context of usability research. The major aim is to induce users to behave as they would behave in an actual online banking scenario to achieve the optimal outcome.

Three different techniques were applied and eventually an experiment was conducted wherein each user interacted practically with each technique. The methods employed in the research demanded that usability techniques should be implemented in tandem with safety measures aimed at enhancing the users' understanding of security pointers. The findings revealed that according to the users, fingerprints are the preferred and most secure authentication mode.

High levels of risk are associated with online banking, with security being the major issue, as clients' personal accounts, transaction records, and credit card information are all at stake. Recently, security has also emerged as a major concern regarding the increasing numbers of bank users in Saudi Arabia, where almost 20 million people availed of online banking services in 2017 [16]. Verification techniques play an important role, and banks endeavor to confirm the user identity to ensure a safe process. Website security is frequently determined by how effective the website's verification technique is. Therefore, two-factor verification techniques are used in online banking systems to ensure effective

and safe verification. The user information and usability of banking systems must be protected by the bank owners. However, handling the security of users can be challenging, as users are more inclined to use verification techniques that are easy and consequently, less secure. Clashes between security and usability frequently center on the verification process [17]. This issue has been discussed by experts in the field of human-computer interaction (HCI) and security and new avenues for research on usability and security have also been proposed. As such, this paper is aimed at resolving the differences and describing the present research, which has been designed and performed toward numerous corresponding objectives.

III. IMPLEMENTION

In this section, we describe the development of the online banking OTP application that was designed as a multi-factor authentication mechanism. We developed the mobile application using Android Studio by Java.

The system was designed as follows: a user registers and opens a new account with the purpose-designed online banking system. The user logs into to the system, and is then asked to enter an OTP for security using various OTP technologies. The system authenticates the validity of all these processes and, following the application of each OTP technique, the user will be redirected to the survey page, as shown in Figure 1. There are four methods for providing the user with an OTP: SMS, e-mail, and soft and hard tokens. Each user tries all four methods and then answers the usability survey questions pertaining to each method.

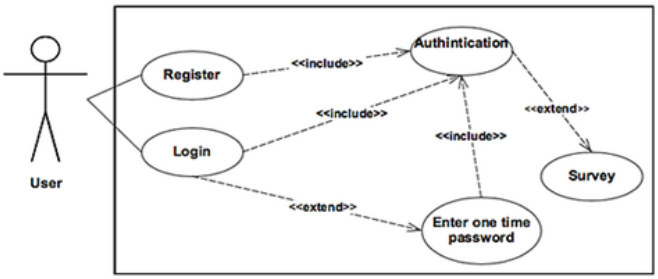

Figure 1. Online Banking System (User Case Diagram)

The OTP validation methods are presented below:

A. SMS Validation

When the user chooses "SMS" from the main menu a notification message reading "SMS Sent" will appear and a message will be sent to the registered mobile number that the user entered during registration, as shown in Figures 2 and 3.

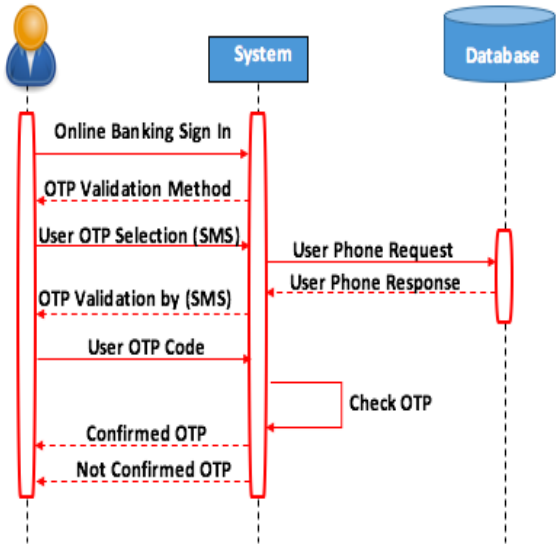

Figure 2. Sequence Diagram (SMS Validation)

Figure 3. SMS Validation

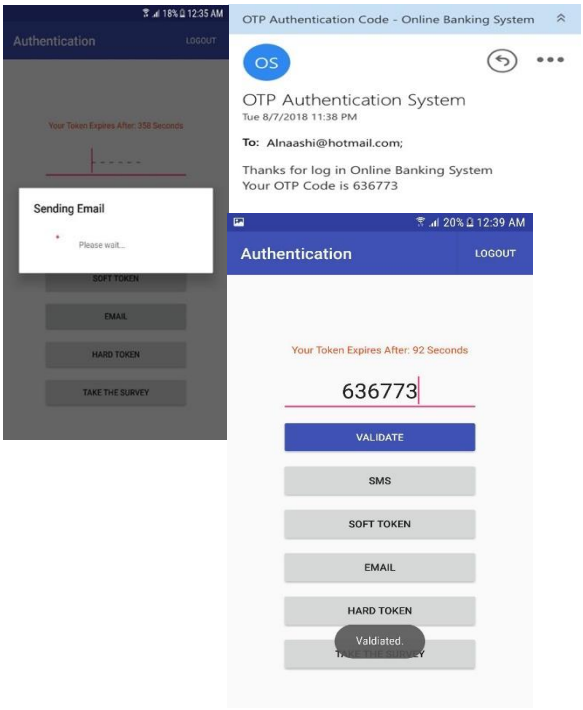

Figure 5. Email Validation

B. Email Validation

Figures 4 and 5 illustrate the e-mail validation process. When the user selects "Email" from the main menu a code will be sent to their registered e-mail address.

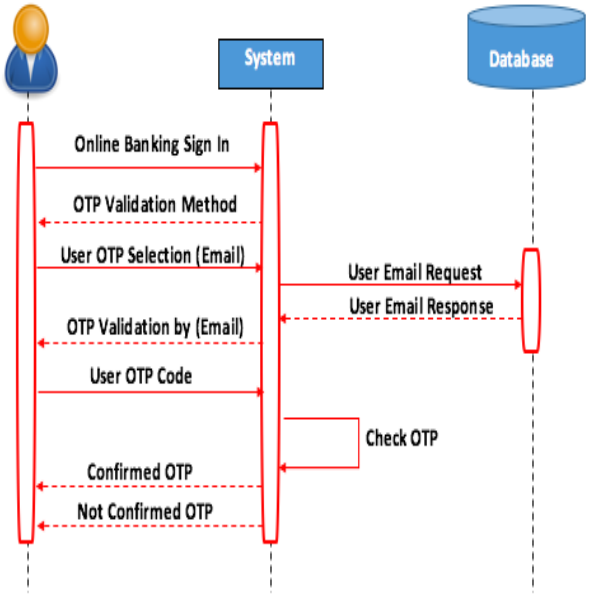

Figure 4. Sequence Diagram (Email Validation)

C. Soft Token Validation

If the user clicks on "Soft Token", then clicks "validate" on the main menu, the soft token will appear at the top of the screen, as shown in Figures 6 and 7.

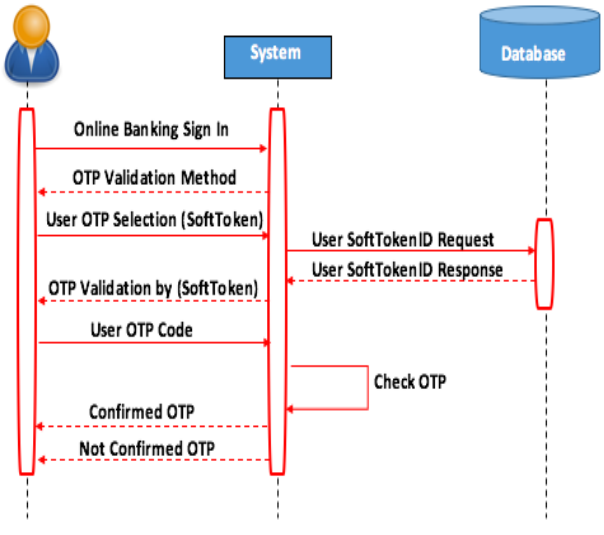

Figure 6. Sequence Diagram (Soft Token Validation)

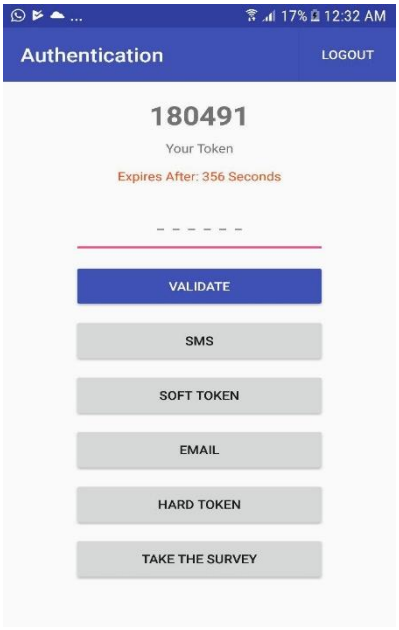

Figure 7. Soft Token Validation

D. Hard Token Validation

For hard token validation, we used the Gemalto hard token which provides users with a random OTP code, as shown in Figures 8 and 9.

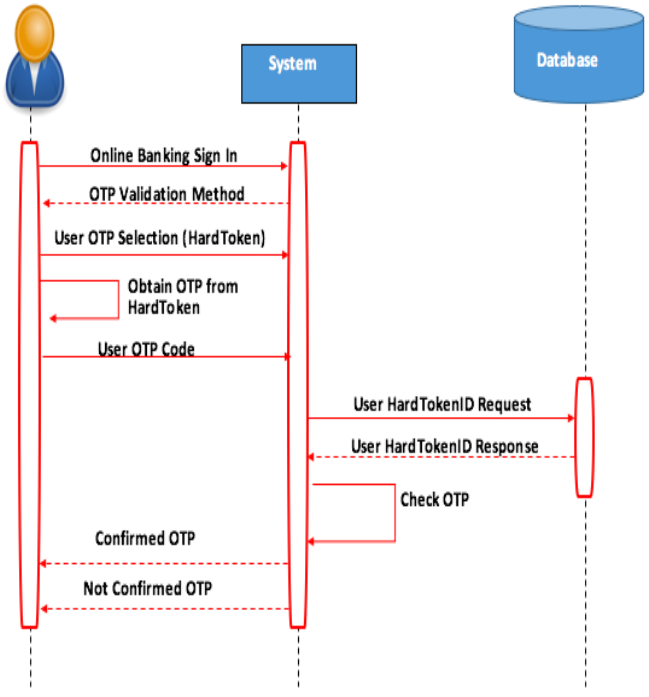

Figure 8. Sequence Diagram (Hard Token Validation)

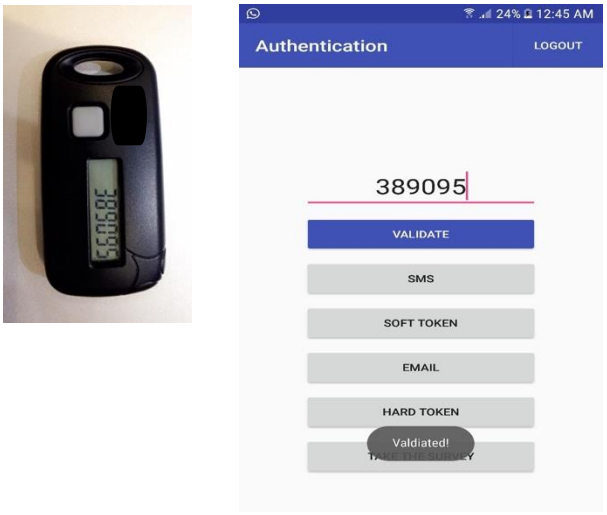

Figure 9. Hard Token Validation

IV. CASE STUDY AND RESULTS

All users who participated in the study were asked to respond to a Google Forms survey, to ascertain the most important usability factors, based on the respondents' answers concerning the usability of the OTP methods implemented.

The respondents comprised 72.5% male and 27.5% female users. Table 1 presents the respondents' education levels: most (around 43%) held bachelor's degrees, while 23% were still undergraduates. Not all participants specialized in computer science.

Table 1. Participants' Levels of Education

High School or Lower	3%
High School Degree	19%
Some College Experience; Not Yet Graduated	23%
Bachelor's Degree	43%
Master's Degree	8%
PhD Degree	4%

The participants were required to use each OTP method separately and to answer questions pertaining to the usability of the method based on factors recommended by previous research [5, 8, 14].

The results of this survey are presented Figure 10. The first question concerned the preferred OTP method, and it emerged that 65% of participants preferred the SMS method. This method was also the most secure from the respondent's point of view. Participants also reported that it was the most well integrated method, while 57.5% found it to be the easiest. SMS was also the fastest OTP method while Email was the slowest. However, 85% of respondents believed that they should invest some time in learning how to use the hard token method while only 5% felt it would be worthwhile to spend time learning to use the other methods. Half of respondents were confident in using the SMS method with 5% hesitant regarding the e-mail method. Finally, respondents believed the hard token method to be the most cumbersome, followed by the e-mail method, while overall the SMS and soft token methods were regarded as convenient. The time interval between the sending of the OTP and input of the OTP into the authentication system was also examined and measured, as shown in Table 2. The SMS method was faster, with a time interval deemed satisfactory by 77.5%. The soft token method was also deemed sufficient (67.5%). On the other hand, the e-mail method was unsatisfactory, perhaps owing to delays based on the e-mail provider used. Finally, the hard token method may also be associated with delays owing to issues of locating the device or the login procedure on the device itself.

Table 2. Time Intervals

OTP method	Yes	No	Fair
SMS	77.5%	5%	17.5%
Email	22.5%	52.5%	25%
Soft Token	67.5%	17.5%	15%
Hard Token	47.5%	42.5%	10%

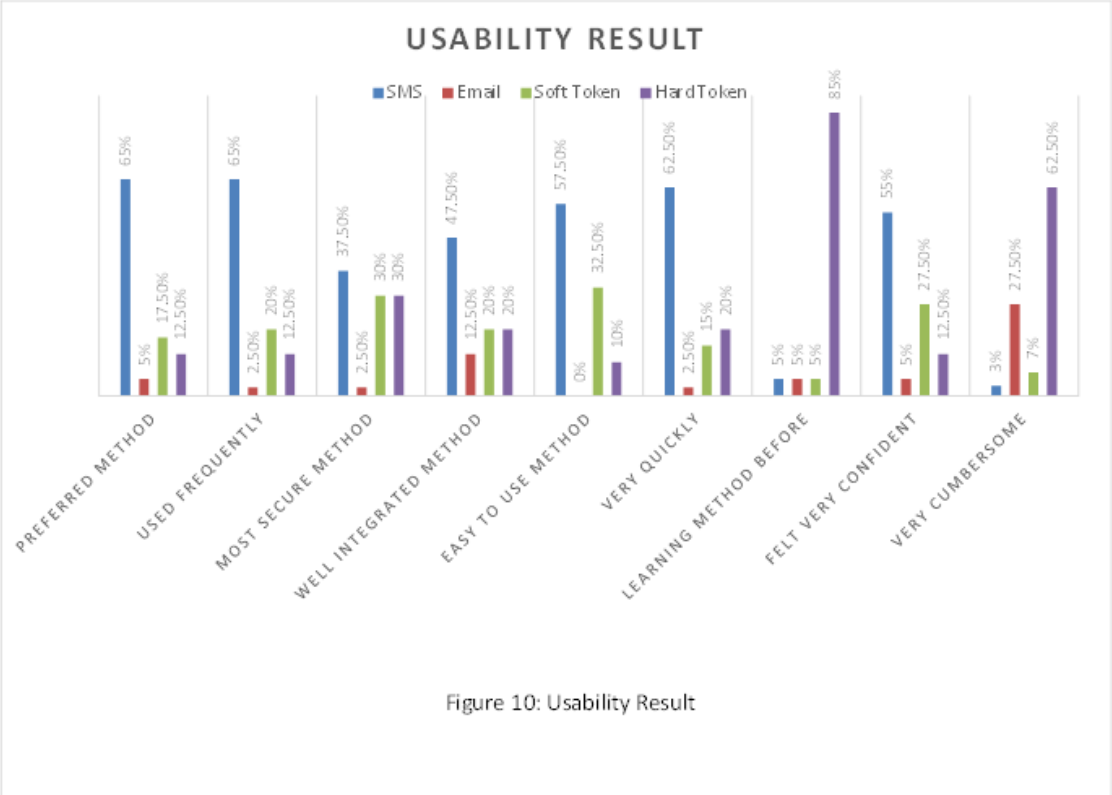

Figure 10: Usability Result

The usability results presented in Figure 10 and the time intervals presented in Table 2 generated further questions concerning difficulties that participants might have encountered in using these technologies. The first question concerned the consistency of the methods, and 40% of respondents found the hard token method to be the most inconsistent, as shown in Figure 11.

We also asked which method was considered the most unnecessarily complex, and again the hard token method scored highest at 45% (Figure 11). Finally, 55% of respondents believed that they would require technical support to use the hard token method while 19.5% of respondents believed that none of OTP methods would necessitate technical support.

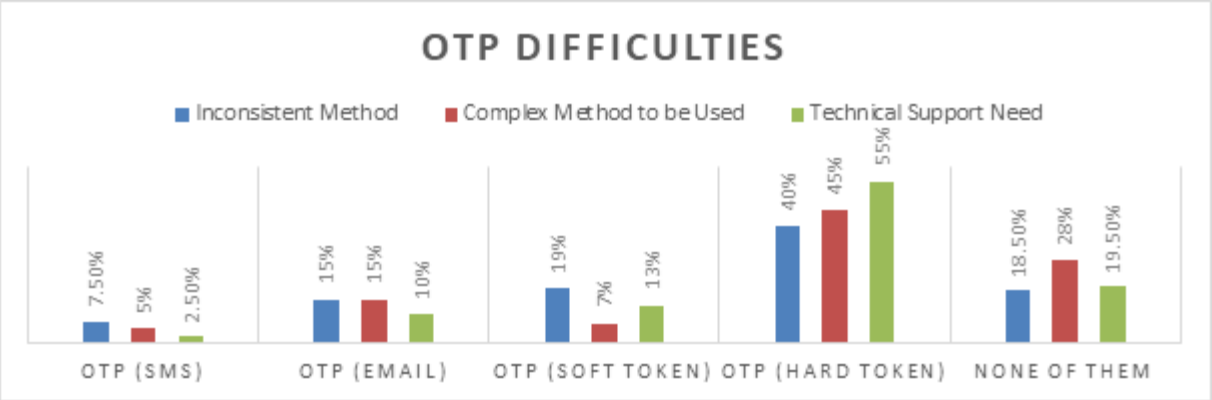

Figure 11. OTP Technology Difficulties

As may be seen from the survey results, SMS is the preferred OTP method for online banking in Saudi Arabia, with the hard token, regarded as the most complex method, is the least preferred.

V. CONCLUSION

This research presented a method for assessing various multi-factor authentication systems based on users' experiences in trying four different OTP-generation techniques (SMS, e-mail, soft and hard tokens), and subsequently ascertaining the users' preferred methods via survey. The experiment offered users a hands-on experience with each technique, allowing them to evaluate all these techniques toward the optimal usability outcomes based on the subsequent survey. The majority of the users who tested the system preferred the SMS method for OTP generation.

Usability of biometric verification methods should be prioritized in future studies, the results of which should be compared with previous findings.

VI. REFERENCES

[1]. N. Bevan, "International standards for HCI and usability," International Journal of Human-Computer Studies, vol. 55, pp. 533-552, 2001.

[2]. T. Jokela, N. Iivari, J. Matero and M. Karukka, "The standard of user-centered design and the standard definition of usability: Analyzing ISO 13407 against ISO 9241-11," in Proceedings of the Latin American Conference on Human-Computer Interaction, 2003, pp. 53-60.

[3]. M. Y. Ivory and M. A. Hearst, "The state of the art in automating usability evaluation of user interfaces," ACM Computing Surveys (CSUR), vol. 33, pp. 470-516, 2001.

[4]. J. M. Carroll, "Human–Computer Interaction," Encyclopedia of Cognitive Science, pp. 24-32, 2009.

[5]. Y. Rogers, H. Sharp and J. Preece, Interaction Design: Beyond Human-Computer Interaction. John Wiley & Sons, 2011.

[6]. J. Preece, Y. Rogers, H. Sharp, D. Benyon, S. Holland and T. Carey, Human-Computer Interaction. Addison-Wesley Longman Ltd., 1994.

[7]. A. Dix, Human-Computer Interaction (Pp. 1327-1331). Springer US: Springer, 2009.

[8]. J. Lazar, J. H. Feng and H. Hochheiser, Research Methods in Human-Computer Interaction. John Wiley & Sons, 2010.

[9]. S. B. Shneiderman and C. Plaisant, Designing the user interface 4th edition, Pearson Addison Wesley, USA, 2005.

[10]. J. Heer and B. Shneiderman, "Interactive dynamics for visual analysis," Queue, vol. 10, pp. 30, 2012.

[11]. J. Lazar, J. H. Feng and H. Hochheiser, Research Methods in Human-Computer Interaction. John Wiley & Sons, 2010.

[12]. Z. Obrenovic and D. Starcevic, "Modeling multimodal human-computer interaction," Computer, vol. 37, pp. 65-72, 2004.

[13]. A. Bangor, K. Joseph, M. Sweeney-Dillon, G. Stettler and J. Pratt, "Using the SUS to help demonstrate usability's value to business goals," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2013, pp. 202-205.

[14]. W. Hwang and G. Salvendy, "Number of people required for usability evaluation: the 10±2 rule," Commune ACM, vol. 53, pp. 130-133, 2010.

[15]. U Census Bureau, QUARTERLY RETAIL E-COMMERCE SALES.

[16]. Hyde, D. (2012). "Hackers crack new online banking security putting 25 m people at risk," Available from: http://www.thisismoney.co.uk/money/saving/article2096060/Hackerscracknew-online. Available online. Accessed on 13/03/2018].

[17]. Nodder, C. "Users and trust: A Microsoft case study," in L, Cranor, S., Garfinkel, Eds. Security and Usability. O'Reilly; 2005, pp. 589–606

[18]. Whitten, A., and Tygar, J.D. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in Proceedings of the 8th USENIX Security Symposium, 99, McGraw- Hill, 1999

[19]. Computing Research Association. "Four Grand Challenged in Trustworthy Computing", Final report of CRA Conference on Grand Challenged in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16 – 19, 2003

[20]. Piazzalunga, U., Savaneschi, P., and Coffetti, P. (The usability of security devices. In: L, Cranor, S., Garfinkel, editors. Security and Usability. O'Reilly; 2005, pp. 221–42

[21]. S. Kiljan, "Exploring, Expanding and Evaluating Usable Security in Online Banking", Open Universiteit, 2017.

[22]. A. Hiltgen, T. Kramp, and T. Weigold, "Secure internet banking authentication," IEEE Security and Privacy, vol. 4, no. 2, pp. 21–29, 2006.

[23]. C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in e-banking and the effects of experience," Interacting with Computers, vol. 22, no. 3, pp. 153 – 164, 2010. http://www.ijimt.org/papers/391-D0493.pdf]