A Two-Layer Authentication Security Through Personal Mobile SMS for KRG-Iraq E-Government System

Saman M. Abdullah[1] & Musa M. Ameen[2] & Sipan Asaad Ahmed[3] & Alina Najdat Muhamad[4]

[12,3, &4] Computer Engineering Department, Faculty of Engineering, Tishk International University, Erbil, Iraq
[1] Software Engineering Department, Faculty of Engineering, Koya University, Erbil, Iraq
Correspondence: Saman M. Abdullah, Tishk International University, Erbil, Iraq
Email: saman.mirza@tiu.edu.iq

Doi: 10.23918/eajse.v8i3p234

Abstract: This work is presenting the design and implementation of a two-factor authentication login system using mobile SMS. The main aim of this project is to build, present and add new security layer for the E- Government websites of KRG-Iraq that proposed by the IT section in the KRG Ministry Council. The plan of KRG IT section is to tie individuals to do their works and activities formally over the KRG official websites. However, the login security of such websites should be controlled so that unauthorized users should not be able to access to data belonged to other users. This work follows the scenario-based software engineering that thoroughly developers can collect requirements, and accordingly, the proposed project could be designed and achieved correctly. The developed project has been tested based on reviewing ten software testers. The overall acceptability that obtained from the assigned software testers is 86.7%.

Keywords: Two-Layer Authentication, SMS Authentication, E-Government System Authentication

1. Introduction

Recently the IT section in the Ministry of Council of Kurdistan Reginal Government has decided to create a unique social number for each individual and person in Kurdistan for the use as a security layer during processing the formal documentations in governmental departments through accessing the governmental websites (KRG, 2020). The only security issues that assigned for the KRG website is using the username and password, which could be hacked simply by any beginner attacker. This means, the log-in security for the proposed KRG E-Government system is in critical situation. To address this problem, this work proposing another layer for this security to improve the authentication

and accessibility of individual users to governmental websites. The idea that proposed by this work is called Two-factor authentication that proposed by authors (Bardis, Doukas, Markovskyi, & Drigas, 2010). Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves (Fang & Zhan, 2010). Figure-1 shows the flow process of the 2FA that simply could be achieved through the use of SMS.

Received: June 21, 2022
Accepted: December 15, 2022
Abdullah, S.M., & Ameen, M.M., & Ahmed, S.A., & Muhamad, A.N. (2022). A Two-Layer Authentication Security Through Personal Mobile SMS for KRG-Iraq E-Government System. *Eurasian Journal of Science and Engineering*, *8*(3),234-242.

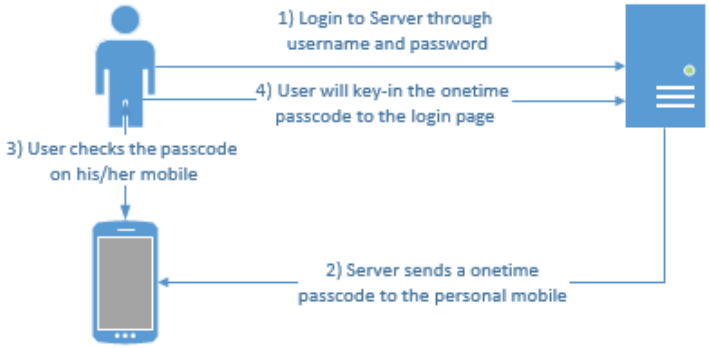

Figure 1: The simple flow of 2FA using SMS

As shown in the figure-1, the two-factor authentication is implemented to better protect both a user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor, typically, a password or passcode. Two-factor authentication methods rely on a user providing a password as the first factor and a second, different factor usually either a security token or a biometric factor, such as a fingerprint or facial scan (Iracleous, Moutsakis, & Efremidis, 2013).

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check (Eldefrawy, Alghathbar, & Khan, 2011). This work will build a website that could be simulating the official or governmental websites. The work tries to attach the scenario of two-layer authentication on

the proposed website. The website could be submitted to the IT section of Ministry Council as a suggestion and as a proposal.

2. Problem Statements and Work Contributions

According to the digital system of the KRG E-Government there is no Two-layer authentication that can secure the login process for individuals, although such security layers will add an extra level of protection that can stop attackers gaining access to government websites. The use of two-factor authentication means hackers have an extra step to bypass if they want to access a government website admin account. This is important as, by gaining access to one of these accounts, hackers could potentially redirect users to fake or malicious sites. The main idea of the project is collaborating the IT-Section of the KRG Government through building and presenting a security prototype that can secure the E-Government website through using the 2FA at the login page using the mobile SMS. This project makes user interaction with E- Government websites more securable than just depend on the personal unique ID that proposed by the IT- Section. The protype can combine both user unique ID and the personal devices. Therefore, the main objective of this work is to build a web-based application that simulates the E-Government of KRG while using the two-layer (factors) authentication through SMS of mobile phones for log-in purposes.

3. Literature Review

Increasing the level of security for any information system has become a major concern among researchers. Personal security or privacy is one of these topics that security experts and researchers are increasingly concerned about. As the number of people who use mobile technology grows, this strategy becomes more efficient (Kaviani, Hawkey, & Beznosov, 2003). Some earlier works that are most relevant to this topic will be presented and reviewed in this section.

Authentication is the process of verifying the user's identity by confirming the data received from a user with those stored in the database to check whether the user is the one claimed to be (Tirfe & Anand, 2022). Authentication is very important as it allows only the privilege user to access system resources. The main mechanisms that are available to authenticate a user are as follows:

1. Something you know (knowledge factor) such as a password, personal identification number (PIN), an answer to a security question.
2. Something you have (ownership factor) such as security token, subscriber identity module (SIM) card, one-time password (OTP) token, employee access card.
3. Something you are (biometric factor) such as biometric fingerprint, face, iris, retina, voice, gait, keystroke dynamics, gaze gestures, signature, deoxyribonucleic acid (DNA).

The above-mentioned mechanisms could be achieved through one of the following types of security authentication processes.

1. Single-Factor Authentication (SFA) Single-factor authentication. This mothed has been defined by Rouse and Rahav (Tirfe & Anand, 2022). With such system, the third party will authenticate a request of a user through identifying something that linked to that user, such as PIN to unlick a phone. This technique has been used by many companies as it is very simple and user-friendly. However, the simplicity of the technique makes it be targeted by many attacks such as surfing attacks, brute force attacks, social engineering attacks and impersonation attack. Therefore, such authentication process is not recommended for financial and bank transaction issues.
2. Two-Factor Authentication (2FA) Two-factor authentication was defined by Rahav (Ali, Ally Dida, & Elikana Sam, 2020). Here, the process of authentication relay on something you know (means something that be your privacy) linked with other information that you provide over the system. The 2FA usually attached to mobile banking activities. However, this type of authentication is not fully effective against many attacks, such as MIMT and phishing.
3. Multifactor Authentication (MFA) which has been defined by Rahav as the process via which a user wants to get access a resource that needs authentication on multiple identifiers such as something you know, or something you have, or something linked to the identify to grant access. With MFA, three factors are used for authentication, which are knowledge, ownership, and biometric.

To achieve authentication many works have been published to argue the most securable techniques. A work (Kaviani et al., 2003) published a paper suggesting a new level of authentication utilizing mobile SMS. Some programming technologies were used to create and implement the project. The work examined the application's usability as well as the user's satisfaction with it. There have been no tests performed on this work.to check the security satisfaction of the application against real users or on some real projects. Another study showed how the security level of several well-known websites might

be raised and strengthened by employing the two-factor authentication technique, particularly when using mobile devices (Dmitrienko,

Liebchen, Rossow, & Sadeghi, 2014). The project puts Google, Dropbox, Twitter, and Facebook's websites to the test. The research discovered various methods that might easily circumvent the log-in stage and gain access when access was granted without two-factor authentication. Another study applied the concept of two-layer authentication to the security of financial accounts (Bardis et al., 2010). The research demonstrates that using two-factor authentication (two-factor authentication) to conduct online banking or Internet banking transactions is more secure (Behera, Misra, Patro, & Roy, 2022).

The 2FA process is proposed for many applications, especially, for payment and finance issues. Two factor Authentication has been proposed as a security layer for micro-payment while wearable devices or mobiles have been used (Cha, Lee, Park, & Ji, 2015). Although the work (Cha et al., 2015) argued that 2FA could be used as a great additional security level, results in the work (Amrutiya, Jhamb, Priyadarshi, & Bhatia, 2019) shows that the SMS based 2FA is a trust less way for making smart contract in the blockchain. The method that could be considered as a most effective for reducing the risk of authentication process from being attacked by intruders are to find out a solution that minimizing the process of the user and builds the authentication process with strong cryptography which follows standards mainly by using digital certificates (Tirfe & Anand, 2022). However, intruders or attackers can use a variety of penetration methods such as social engineering (phishing), man-in-the-middle attacks (MITA) and breaching of weak credential to get authentication access of a secure network infrastructure.

Most information systems need strong access authentication. A work has designed a new method of authentication for academic information systems (Shirvanian & Agrawal, 2021) to provide a validity and reliability of academic data. The work shows that using 2FA with SMS or passing any token to the users' device makes the security of the information system more robust. The work showed that using second level of login systems doesn't over-loaded the systems and no delay recorded even at the time when many new students are registered, or current student renew their registration.

It seemed that 2FA can be utilized in many applications and could be considered for different purposes. In this work, the technique of 2FA has been proposed for an E-Government system that aims processing individuals' requests through online and through a unique number of user identification. The rest of the paper show the design and implementation of 2FA with an E-Government simulated website.

4. Work Methodology

The problems mentioned in the previous section can be simulated and solved through building a web application that can comprehend it. In this section, the different stages, which are shown in the figure 2, involved in the development of a website that applying two factor authentication concepts.

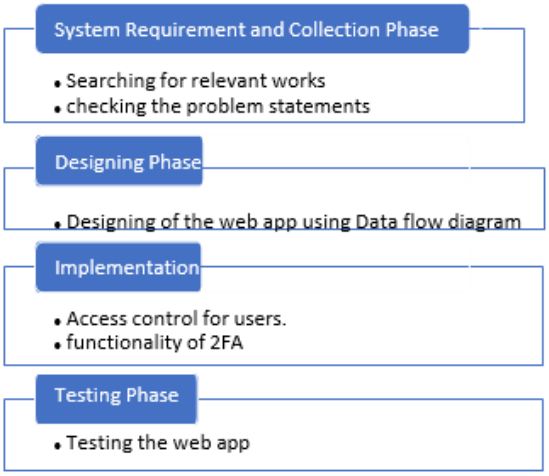

Figure 2: Min Framework for the work methodology

4.1 The 2FA Project Framework

The 2FA in this work could be represented throughout three main figures: figure 2, figure3 and figure 4. In this section only figure 2, which shows the flow of the work from the scratch, will be presented. It also representing the scenario of the work. A user could start by sending a request to the system that the user wants to check information over the E-Government. The projects respond is checking the first verification step through asking the username and the password. If available, then the system will send a one-time code through a registered mobile phone for the user. After that, the user should key-in the one-time code in the right place over the website. The system will double check the code, and the user could access the system only when the second layer of verification will be approved.

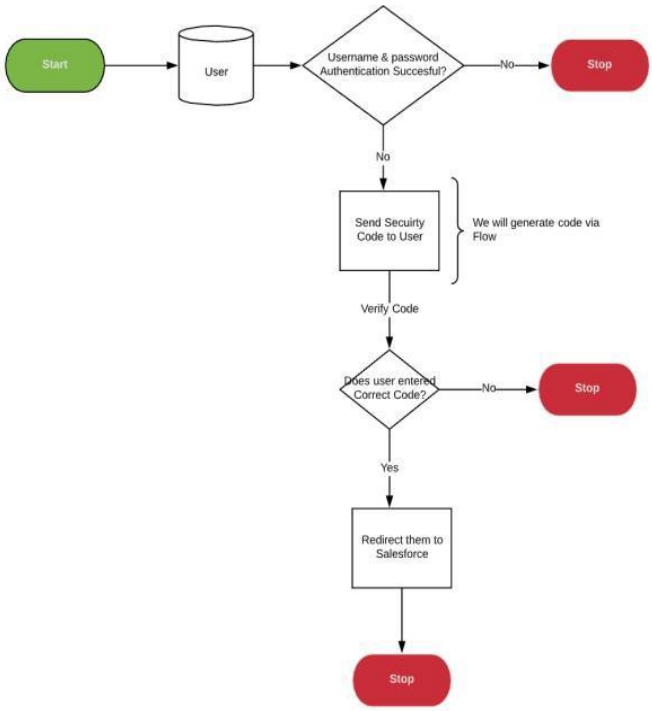

Figure 3: The work-flow of the proposed 2FA Project

4.2 The 2FA Website Roadmap

In this work, a website has been designed and implemented so that it can be simulated as the E-Government system that proposed by the IT section of KRG-Iraq government. Although the departments that belong to KRG government is more than has been covered by the simulated website, the project tried to involve most effective departments. Figure 3 shows the roadmap of the simulated website that designed for implementing the scenario that mentioned in the section 4.1.

All security and authentication activities that mentioned in the figure-3 could be seen in the first block of the figure, which is called login page. Only after getting confirmation from the system, a user can login and go the next step, which is Civil Registration Department (CRD). This CRD is not under the control of individuals. This part just showing an individual's privacy information. However, from this page an individual can be sure that he/she is browsing his/her pages. A sample of these pages will be shown in the subsequent sections.

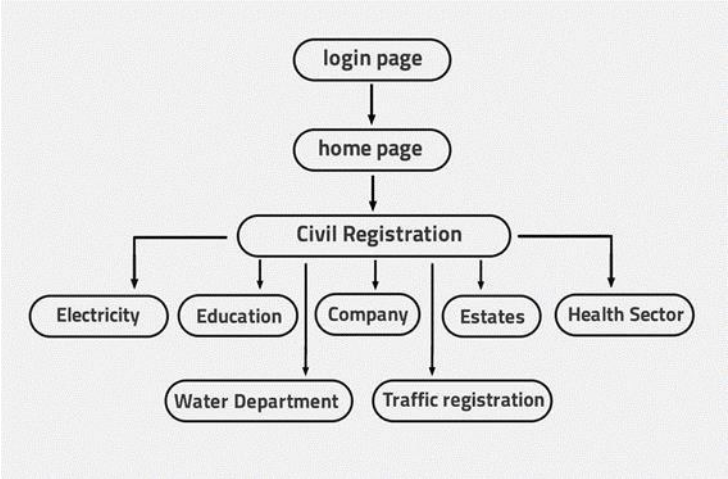

Figure 4: The roadmap of the KRG simulated website

4.3 The 2FA Website: Backend

The backend for any website is an important part of the website's design process. The back- end may consist of a server, an application, and a database. A back-end developer builds and maintains the technology that powers those components which, together, enable the user-facing side of the website to even exist in the first place. For this work, the back-end design comes as showed in the figure 4.

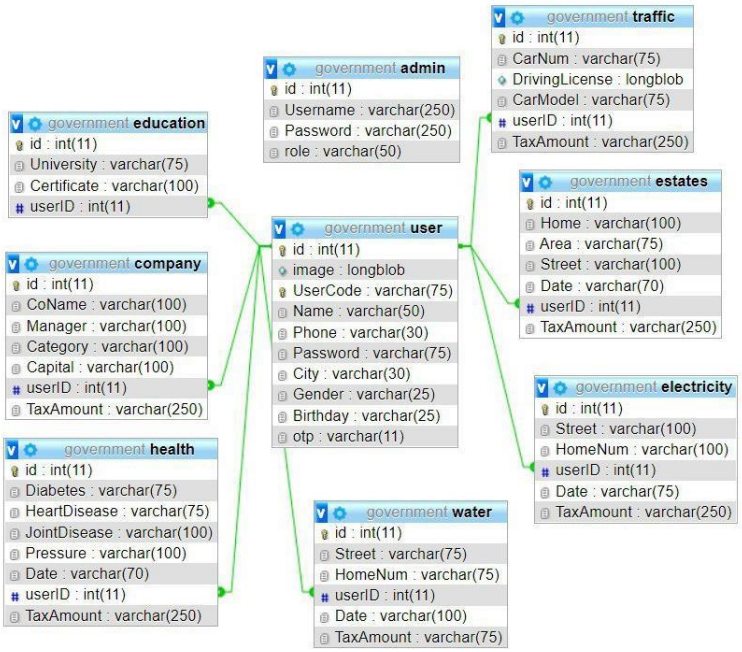

Figure 5: The back-end design for the proposed project

5. Work Implementation and Test

5.1 Work Implementation

This sub-section shows the implementation of the proposed project. The first part of the project is the registration page that allowed a user to be a member in the system. The idea of this work is to attach a two-layer authentication security verification to the E-Government system. Most aims that targeted by this work could be seen in this log-in page. The fist webpage that a user can visit is registration webpage. After the system accepts the user, the accessibility to the other parts of the system will be granted. However, first the user should be passed under a two-layer authentication process. The first layer is to key-in the username and the password, as shown in the Figure 7-a. Then, the system will generate a one-time code and will send it to the mobile that registered with the corresponding user, Figure 7-b.

5.2 Work Testing

The completed project has been tested with ten software testers against three main questions that concerned the security issues, user-friendly of the webpages, and requirement satisfaction. According to the flow work of building any systems, the last part of the process is to test the system against some predefined benchmarks. For this project, three benchmarks have been assigned. The first benchmark is checking whether the objectives, the aims and the requirements that defined for this project have been achieved or not. The second benchmark is the friendly use of the systema and the style of the website.

The last benchmark is the security check. The process of testing has been achieved by nine testers. Each one has marked all three benchmarks over a scall from one to five (one is very bad and five is very good. Most testers have agreed on the achieving the requirements up to 4.3, and the overall percentage of the agreement reaches 86.7%. Details of the testing process is illustrating in the table 1.

Table 1: The testers result against the benchmarks

Testers	Requirement Achievements	User Friendly	Security achievement
Tester-1	5	4	4
Tester-2	5	5	5
Tester-3	4	4	3
Tester-4	3	5	4
Tester-5	5	3	5
Tester-6	4	4	5
Tester-7	5	5	4
Tester-8	2	5	5
Tester-9	4	4	5
Tester-10	5	5	4
Average	4.2	4.4	4.4

References

Ali, G., Ally Dida, M., & Elikana Sam, A. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet, 12*(10), 160.

Amrutiya, V., Jhamb, S., Priyadarshi, P., & Bhatia, A. (2019). *Trustless two-factor authentication using smart contracts in blockchains.* Paper presented at the 2019 international conference on information networking (ICOIN).

Bardis, N. G., Doukas, N., Markovskyi, O. P., & Drigas, A. (2010). *Two level efficient user authentication scheme.* Paper presented at the 4th IEEE International Conference on Digital Ecosystems and Technologies.

Behera, R. K., Misra, M., Patro, A., & Roy, D. S. (2022). An Efficient Two-Wheeler Anti-Theft System Based on Three-Layer Architecture. In *Advances in Communication, Devices and Networking*, 393-403, Springer.

Cha, B.-R., Lee, S.-H., Park, S.-B., & Ji, G.-K. L. Y.-K. (2015). Design of micro-payment to strengthen security by 2 factor authentication with mobile & wearable devices. *Advanced Science and Technology Letters, 109*(7), 28-32.

Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A.-R. (2014). SECURITY ANALYSIS OF MOBILE TWO- FACTOR AUTHENTICATION SCHEMES. *Intel Technology Journal, 18*(4).

Eldefrawy, M. H., Alghathbar, K., & Khan, M. K. (2011). *OTP-based two-factor authentication using mobile phones.* Paper presented at the 2011 eighth international conference on information technology: new generations.

Fang, X., & Zhan, J. (2010). *Online banking authentication using mobile phones.* Paper presented at the 2010 5th International Conference on Future Information Technology.

Iracleous, D., Moutsakis, K., & Efremidis, O. (2013). Performance of Web Services Security Mechanisms: Analysis and Evaluation. *Journal of Applied Mathematics and Bioinformatics, 3*(4), 107.

Kaviani, N., Hawkey, K., & Beznosov, K. (2003). A Two-factor Authentication Mechanism Using Mobile Phones. *available at, Laboratory for Education and Research in Secure Systems*

Engineering, University of British Columbia, Technical report LERSSE-TR-2008-03, (Aug. 20, 2008).

KRG. (2020). Department of Information Technology. Retrieved from https://gov.krd/dit-en/

Shirvanian, M., & Agrawal, S. (2021). *2D-2FA: A new dimension in two-factor authentication.* Paper presented at the Annual Computer Security Applications Conference.

Tirfe, D., & Anand, V. K. (2022). A survey on trends of two-factor authentication. In *Contemporary Issues in Communication, Cloud and Big Data Analytics*, 285-296, Springer.