

The Libyan Academy

Tripoli, Libya



**School of Applied Sciences and Engineering
Department of Electrical and Computer Engineering**

Securing E-government web portal access by two-factor authentication

*A Dissertation submitted to
The Department of Electrical and Computer Engineering in
conformity with the department requirements as partial
fulfillment for the degree of
Master of Science*

**By:
Hamdi Ahmed Jaber**

**Supervision By:
Dr. Elbahlul Fgee**

Fall 2015

Abstract

This dissertation proposes a highly secure and easy to use authentication solution that enhances the authentication security of Libyan e-government web portal and solve the drawbacks of traditional Two-factor authentication systems that was not solved in the previous studies. The motivation is the risk of illegal access to the Libyan e-government web portal and probability of its occurrence and its potential impact. This thesis uses technical comparisons, tradeoffs, current systems tests and evaluations and online survey in the study methodology. Resulted in a new authentication system that avoids the drawbacks of Two-factor authentication technology, mitigating the risks exposed to the e-government web portal authentication. The proposed solution Implementation was included in the thesis.

الخلاصة

تقترح هذه الأطروحة نظام مصادقة مزدوج متقدم وآمن للغاية وسهل الاستخدام مما يعزز أمن تسجيل دخول المستخدمين على البوابة الإلكترونية للحكومة الليبية وحل عيوب نظم المصادقة المزدوجة التقليدية التي لم تحل في الدراسات السابقة. الدافع هو خطر الدخول غير المشروع إلى بوابة الحكومة الليبية على شبكة الإنترنت من حيث احتمالية حدوثه وتأثيره السلبي. تستخدم هذه الأطروحة المقارنات الفنية والمفاضلات واختبارات لنظم المصادقة المزدوجة الحالية وتقييم واستطلاع على الانترنت في منهجية الدراسة وتصميم للنظام الجديد. مما أسفر عن نظام المصادقة الجديد الذي يتجنب عيوب نظم المصادقة المزدوجة التقليدية، والتخفيف من مخاطر تعرض بوابة الحكومة الإلكترونية الليبية لدخول مستخدمين غير شرعيين. كما تم تنفيذ الحل المقترح في الأطروحة.

Acknowledgements

بسم الله الرحمن الرحيم

قَالَ لَوْ سَجَّانَكَ لَا عِلْمَ لَنَا إِلَّا بِاللَّهِ عَلَيْهِ تَوَكَّلْنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ

صدق الله العظيم

First, all praise is for Allah, Who enlighten us with faith and knowledge, and who is sufficient for us and has sheltered us.

For my father, mother, brothers and sisters. Thanks for everything.

My wife and son, Thanks for being in my life. You are always a great support.

My supervisor, Dr. Elbahlul Fgee, thanks for trust, time, and patience.

May Allah grant you a bright future and everlasting happiness.

Index

Abstract.....	II
Acknowledgements.....	IV
Index.....	V
List of tables.....	IX
List of figures.....	X

CHAPTER 1: Introduction	1
1.1. Problem statement.....	2
1.1.1. Two-factor authentication drawbacks.....	4
1.2. Motivation.....	5
1.3. Proposed solution.....	6
1.4. Dissertation layout.....	7

CHAPTER 2: Internet portals security	9
2.1. Internet portals security risk.	10
2.1.1. Replay.....	11
2.1.2. Session hijacking.....	11
2.1.3. Phishing....	11
2.1.4. Man-in-the-middle.....	11
2.1.5. Insider attacks.....	11
2.1.6. Malware....	11
2.1.7. Password discovery attacks....	12
2.1.8. Shoulder surfing.....	12
2.1.9. Social engineering attacks.	12

CHAPTER 3: Background and authentication review	13
3.1. Problem Analysis.....	13
3.1.1. How the traditional password system can be compromised.....	14
3.2. Authentication and Authorization.....	14
3.3. Erased weakness of passwords.....	15
3.4. The authentication factors.....	17
3.4.1. The knowledge factor.....	18
3.4.2. The possession factor.....	18
3.4.3. The characteristics factor.....	18
3.5. Two-factor authentication concept.....	19
3.6. Single-factor vs multi-factor authentications.....	19
3.7. Two-factor authentication benefits.....	20
3.8. Where and how to implement Two-factor authentication.....	21
3.9. Two-factor authentication success criterion.....	22
3.9.1. Customer acceptance.....	22
3.9.2. Token management difficulty.....	22
3.9.3. Credential replacement.....	22
3.9.4. System costs.....	23
3.10. Increase the security of accessing E-government web portal with Two-factor authentication.....	23
3.11. Two-factor authentication problems and challenges.....	24
 CHAPTER 4: Authentication factors and technologies.....	 26
4.1. Shared secret	26
4.2. Digital certificate.....	27
4.3. One-Time Password (OTP).....	27
4.3.1. HMAC-Based one-time password algorithm (HOTP).....	28
4.3.2. Time-Based one-time password algorithm (TOTP)....	28
4.4. Tokens with a display (disconnected tokens).....	29
4.5. Connected tokens.....	30
4.6. Magnetic stripe cards.....	30
4.7. Software tokens.....	31
4.8. Mobile phones.....	32
4.8.1. SMS one time password.....	32
4.8.2. Phone calls.....	32

4.8.3. Mobile application/software token.....	32
4.8.4. Smartphone push.....	33
4.8.5. Mobile signature.....	33
4.9. Biometrics.....	33
4.10. Image based authentication.....	35
4.11. Two-factor authentication methods examples.....	36
4.12. Recommendations and Best practices of Two-factor authentication with internet portals.....	36
CHAPTER 5: Comparative analysis of Two-factor authentication.....	38
5.1. Technical aspects.....	39
5.1.1. Easy of distribute to the public and cost effectiveness.....	40
5.1.2. Usability.....	43
5.1.3. Standardization.....	49
5.1.4. One Time Passwords implementation versus other existing methods.....	49
5.2. Online survey.....	51
5.2.1. Online survey results.....	52
5.3. Two-factor authentication methods tests.....	55
5.3.1. Test results.....	57
CHAPTER 6: Proposed solution and Implementation.....	64
6.1. Proposed main authentication method.....	65
6.2. Proposed alternative authentication method to be used as a backup.....	68
6.3. Proposed solution implementation.....	72
CHAPTER 7: Dissertation Results	84
7.1. Introduction.....	84
7.2. Results summary.....	84
7.3. Security limitations that are solved by proposed solution.....	87
7.4. E-government web portal user account creation and first login steps..	88
7.5. E-government web portal normal login steps.....	94
7.6. Emergency user account login steps.....	98

CHAPTER 8: Conclusion	104
8.1. Introduction.....	104
8.2. Research Objectives and Contributions.....	105
8.3. Future Work.....	107
8.4. Final Word.....	108
 REFERENCES.....	 109
APPENDIX A Online survey questions	112
APPENDIX B Online survey detailed results	114
APPENDIX C Sample testing screen shots.....	121
APPENDIX D Implementation source code.....	124

List of Tables

Table 1: The Factors of Authentication.....	18
Table 2: Two-factor implementations provided by different web services ...	24
Table 3: authentication factors technologies and related examples.....	36
Table 4: System and authentication requirements of each suggested method.....	40
Table 5: per user cost effectiveness for system owner (Government).....	41
Table 6: per user cost effectiveness per user for system user (Client).....	42
Table 7: Overview of usability dimensions.....	46
Table 8: Direct usability criterion of the eight suggested methods.....	48
Table 9: how Two-factor authentication with OTP performs better than the other existing systems.....	51
Table 10: Online survey participants age range.....	52
Table 11: Online survey participants qualification.....	53
Table 12: Online survey participants daily internet usage.....	53
Table 13: Online survey preferred second factor authentication.....	54

List of Figures

Figure 1: Multi-factor User/Server verification process	2
Figure 2: One-factor authentication system attacks	3
Figure 3: The authentication approaches	7
Figure 4: Password Length vs Password Entropy.....	17
Figure 5: the cost effectiveness for the system owner.....	42
Figure 6: the cost effectiveness for the system user.....	42
Figure 7: Outcome cost effectiveness for the system owner and system users	43
Figure 8: Total usability value of the eight suggested methods.....	48
Figure 9: Online survey SMS delivery assurance (Tripoli).....	58
Figure 10: Online survey SMS delivery assurance (Benghazi).....	59
Figure 11: Online survey SMS processing time (Tripoli).....	59
Figure 12: Online survey SMS processing time (Benghazi).....	60
Figure 13: Online survey Mobile push processing time (Tripoli).....	61
Figure 14: Online survey Mobile push processing time (Benghazi).....	61
Figure 15: Online survey Email message processing time (Tripoli).....	62
Figure 16: Online survey Email message processing time (Benghazi).....	62
Figure 17: Overall value of Two-factor authentication methods.....	64

Figure 18: Overall value of Two-factor authentication methods.....	70
Figure 19: initial login step.....	73
Figure 20: choosing mobile number to receive OTP	74
Figure 21: received SMS message contains OTP and login details	75
Figure 22: entering the received one-time password	75
Figure 23: image based authentication step	76
Figure 24: successful login to the system	77
Figure 25: confirmatory feedback SMS message	78
Figure 26: Successful login confirmatory Email	78
Figure 27: Wrong NID/Password entered	79
Figure 27: Wrong NID/Password entered	80
Figure 29: Wrong password alert Email	80
Figure 30: Wrong access code entered	81
Figure 31: Wrong access code alert SMS	81
Figure 32: Wrong access code alert Email	82
Figure 33: Image category mismatch	82
Figure 34: Image category mismatch alert SMS	83
Figure 35: Image category mismatch alert Email	83
Figure 36: main authentication method	86
Figure 37: Account creation and normal login process flow chart	92

Figure 38: Normal login process flow chart	96
Figure 39: Emergency account login steps - Password lost/forgot flow chart	100
Figure 40: Emergency account login steps - Mobile phone lost/SMS delays flow chart	102

1. Introduction

This dissertation answers the question about the best available authentication method that fits e-government web portal security needs based on system requirements, technical specification, cost, time for process, ease of use and ability to distribute it to the public users.

While the basic authentication method (User ID and password) is the most commonly used authentication mechanism. There are many shortcomings of a password authentication mechanism and argue that passwords are at the edge of breaking down, especially in the web environments. It is not secure enough for huge sensitive systems like e-government, banking and online payment systems. These reasons give the motivation to develop a vision of using Two-factor authentication on E-government web portal.

Two-factor authentication (also known as two-step verification) is an approach for authentication that requires the presentation of two or more of the three authentication factors: a knowledge factor (something only the user knows), a possession factor (something only the user has) and an inherence factor (something only the user is). After presentation of the first factor, the other party for authentication will be required to validate user identity.

Two-factor authentication is not a new concept. It has been used years ago. As an example, when a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card the customer slides into the machine (something the user has). The second factor is the PIN the customer enters through the keypad (something the user knows). Without the collaborating verification of both factors, authentication does not succeed. This scenario illustrates the basic concept of most Two-factor authentication systems: the combination of a knowledge factor and a possession factor.

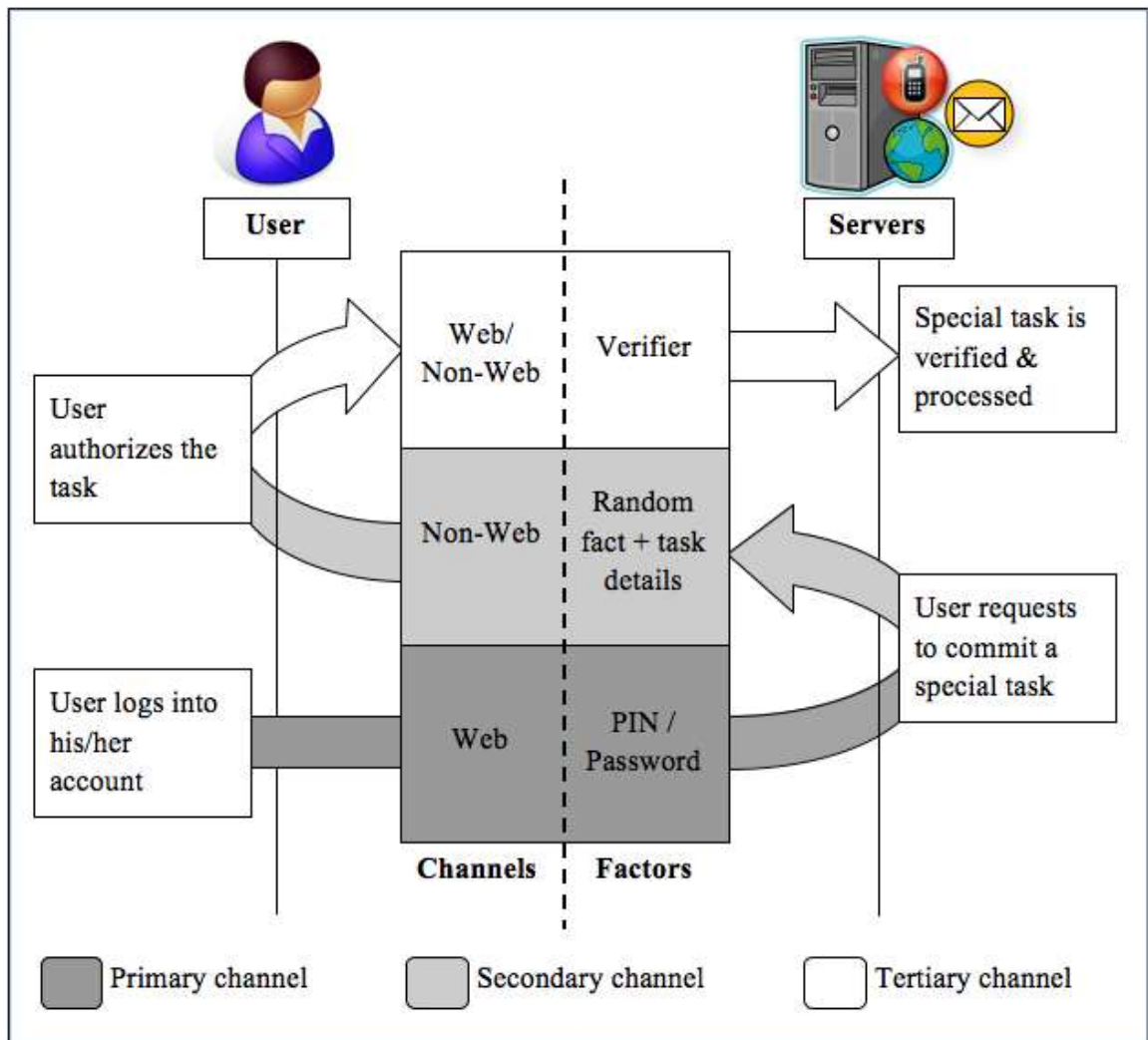


Figure 1: Multi-factor User/Server verification process

1.1. Problem statement

Armored the e-government web portal with Two-factor authentication system and how to implement it and the benefits of it are studied in this dissertation to secure the e-government web portal authentication process.

One of the major shortfalls of the one-factor authentication systems is the ease with which they can be cracked. This threat has increased over time as new and modern methods can be used for guessing and cracking authentication systems. The need for better and more secure systems has given rise to the concept of the Two-factor authentication system. In this

new system the first factor is just a usual password that created during creation of the account. The second factor will be one of the methods will be suggested later after study each one and decide the best method to implement with the e-government web portal.

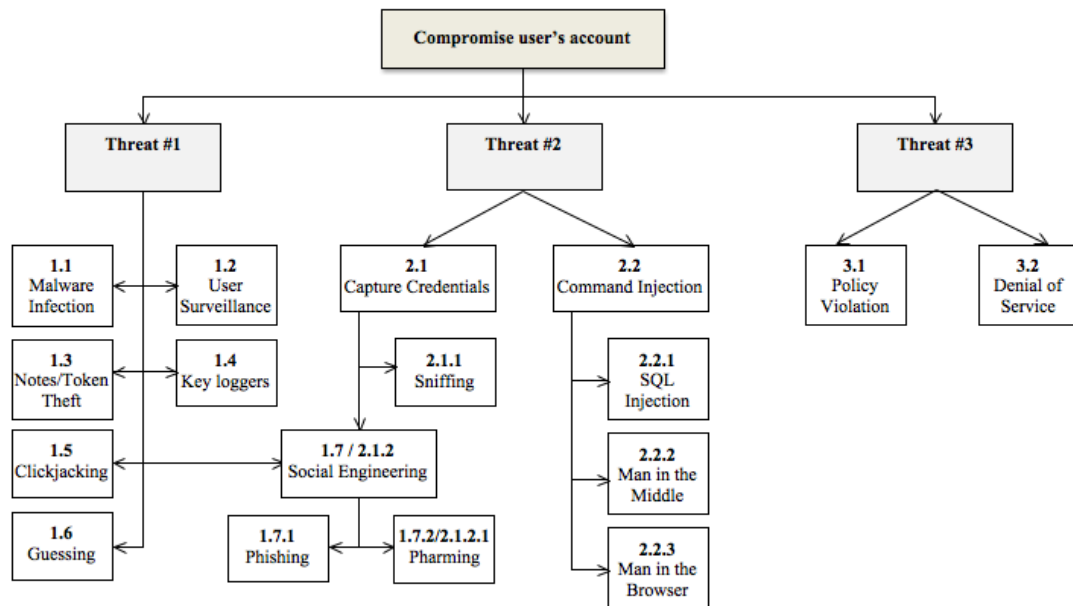


Figure 2: One-factor authentication system attacks

While it is easy for anyone to reach the login screen of the E-government web portal. Preventing unauthorized access is a big challenge for the system administrators and should be limited to authorized users to their accounts only. When an unauthorized person uses any of the common forms of malicious attacks against similar system when the system use password only authentication. An attacker may gain access to authorized user account illegally with compromised login credentials and use it illegally. In this case and unless the authorized user has changed his account password, nothing will prevent the unauthorized person from access it while he knows the valid login ID/Password. The implementation and usage of a Two-factor authentication system are more complex and difficult to crack by an attacker.

1.1.1. Two-factor authentication drawbacks

There are some limitations and vulnerabilities of Two-factor authentication systems.

Below are the known limitations and drawbacks of traditional Two-factor authentication systems from a previous studies^{[27][28][32][33][34]} in order to understand the security risks related to Two-factor authentication technologies.

- **Untrustworthy Interface:** In many cases, the security of an application boils down to the question as to whether a trustworthy user interface exists. Since Trojans or viruses might attack mobile devices, which have become as complex as PCs, this assumption cannot always be made. Besides that, the full range of browser-related vulnerabilities, e.g., phishing applies to mobile devices as well.
- **Theft/Loss of the Device:** An additional vulnerability, which is rather uncommon in the desktop world, but very serious when it comes to mobile devices (and laptops), is theft or loss of the device. Because mobile devices are very small and are usually carried around by their owners are stolen or lost very often. A mobile device could somehow be used to verify an individual's identity, but it should not contain the individual's identity because mobile phones are frequently lost or stolen.
- **Man-in-the-middle-attacks:** Even the best protection against physical attacks and an unbreakable encryption scheme do not help when the user token cannot identify the party on the other side. Especially in the case of online authentication, where the communication is tunneled via many hops, this vulnerability becomes a serious issue. The attacker inserts himself between the authentication server and the user token. Even if the channel is

encrypted, both sides believe they are talking to each other, and the attacker can intercept, delete or modify the communications.

- **Cryptographic attacks:** These attacks directly target the cryptographic algorithms. The scientific community is continuously reviewing published algorithms. Successful cryptographic attacks will, over time, lead to a need for greater key lengths.
- **Eavesdropping:** The communication between two contactless devices can be eavesdropped from a certain distance. In this case, the attacker would first record the communications from a close distance and later try to break the encryption (if any) with appropriate equipment. The most popular example for this vulnerability is a well-known weakness in the basic access control (BAC) mechanism deployed in electronic passports ^[32].

This dissertation will develop a solution that overcomes all the above drawbacks of Two-factor authentication systems

1.2. Motivation

Armored the e-government web portal with advanced Two-factor authentication system to secure the authentication process.

- Provide shielding for e-government web portal and their users from known security attacks that tries to gain access to their accounts
- Provide a strong, secure e-government web portal authentication system that avoids the drawbacks of traditional Two-factor authentication methods
- Obtain a higher authentication security guarantee than when using static password only or traditional Two-factor authentication technologies

1.3. Proposed Solution

This dissertation contributes to propose an advanced authentication system that has high security and decreases the risk of illegal access to the E-government web portal by using multi-step authentication system that involves two authentication factors:

- a. Something only the account owner (user) knows: User account password will be created alongside the user account itself and user can reset it via the portal at any time after successful login.
- b. Something only the account owner (user) has or get: Random one-time password the system will generate and send to the account owner via a different channel after he entered his user ID/Password in the login screen alongside the appearance of another screen asked for that security number to let the user complete the authentication process. The other channel the system will use to send the security number decided later during the thesis.

The proposed solution will also provide a custom designed image based authentication step as an added layer of security to combine the strength of the three authentication approaches: multilevel, multi-channel, and multi-factor and resist all illegal authentication threats. Figure 2 shows the authentication approaches.

As there are too many methods and techniques in Two-factor authentication. This thesis focuses on methods that usable with E-government web portal, and can be distributed among the public users of such huge system. It will be affordable and easy to implement and use for the ordinary people.

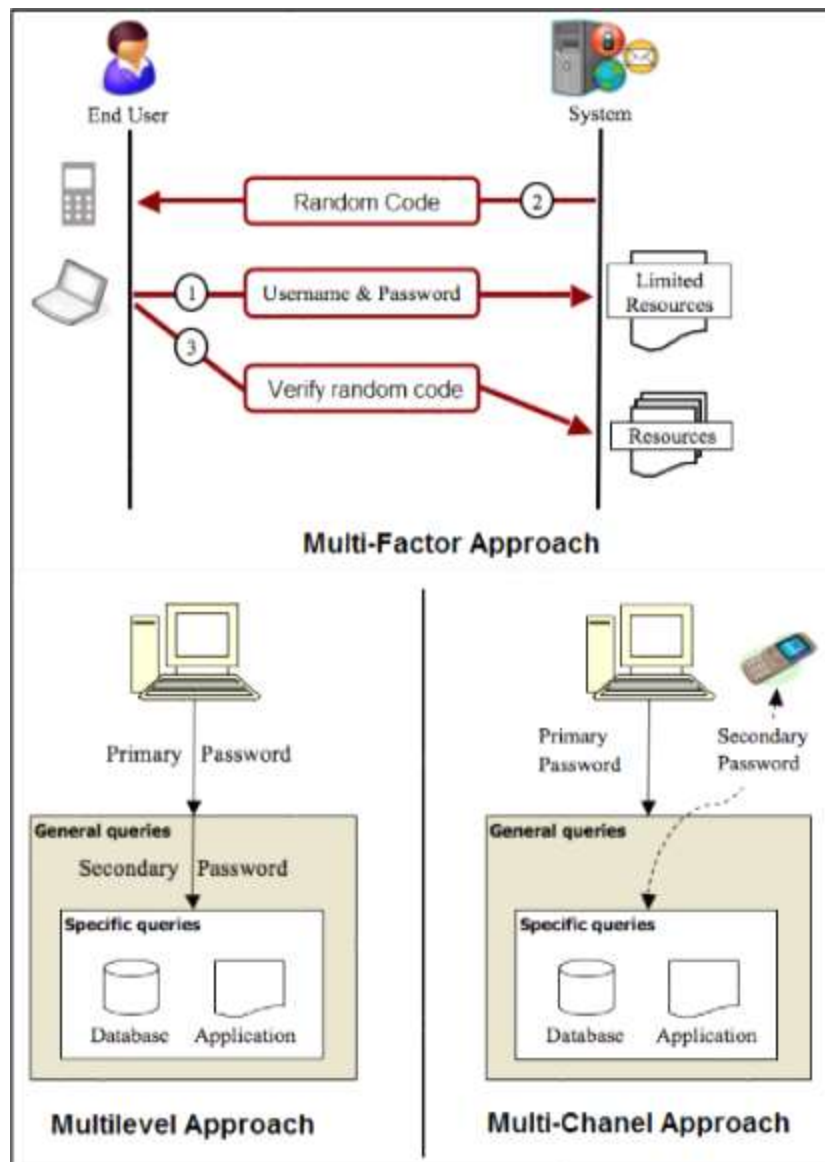


Figure 3: The authentication approaches.

1.4.Dissertation Layout

This dissertation organized into the following chapters:

Chapter 2 Internet portals security: This chapter gives a brief introduction of IT security and covers the security threats related to the authentication process. It also discusses authentication mechanisms implemented on major web and e-government portals.

Chapter 3 Background and authentication review: This chapter presents a review on authentication, its types, and implementation

mechanisms found in the industry. The chapter also analysis the authentication problem and Two-factor authentication success criteria.

Chapter 4 Authentication factors and technologies: This chapter reviews the various types of authentication factors. It also explains the authentication token technologies in detail. It also discusses Two-factor authentication methods examples and how they can be evaluated in practical terms.

Chapter 5 Comparative analysis of Two-factor authentication: To develop a strong authentication system. This chapter is studying the data gathered from a previous references, custom online survey, previous references, technical comparisons and trade-offs between eight methods that are widely used in Two-factor authentication systems, and also gives implementation and test results from several aspects and criteria that are required for e-government portal.

Chapter 6 Proposed solution and Implementation: This chapter proposed a final solution to implement Two-factor authentication on e-government web portal based on data gathered during the previous chapter. It also proposed a backup method of Two-factor authentication on e-government web portal to use in case of unavailability of the primary method.

Chapter 7 Dissertation Results: This chapter presents the dissertation problem solution that covers all the needed points. It also presents a written procedures of login process using the normal and backup methods that suggested from the evaluation of the data gathered through the previous chapters of this thesis.

Chapter 8 Conclusion: This final chapter concludes the study by giving an overview of this dissertation. It also summarizes the main results and lists future research paths.

2. Internet portals security

This chapter discusses the concept of IT security and covers the security threats related to the authentication process. It also discusses authentication mechanisms implemented on major web and e-government portals

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. The field includes all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction of data, and is of growing importance due to the increasing reliance on computer systems in most societies^[30]. It includes physical security to prevent theft of equipment and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security". Those terms generally do not refer to physical security, but a common belief among computer security experts is that a physical security breach is one of the worst kind of security breaches as it generally allows full access to both data and equipment.

Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data. Cybersecurity attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of cybersecurity is to protect data both in transit and at rest. Counter measures can be put in place in order to increase the security of data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization^[31]

A web portal is most often one specially designed web page, which brings information together from diverse sources in a uniform way. The main concept is to present the user with a single web page that brings together or aggregates content from a number of other systems or servers. Many governments already committed to creating portal sites for their citizens.

2.1. Web portals security risk

Web portals require a set of security requirements:

- **Authentication:** capability to identify who is using the services (person or software program). Processes of verifying that you are who you say you are.
- **Authorization:** capability to give rights access to resources. Process to verify someone has the rights to do what she is trying to do.
- **Confidentiality:** capability to prevent unauthorized access to information
- **Integrity:** Capability to prevent unauthorized modification of the data, and ensuring that information can be relied upon and is accurate and complete.
- **Traceability:** capability to chronologically interrelate any transaction to a person or system that performed the action in a way that is verifiable.

Note: This dissertation is about securing the authentication process. Authorization, confidentiality, integrity and traceability are beyond the scope of this dissertation

Security threats related to the authentication process discussed below. These threats discussed with respect to the web portal and include security risks related to the remote authentication process.

2.1.1. Replay

In a replay attack, the attacker records the data communicated during a successful authentication attempt. The attacker can then replay the recorded data and authenticate himself any time later.

2.1.2. Session hijacking

An attacker waits until the user authenticates against the verifier. Once the communication session is established, the attacker takes over the session.

2.1.3. Phishing

A phishing attacker traps the user through forged electronic communication. The victim provides its secrets to the attacker, considering it as the actual verifier. While the victim believes it is communicating with a trustworthy entity, it is actually communicating to an attacker.

2.1.4. Man-in-the-middle

In a man-in-the-middle (MITM) attack, the attacker places himself in the middle of a communication channel and poses itself as a valid verifier to the user and as a valid user to the verifier.

2.1.5. Insider attacks

The insider attack is someone inside the security perimeter deliberately compromises the security. The inside attackers pose a big threat to the organization's security. They can create opportunities for the attackers by deliberately revealing the internal authentication process and secret tokens.

2.1.6. Malware

Malware is a general term used for a piece of software trying to compromise the authentication process. Malware try to collect

confidential information and interfere in the authentication process using it. A malware can be a key logger, Trojan, computer virus or spyware, etc.

2.1.7. Password discovery attacks

Password discovery attack is the process of illegal recovery of the passwords.

2.1.8. Shoulder surfing

An attacker tries to get the secret information (pin, password) as the victim enters it on the keyboard. Even a partially successful shoulder surfing attack can be dangerous when used with other security threat combinations.

2.1.9. Social engineering attacks

Social engineering attackers achieve a certain level of trust, to persuade the victim to expose the secret. Social engineering attackers can use the Internet, telephonic conversation or even one to one conversation with the victim ^{[1][13]}.

3. Background and authentication review

This chapter presents a review on authentication, its types, and implementation mechanisms found in the industry. The chapter also analysis the authentication problem and Two-factor authentication success criteria

By definition, authentication means using one or more mechanisms to prove that the person is who he claims to be [7]. Once the identity of the human or machine validated, the access granted. There are three universally recognized classes of factors for authentication exist today, which is what the user knows (e.g. passwords, PIN's), what the user has (e.g. smart cards or tokens), and what the user are (e.g. fingerprints, face recognition, biometrics, etc.). Two-factor authentication is a mechanism, which implements two of the above-mentioned factors and considered stronger and more secure than the traditionally implemented one-factor authentication system. Recent work is trying alternative factors such as a fourth factor, e.g. somebody the user knows, which is based on the notion of vouching [7]. Only recently, Two-factor authentication systems based on mobile devices have started to gather some interest within the research community.

3.1. Problem Analysis

Two-factor authentication is an innovative authentication system that provides access to Web-based resources by using a two-way user authentication through two of the three authentication factors. It is used to solve the authentication flaws of the web-based Internet and Intranet portals.

Two-factor authentication designed to provide security for Web-based Internet and Intranet applications, and requires users to authenticate themselves with two unique criteria, a username and password, and a second method using other authentication factor during the

authentication[8] before the user allowed to access a secured web resource.

As the Web-based portals become an important tool for government transactions, the level of security becomes a major concern in an organization's transaction system. Transactions in these days are secured using passwords.

3.1.1. How the traditional password system can be compromised

- Passwords can be captured while they are being entered into the browser. For instance, by 'trojan- horse' applications which most of the users might have unknowingly installed, while installing shareware applications, while reading a malicious Email, or while even visiting a dubious website.
- Some users may save their passwords on their internet browsers, which can be seen by anyone with access to the terminals, including their PC technician, or if they are using a cyber cafe machine, anyone who uses that terminal after them.

3.2. Authentication and Authorization

Authentication and authorization are two different concepts and should not be confused with each other.

Authentication is the process of establishing confidence in the identity of users or information systems. It is the process to verify, if the entity is the one it claims to be. Authentication is the key to ensure security. Authorization is the process of determining access rights to the secured resources. An authorization process occurs after successful authentication process. It determines the level of access to a user resource and makes sure that a certain entity can exactly do what it is supposed to do ^[9].

Note: Authorization process is beyond the scope of this dissertation.

3.3. Erased weakness of passwords

Password authentication is the most commonly used single-factor authentication mechanism. This section analyses the shortcomings of a password authentication mechanism and argues that passwords are at the edge of breaking down, especially in the web environments.

A password is a secret shared between the system user and the system verifier. A system user is one who claims to know the secret, and the system verifier is one who confirms or denies this claim. The correct user name and password are provided to the system verifier to access the secured resources.

Password authentication has received criticism over the past for allowing users to choose weak passwords. Weak passwords are easy to crack. The studies have shown that a large number of users choose weak passwords. Twenty two percent of the user-chosen passwords could be easily recovered, according to Columbia University research. Bruce Schneier used a publicly available password recovery software and experimented that fifty five percent of the MySpace passwords could be cracked within eight hours. The password recovery software used was capable of testing 200,000 passwords per second. He further mentioned that "password1" was the most commonly used passwords among the users. These studies show ignorance and carelessness among users while selecting passwords [9].

Online attacks can be avoided by blocking the user's account after a certain number of wrong authentication attempts. While this solution seems helpful at the beginning, it also brings some other problems.

Disabling an account on multiple wrong authentication attempts opens a door for the denial of service attacks. The attacker can easily disable the actual user from using its account by intentional false attempts.

Recent security guidelines force the users to choose random passwords [10]. The idea behind these guidelines is that randomness increases the password strength. Strong passwords are those with higher randomness involved. Users are asked to use numerals along with capital and lower-case letters in the passwords to increase its randomness. They are encouraged to use long passwords with eight or more characters [11].

Figure 4 shows the relation between entropy (disorder or randomness in the password) and password length with respect to different password choosing techniques. The passwords can be chosen randomly, using abbreviations, using phone numbers or using a combination of all these for any given password length, a randomly chosen password has the highest entropy.

A password can be made stronger by increasing its randomness. It is the only option to strengthen the password authentication. On the other hand, the password randomness is already at its peak. Users using numbers, special characters, small and large alphabet letters in passwords. Most of the organizations already require strong passwords with up to eight character length. If it forces the users to choose a highly random password, it will be difficult to memorize it and will be inclined to write it down somewhere, resulting in increased risk of insider attacks.

System generated passwords have high entropy values. At the same time, it is hard to memorize and more prone to be written down by users. Zviran and Haga in which 106 students participated conducted a similar research.

The students asked to choose a password of their own choice. In addition, they were given a random password to remember. After a three-month gap, the students asked to recall both the chosen and random password. The probability of writing down the passwords increased almost five times for random passwords ^[12]. The results shows that forcing users to choose high entropy passwords would not help in the future.

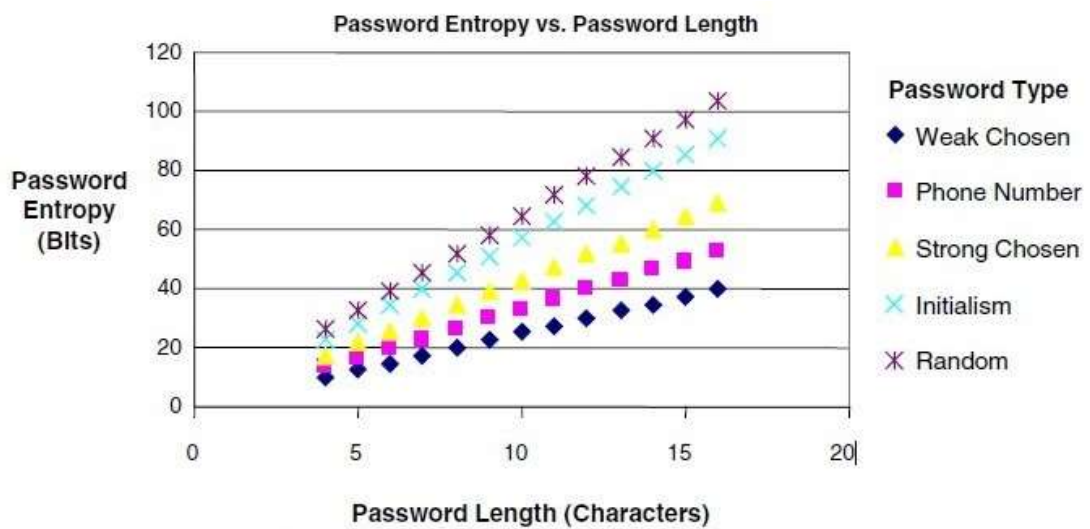


Figure 4: Password Entropy vs Password Length ^[13]

That makes it clear that passwords do not provide further room for strong authentication and any attempt to use passwords only will result a weak authentication system.

3.4. The authentication factors

The possible approach of authenticating system user falls under three categories ^[14]. These categories are based upon the factors of authentication used during the authentication process. There are three factors of authentication, as explained below

3.4.1. The knowledge factor

Something the user “know” falls into this factor. A secret is shared between the user and the information security system. The shared secret is used as an authentication token. Some examples of the secret are password, PIN, personal question or a picture.

3.4.2. The possession factor

Something the user “has” is used as an authentication token during the authentication process. The possession factor can be a software or a hardware token. Some examples are smart cards, USB tokens and one-time password generators.

3.4.3. The characteristics factor

Authentication tokens belonging to this factor are based on something the user “is”. Each person has certain characteristics, which distinguish him from others. Biometrics like fingerprints, iris and retina patterns can be used as authentication tokens.

Table 1 provides some examples of authentication tokens related to the three authentication factors.

Table 1: The Factors of Authentication

Knows	Something a user	
	Has	IS
Password	Smart card	Fingerprints
PIN	Cryptographic key	Retina
Secret question	USB token	Iris
	SIM card	Face
	OTP Generator	Hand geometry

3.5. Two-factor authentication concept

The Two-factor authentication is an extra layer of security that is part of multi factor authentication. in today's world of increasing digital crime and Internet fraud, many people will be highly familiar with the importance of online security, logins, usernames and passwords, but they do not know what it is or how it works even though they may use it every single day.

With standard security procedures (especially online) only requiring a simple username and password, it has become increasingly easy for criminals to gain access to a user's private data such as personal or financial details.

Two-factor authentication is a combination of any two of the above three factors. When this is applied throughout the business world, it is usually made from knowledge and possession factors. This is because the biometrics is very expensive and very complicated to roll out. By providing two separate factors of system logon provides protection to the real user.

Using a Two-factor authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via Email, because the criminal would need more than just the users name and password details.

3.6. Single-factor vs multi-factor authentications

Single-factor authentication is any authentication system uses only one of the three authentication factors (knowledge factor, possession factor or characteristics factor). Single-factor authentication does not require another authentication factor in the authentication process. Two or more

than two single-factor authentication method must be combined together to provide a Two-factor authentication solution.

Multi-factor uses more than one authentication factor. A multi-factor belongs to a first authentication factor and requires an extra factor or two for the success authentication process. The authentication will not complete successfully without this extra authentication factor or factors. Any two of authentication factors can be used in a Two-factor authentication solution.

3.7. Two-factor authentication benefits

Two-factor authentication is a practical way to add further security to the user logon sequence. In the modern connected world, a password is the weakest link.

Traditional Two-factor authentication in the enterprise solutions has always relied on the use of hardware tokens that users have to carry on their person. The most famous being the hardware token, which would reside upon the user key ring. These tokens generate one-time passwords for the second stage during the login process. However, hardware tokens can be considered costly.

Another method is using a mobile phone or device that already in place provides a mechanism to seamlessly enable and deploy over one hundred thousand user per hour. It works with all phone types, from landlines to smartphone platforms. As well as supporting devices such as iPads, Tablets, laptop and desktop environments.

3.8. Where and how to implement Two-factor authentication

Two-factor authentication is a good solution for Government, Banking, Retail, Manufacturing and any web application.

More people now need to utilize networked devices, especially to connect to online resources and communicate with others using the Internet. The variety of online services offered has attracted people from different backgrounds to communicate and utilize them. Along with other factors, such as availability of the Internet and communication services, even the average citizen who is barely computer literate is now communicating and interacting, on daily basis, with many online services.

E-government web portal users encouraged to carry out critical online transactions. Such online services are crucial and pose greater damage to users and government than do other online services.

E-government can adopt Two-factor authentication for many use cases to protect governmental information and data against unauthorized access. Those use cases include the following:

- Internal or local access: Employee access to critical applications, and/or administrator access to E-government servers and network devices.
- External or remote access: Remote or mobile employee access to the E-government backend systems via the VPN or portal access.
- Citizens/users entry points: Between the public network/Internet system users and the internal E-government network.

The first and second use case are beyond the scope of this dissertation

3.9. Two-factor authentication success criterion

Many authentication solutions are available these days. The success of an authentication solution is determined by its technical and non-technical adoption feasibility. In addition, the acceptance level of a particular solution is determined by the solution providers as well as by its users. The goal is to provide a solution that can achieve the entire below success criteria:

3.9.1. Customer acceptance

Customer acceptance plays an important role in the success or failure of Two-factor authentication solution. The required skill level and the required hardware or software support indicate customer acceptance.

User-unfriendly Two-factor authentication processes require client education and result in higher cost. On the other hand, simplistic solutions might not provide the required security level. A successful Two-factor authentication solution should simultaneously provide high-security level and ease of use. Software and hardware requirements of the Two-factor authentication system are the major acceptance indicators.

3.9.2. Token management difficulty

The success of Two-factor authentication solution is highly depended on the creation, distribution and management of the Two-factor authentication hardware tokens. Some hardware tokens are easier to manage than others. In a trivial solution like passwords, the users can create a password remotely and there is no need to distribute any hardware tokens.

3.9.3. Credential replacement

Authentication hardware tokens expire after a certain period and must be replaced. Furthermore, the compromised hardware tokens should be revoked and replaced with the new ones. A successful

Two-factor authentication solution should allow smooth replacement of hardware tokens if implemented on a large scale as well as on a small scale.

3.9.4. System costs

Cost is a major decision factor for system owners to adopt a security solution. The cost should be calculated for the entire estimated life cycle of the Two-factor authentication solution. Some solutions incur high acquisition cost and low maintenance cost while others may incur low acquisition cost and high-maintenance cost. A solution with a higher acquisition cost is not necessarily a costly solution. In the long run, it might be cheaper than the one incurring low acquisition cost and high maintenance.

3.10. Increase the security of accessing E-government web portal with Two-factor authentication

The Internet is a medium who allows a large number of people or organizations, to communicate with each other in a few seconds, without much effort and charges. Now on-line fraud is very popular all over the world. It has become a major source of revenue for criminals. The most practical way to strengthen authentication is to require a second factor after the username/password stage. Since a password is something that a user knows, ensuring that the user also has something thwarts attackers who steal or gain access to passwords.

Traditional Two-factor authentication solutions use hardware tokens. Hardware tokens have high cost in large enterprise systems like e-government. It takes time and effort to distribute them, track who has which one, and replaces them when they break. They are easy to lose,

hard to use, and users consistently report high levels of frustration with token-based systems.

That advantage the mobile phone as the second factor. It is a device that people already have, know how to use, and notice when it is missing. Using an existing device reduces deployment and training costs, and improves the end-user experience of the entire system and it works internationally. In the simplest case, users receive an SMS message containing the access code.

Table 2: Two-factor implementations provided by different web services

Web Services	1st Authentication Factor	2nd Authentication Factor
Amazon Web Services	Password	Hardware token generator OR Software token generator
Google	Password	Software token generator OR Message sent to mobile phone
Facebook	Password	Software token generator OR Message sent to mobile phone
PayPal/eBay	Password	Hardware token generator OR Text Message sent to mobile phone
Dropbox	Password	Software token generator OR Message sent to mobile phone

3.11. Two-factor authentication problems and challenges

Two-factor authentication is not easy to implement. For instance, the security firm Duo Security recently reported a serious flaw in Google's two-step login process. The problem, which was soon fixed, stemmed from Google applying the feature across its many services. Despite being

one of the Internet's giants, while its technology was solid, its implementation was flawed.

Users will likely see Two-factor authentication as a hassle. They may find it tedious to have a trusted device or hardware token with them at all times in order to log in. Therefore, some authentication scenarios may require an option for users to skip Two-factor authentication for frequently accessed systems.

These points of a Two-factor authentication implementation may be eased with the following measures:

- Select a factor that fits enterprise needs. The options include hardware-/software-based tokens or sending SMS messages to smartphones. Enterprises that are geographically centralized will appreciate physical tokens, while others with a constantly moving workforce may wish to use software-based tokens or mobile options.
- Provide sufficient user support. Getting the back-end server components installed and configured takes a while, and integrating and testing applications takes time too. Self-service, sufficient training and a well-staffed helpdesk and support team will be essential to get users accustomed to the technology and able to successfully navigate through the transition period.
- Two-factor authentication is becoming an essential element of modern enterprise IT security programs, yet it remains complex and difficult to understand, implement and manage.

There are many Two-factor authentication mechanisms, this dissertation analyzes these systems based on operational, financial and relative security aspects. Even though, it is a bigger leap in authentication security than password-only systems. The next chapter discusses the technologies used by Two-factor authentication.

4. Authentication factors and technologies

This chapter discusses the various types of authentication factors. It also explains the authentication token technologies in detail. Discusses Two-factor authentication methods examples and how they can be evaluated in practical terms.

As mentioned in the introductory chapter, Two-factor authentication requires the presentation of two or more of the three authentication factors, the knowledge factor, the possession factor and an inheritance factor. These technologies are important to mention as all the authentication tokens are based on them. One or more of these technologies are combined to construct an authentication token.

4.1. Shared secret

A shared secret is an old and common authentication technique. It belongs to the knowledge factor of authentication. The claimant and the verifier share a secret with each other and the secret is known only to both of them. The shared secret is commonly used with a user ID during the authentication. Examples of shared secret are password, PIN and a personal question.

Passwords are widely used for authentication, but the fact is, they do not resist most of the security threats. High entropy passwords can partially resist the password discovery attacks and shoulder surfing attacks.

Shared secret as a knowledge factor (Password, PIN and Pattern) is still mandatory in all today authentication standards. It is always used as the first authentication factor along with the user ID. For the second authentication factor, there are many methods used as a second authentication channel.

4.2. Digital certificate

The user token and the system authentication verifier use digital certificates to authenticate themselves against each other.

Digital certificates can be self-signed or signed by a certificate authority. Both the mechanisms provide the same security level. The difference is that all self-signed certificates must be stored on the system verifier side.

The certificates are resistant to the security risks of the shared secrets. While a certificate might be stolen or copied, it cannot be known or revealed to attackers. Attacks like shoulder surfing, replay and brute-force are ineffective on the certificates.

4.3. One-Time Password (OTP)

One-time passwords are generated by an algorithm. They are different from typical passwords, as they do not repeat themselves. Every next password generated will be different from the previous ones. The password-generating algorithm uses an underlying secret as a seed. The seed is shared between the user token and the system authentication verifier. During the authentication process, the user token and the system authentication verifier generate the one-time password individually. The user sends the one-time password to the system authentication verifier, which compares it with the locally generated password. The user is authenticated if both the passwords match.

Nowadays, One-time passwords are very common. Generally, via SMS sent to registered mobile phone for authentication. Scratch cards or vouchers for mobile phone credit also use one-time passwords.

The password generating software can be embedded in a hardware. Java Smart cards, USB dongles, and mobile phones can run the password generating software to generate one-time passwords. In addition, hardware disconnected tokens are using one-time password.

One-time passwords technology has certainly increased the customer acceptance of Two-factor authentication. It can be distributed in software, hardware and even in paper form and open new opportunities for Two-factor authentication solutions. One-time password algorithms come in two forms:

4.3.1. HMAC-Based one-time password algorithm (HOTP): HOTP is an event-based password-generating algorithm. The passwords are generated based on Hashed Message Authentication Code (HMAC) ^[16]. The user token and the system authentication verifier agree on a counter value at the beginning. The counter is incremented each time the event occurs, i.e. a password is generated. The user and the verifier keep track of the counter value. The difference in counter value on both sides is known as window size ^[16]. If the password generated on the user's side is out of the window size, it will be rejected from the verifier. The user token has to synchronize the counter with the verifier in this case.

4.3.2. Time-Based one-time password algorithm (TOTP): Time-based one-time password algorithm is an extension of the HOTP algorithm to support the time-based moving factor ^[17]. It is an improved version of the previous algorithm. HOTP had one major drawback. The passwords generated by HOTP are not time sensitive.

They have no validity time limit and can be used any time later. This increases the security risk as the password-generating token can be shared with an attacker for a short period. The attacker can note down the password and uses it later to authenticate itself. As the passwords

do not expire, the attacker has full freedom to use the stolen password.

Time-based one-time password algorithm prevents this situation. The passwords generated by TOTP algorithm are valid only for a short period. The passwords expire after the validity period and cannot be used for authentication. The password validity time can be set in the algorithm and is normally set to 30 to 60 seconds.

4.4. Tokens with a display (disconnected tokens)

A number of types of pocket-sized authentication token are available, which display a changing passcode on an LCD or e-ink display, which must be typed in at an authentication screen, thus avoiding the need for an electronic connection. There are three types of disconnected tokens:

- In a "sequence-based" token, the token may have a button that is pressed to switch it on and display a new passcode.
- In a "time-based" token, the token generally contains a quartz time source, allowing the absolute time to be used as the challenge and a new pass code to be displayed (usually) every 30 or 60 seconds.
- The token may have a small keypad on which a challenge can be entered. This may either be a fixed PIN assigned to the user, or a challenge generated by the server and displayed on the authentication screen, or both.

Display tokens have the advantage that no drivers or electronic interfaces are required for the user access device. A disadvantage in some sectors is that the display is usually small, and may be difficult to read for visually impaired users.

The display tokens are generally designed to be attached to a key ring, or as a device that can be carried in a pocket or handbag.

4.5. Connected tokens

Like display tokens, connected tokens embody a shared secret. This is normally interrogated by a challenge/response to avoid exposing it. Most types of connected tokens have at least some level of copy protection. For electronic tokens that require a physical connection, the form-factor of the electronic interface used to connect the token to the machine (smartcards, USB port, audio port) sets a minimum size of the token. Some types of tokens require a device-reader, possibly with special device drivers, whereas others use an interface which is almost universally available such as USB.

In a business or government environment, where the details of the user-access-device (connected-token hardware) and its capabilities are known, and any required device drivers are deployed in advance, an authentication-token may be more convenient than a pin or a passphrase, as there is no need to type a passcode.

Tokens can be compromised by been stolen/lost, by being cloned, or by the user giving their token to someone else, but tokens can be denied if the user loses them or the user/adversary ruins the token and/or token-reader.

4.6. Magnetic stripe cards

Magnetic stripe cards (credit cards, debit cards, ATM cards, etc.) are easily cloned and so are being or have been replaced in various regions by smart cards, particularly in banking. However, even though the data on the magnetic stripe is easily copied, researchers at Washington

University in St. Louis have found[18] that the random and unique disposition of the billions of individual magnetic particles on each magnetic stripe can be used to derive a "magnetic fingerprint" which is difficult, but not impossible to clone.

It does require a special reader that can read the magnetic fingerprint value, but these readers can be swapped out incrementally as old readers wear down. So the actual investment could be incorporated as an incremental increase of current business cost expectations.

4.7. Software tokens

It is a computer-simulated software-based tokens. The functionality of any disconnected token can be emulated as a "soft token" on a PC or smartphone using deployed software, where that device itself becomes the possession factor. This saves on deployment costs, but against that, the secret is vulnerable to any attacker or malware that can gain full access to the device. The Zeus Trojan, which can now infect mobile devices running Android or BlackBerry OS, specifically targets banking credentials and may forward them to the attacker at a website set up for the purpose, or by SMS messaging. ^[18]

As explained earlier, hardware tokens are hardware devices having storage capacity and optionally an integrated chip to do some computation. They can store a cryptographic key or can compute one-time passwords using their computing capability.

Software tokens are software implementations of hardware tokens. They can optionally use the computational capability of the platform they are installed on.

4.8. Mobile phones

A new category of Two-factor authentication tools transforms the user's mobile phone into a token device using either SMS messaging, an interactive telephone call, or via a downloadable application to a smartphone. Since the user now communicates over two channels, the mobile phone becomes a Two-factor authentication mechanism.

4.8.1. SMS one time password: SMS one time password uses information sent in an SMS to the user as part of the login process. One scenario is where a user either registers (or updates) their contact information on a website. During this time, the user is also asked to enter his or her regularly used telephone number(s) and verifying it during the registration process. The next time the user logs into the website, they must enter their username and password, if they enter the correct information, the user then chooses the phone number at which they can be contacted immediately from their previously registered phone numbers. The user will be instantly called or receive an SMS text message with a unique OTP. The user then enters this OTP into the website to prove their identity, and if the OTP entered is correct, the user will be granted access to their account. This process provides an extra layer of online security beyond username and password.

4.8.2. Phone calls: In 2011, OTP has started offering to mobile and landline phones via phone calls as a Two-factor authentication method. The user can receive the OTP via an automated call using text-to-speech conversion. It is almost used as a backup Two-factor authentication method if he cannot use the primary one after signing in with their account password.

4.8.3. Mobile application/software token: Smart phones and tablets can use a dedicated mobile device application for secure access to online services. The mobile device application uses the Web browser or

Web service capabilities of the device for authentication and subsequent access to the service.

4.8.4. Smartphone push: The push notification services offered by modern mobile platforms to provide a real-time challenge/response mechanism on a mobile device. Upon performing a sensitive transaction or login, the user will instantly receive a challenge pushed to their mobile phone, be prompted with the full details of that transaction, and be able to respond to approve or deny that transaction by simply pressing a button on the mobile phone. Smartphone push authentication has the capability to not only be more user-friendly, but also more secure as a mutually-authenticated connection can be established to the phone over the data network. This method can be a module of the mobile application.

4.8.5. Mobile signature: Mobile signatures are digital signatures created on a SIM card. In such a system, text to be signed is securely sent to the SIM card of a mobile phone. The SIM then displays the text to the end-user who checks it before entering a PIN code to create a signature, which is then sent back to the service provider. Mobile Signature systems have been in use over several years. However, as with magnetic card and client digital certificate solutions, they are vulnerable to malware, are costly to deploy and support, and are strongly resisted by consumers.

4.9. Biometrics

Biometric authentication also satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, Voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to authenticate to the system or vice versa.

Introducing a new user in the biometric authentication system is called enrollment ^[19]. The samples of the user are taken during this process. Samples can belong to physical or behavioral characteristics and are converted into mathematical model templates. The mathematical model templates are stored in a database for comparison during the authentication phase.

Biometrics authentication requires specific hardware and software installed on the user's computer. While this type of authentication is suitable in limited applications, this solution may become unacceptably slow and comparatively expensive when a large number of users are involved. In addition, it is extremely vulnerable to a replay attack: once the biometric information is compromised, it may easily be replayed unless the reader is completely secure and guarded. Voice biometrics have the distinct advantage that it can ask the user to say random phrases, and thereby significantly reduce the risk of a successful replay attack. Finally, there is great user resistance to biometric authentication. Users resist having their personal physical characteristics captured and recorded for authentication purposes. In short, selection and successful deployment of a biometric authentication system need careful consideration of many factors.

Biometric information may be mechanically copied and cannot be easily changed. This is perceived as a key disadvantage since, if discovered, the compromised data cannot be changed. A user can easily change his or her password. However, a user cannot change their fingerprint.

Historically, fingerprints have been used as the most authoritative method of authentication. Other biometric methods such as retinal scans are promising, but have shown themselves to be easily spoofable in practice.

International travelers to many countries are now routinely required to provide fingerprints and/or iris scans to pass. This stockpile of records reduces the strength of biometric-protected resources. For example, these governments can now potentially unlock that traveler PC or decrypt his flash drives.

Based on the above and due to high implementation and usage cost for thousands of home users who will be hard for them to get the required hardware readers. Using biometric data like fingerprint and iris recognition as a second authentication factor seems to be hard to implement to secure e-government web portal access, but this dissertation will continue to consider it as a possible Two-factor authentication solution for e-government web portal.

4.10. Image based authentication

It is an advanced modern authentication technology. The process of image recognition authentication can involve several tasks. These tasks include, but are not limited to, evaluation of image structure and content and metadata analysis.

One of the techniques of Image based authentication is based on a user's successful identification of his image password set. After the username is sent to the authentication module, it responds by displaying an image set, which consists of images from the user's password set mixed with other images. The user is authenticated by correctly identifying the password images ^[37]. The secret could be based on password image category that belongs to (Cars, buildings, etc.).

4.11. Two-factor authentication methods examples

The technologies mentioned above are used to generate different types of authentication methods. Different combinations of authentication factors technologies give rise to different methods. Table 3 provides some examples of well-known tokens with respect to the technologies used.

Table 3: authentication factors technologies and related examples.

Technologies		Example Tokens
Shared Secrets		Password, PIN, Secret Questions
One-time passwords		TAN Lists, Messages sent on telephone, Scratch cards
Digital Certificates		Self-signed, Issued by a certificate authority
Software tokens	One-time passwords	Mobile devices with one-time password generating software installed. Windows desktop applications are also available to generate one-time passwords.
	Digital Certificates	Cryptographic token placed on a hard drive or imported in a web browser.
Hardware tokens	One-time passwords	Separate hardware tokens generating one-time passwords.
	Digital Certificates	USB tokens, Smart Cards
Biometrics		Fingerprint recognition, Retina recognition, Face recognition, etc.

4.12. Recommendations and Best practices of Two-factor authentication with internet portals

Two-factor authentication as a technology has matured in recent years, and technology costs have gone down significantly.

The implementation pricing of Two-factor authentication depends on the scenarios. For example, the industry verticals, and the size of the enterprise, the usage pattern, user geography, helpdesk presence and sensitivity of the business or data.

System owners should consider the recommendations listed here while identifying their Two-factor authentication needs and plan the project accordingly.

- **Understand the organization IT environment:** This could include understanding the technology landscape that's used inside or outside the enterprise to access information or data and knowing how the IT policies are enforced and what protections are in place. For example, are the users allowed to access the portal information through mobile devices?
- **Find the target users:** Is the Two-factor authentication considered only for selected business units or for remote users as well? In general, most organizations only offer Two-factor authentication for remote access. Limit the implementation, at least in the early stages, to specific use cases.
- **Adopt a risk-based approach:** Most organizations today implement a technology if it helps reduce the risk. Therefore, when there is not a clear scope or group of target users, it will be hard to consider a best effective Two-factor authentication implementation.
- **Avoid unnecessary cost and complexity:** The overall cost of the implementation may vary from scenario to another, depending on the size and requirements of the enterprise. Take into account the number of users, datacenter and users' locations, plus support and help desk coverage factors when determining the cost.

5. Comparative analysis and tests of Two-factor authentication

This chapter will gather data from a custom online survey, previous references, technical comparisons and trade-offs between eight methods that are widely used in Two-factor authentication systems, and also perform tests to the methods from several aspects and criteria that are required for e-government portal authentication system which is:

- Technical aspects as easy of distributing to the public
- Cost effectiveness
- Usability
- Delivery assurance
- Second factor processing time

The methods that will be compared are:

- Hardware Token (Disconnected)
- Hardware Token (Connected)
- Mobile Phone SMS
- Mobile software token
- Mobile push notification
- Email Message
- Biometric (Finger print)
- Biometric (Iris recognition)

The methods that will be tested are:

- Mobile Phone SMS
- Mobile software token
- Mobile push notification
- Email Message

The results of trade-offs, online survey and tests will evaluate the proposed methods to reach a decision on the most appropriate primary and backup Two-factor authentication method for e-government portal.

5.1. Technical aspects

To implement Two-factor authentication with Internet portal, a special add-on should be added to the web portal infrastructure. These add-ons depend on the Two-factor authentication method implemented. An OTP algorithm generator and verifier are mandatory to generate and verify OTPs that will be sent via SMS, Email message or identified by disconnected tokens. Besides an SMS gateway or mail server. Furthermore, a database contains the system users finger print or and eye retina data is mandatory in case of using biometrics. Software token and mobile push also require a special equipment.

The table 4 shows the system and authentication requirements of each suggested method in this dissertation

Table 4: System and authentication requirements of each suggested method

#	System Requirements	Authentication requirements
Hardware Token (Disconnected)	Authentication server with generation algorithm	ID\Password with OTP delivered via disconnected token
Hardware Token (Connected)	Authentication server and authorization server	ID\Password with connect the token into the PC
Mobile Phone (SMS)	Authentication server with generation algorithm	ID\Password with OTP delivered via SMS text message
Mobile Phone (Software token)	Authentication server with generation algorithm	ID\Password with OTP delivered via mobile application
Mobile Phone (Push)	Authentication server and authorization server	ID\Password with push notification delivered via mobile application that require approve
E-mail Message	Authentication server with generation algorithm	ID\Password with OTP delivered via E-mail
Biometric (Finger print)	Authentication server and authorization server	ID\Password with slides the fingerprint on the reader
Biometric (Iris recognition)	Authentication server and authorization server	ID\Password with reading Eye retina print by a special reader

5.1.1. Easy of distributing to the public and cost effectiveness

There are drawbacks to multi-factor authentication that are keeping many approaches from becoming widespread. Some users have difficulty keeping track of a hardware token or USB plug. Many users do not have the technical skills needed to install a client-side software by themselves.

Generally, multi factor solutions require additional investment for implementation and costs for maintenance. Most hardware token-based systems are proprietary, and some vendors even charge an annual fee per user. Deployment of hardware tokens is logistically challenging. Hardware tokens may be damaged or lost and issuance of tokens in large

industries, especially within large enterprise e-government portal needs to be managed.

The cost effectiveness is two sided. System owners/operators and system users. Each side has its own cost for the same criterion. The cost effectiveness involves the financial and operational cost.

The suggested Two-factor authentication methods issuance, maintenance, implementation and replacement cost effectiveness displayed below for the system owner and system users. The tables 5 and 6 and graph figures 5 and 6 shows the cost effectiveness for the system owner and system users. The figure 7 shows the outcome cost effectiveness for the system owner and system users.

Table 5: per user cost effectiveness for system owner (Government)

Method Criterion	Disconnected Hardware Token	Connected Hardware Token	Mobile Phone SMS	Mobile Phone Software token	Mobile Phone Push	E-mail Message	Biometric (Finger print)	Biometric (Iris recognition)
Issuance cost	High	High	Low cost	Low cost	Low cost	Low cost	Medium	Medium
Maintenance cost	High	High	Low cost	Low cost	Low cost	Low cost	Low cost	Low cost
Implementation cost	High	High	Low cost	Low cost	Low cost	Low cost	Medium	Medium
Replacement cost	High	High	No cost	No cost	No cost	No cost	No cost	No cost
Total Points	12	12	3	3	3	3	5	5

Table 6: per user cost effectiveness per user for system user (Client)

Method Criterion	Disconnected Hardware Token	Connected Hardware Token	Mobile Phone SMS	Mobile Phone Software token	Mobile Phone Push	E-mail Message	Biometric (Finger print)	Biometric (Iris recognition)
Issuance cost	Low cost	Low cost	Low cost	Low cost	Low cost	Low cost	Medium	High
Maintenance cost	Low cost	Low cost	Low cost	Low cost	Low cost	Low cost	Medium	High
Implementation cost	Low cost	Low cost	Low cost	Low cost	Low cost	Low cost	Medium	High
Replacement cost	Low cost	Low cost	No cost	No cost	No cost	No cost	Medium	High
Total Points	4	4	3	3	3	3	8	12

Figures 5, 6 and 7 shows the cost effectiveness for the system owner, user and the outcome cost effectiveness for the system owner and system users.

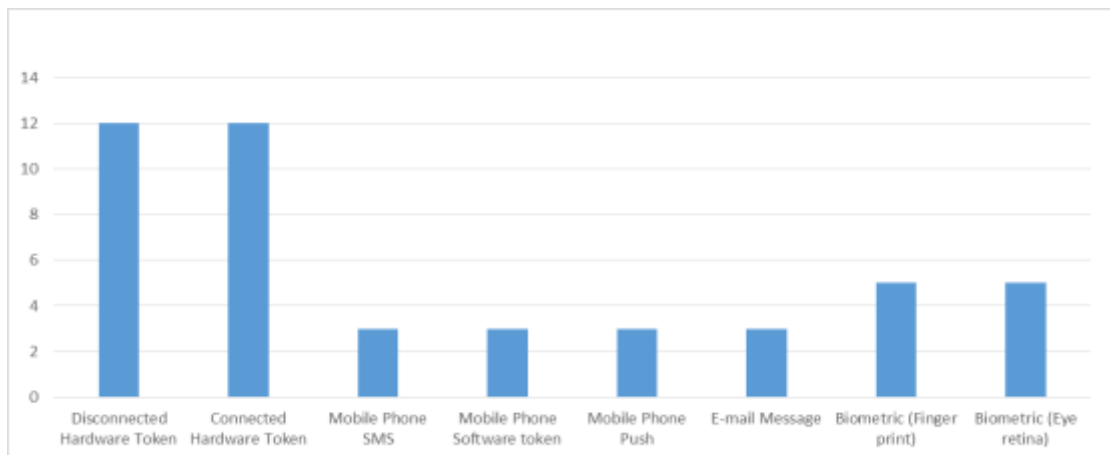


Figure 5: the cost effectiveness for the system owner

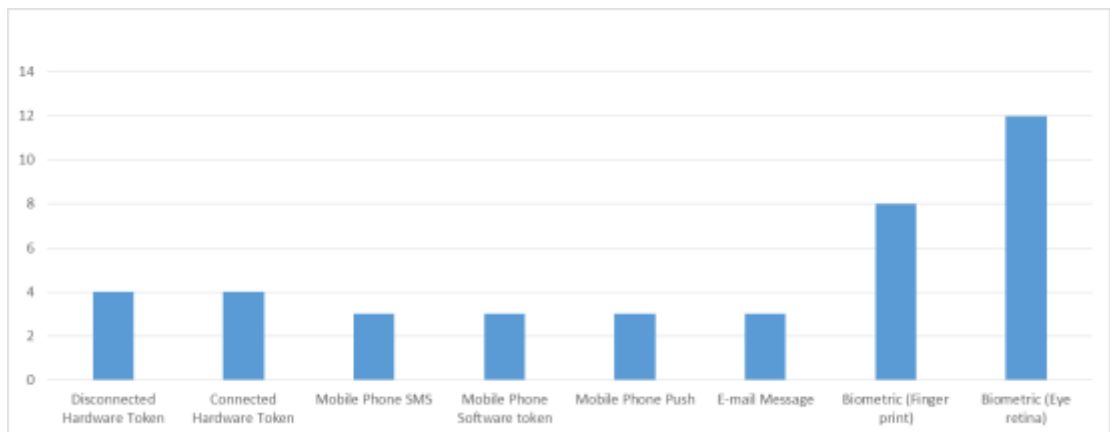


Figure 6: the cost effectiveness for the system user

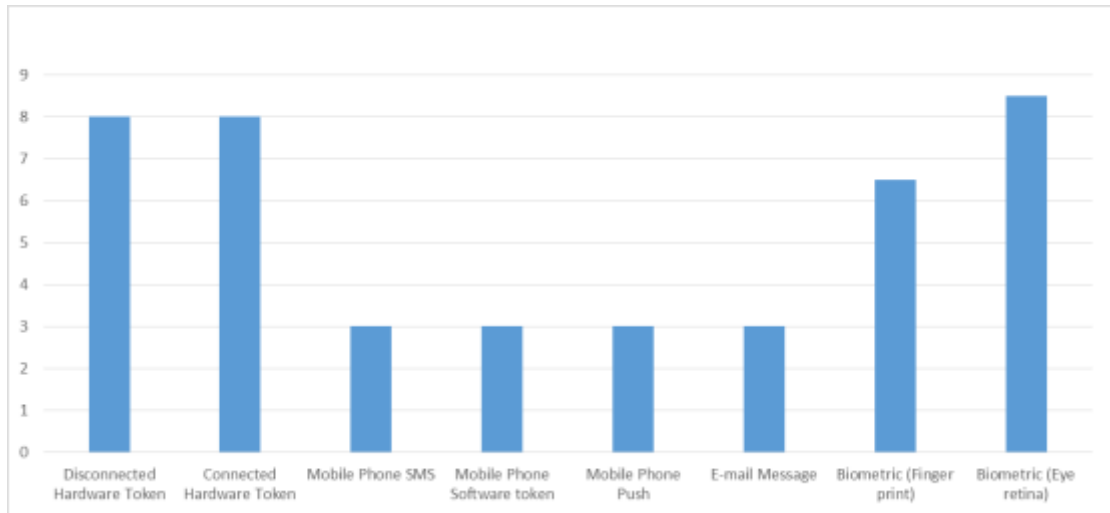


Figure 7: Outcome cost effectiveness for the system owner and system users

5.1.2. Usability

The term “usability” first appeared in the 1960s ^[21] to define the ease with which people, other than software designers, can use a program. It was later introduced in the early 1980s as a replacement for the term ‘user-friendly’ and was defined as “the user’s view of software quality”.

End users of distributed systems perceive security and usability differently depending on context. People tend to perceive usability more than security until they realize the importance of security after falling victim to an online attack that compromises their privacy or assets. Ignoring user perceptions of new technologies might result in dissatisfaction. On average, one dissatisfied user will tell 13 other people about his or her experiences with the system ^[23]. Even worse, for every 30 users having problems with a system, only one user, on average, will call customer support. According to the same source, users usually do not complain to the company about usability issues and do not report them to the service provider. They usually prefer to abandon the service when

they are dissatisfied. Because of this, the e-government web portal must take care when implementing the Two-Factor authentication. These particular technologies can affect users' overall acceptance of the system, especially as it will be a mandatory process to gain access to the portal. That's why it's important to research the end user attitudes as well as the technology's usability.

5.1.2.1. Usability Attributes

Different researchers define usability based upon a list of attributes or dimensions. It is not a single concept, but rather a multi-dimensional property of a user interface that has multiple components. For example, Nielsen identifies the following five usability attributes ^[23]:

- **Learnability:** measured by how easy the system can be learned so the users can start using it at minimum time expected.
- **Efficiency:** another usability attribute that measures the time users need to accomplish tasks after they have learned how to utilize the system.
- **Memorability:** measures how easy to remember the system if the user used it again after he or she has to leave it for a period of time.
- **Errors:** an attribute that measures the rate of errors that the users make during their use of the system. These errors, if exist, have to be minimal and easy to recover from. They must not be of a catastrophic nature.
- **Satisfaction:** measures the users' satisfaction how much they liked using the system.

Whitney Quesenberry ^[24] also defined usability based on five dimensions (called the 5Es):

- **Effective:** how complete and accurate the work is to accomplish.

- **Efficient:** how quickly the work can be completed.
- **Engaging:** how pleasant and satisfying the product interface is to use.
- **Error tolerant:** how good the product is in preventing errors and how it can help the user to recover from mistakes.
- **Easy to learn:** how well the product supports learning throughout its lifetime of use.

A more formal and widely accepted definition of usability is the one by The International Organization for Standardization (ISO). ISO definition reduced the number of the usability dimensions to three: effectiveness, efficiency and satisfaction. The ISO defines usability of a product or service as “the extent to which the product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use ^[25].”

The following points explain the three usability attributes identified by the ISO:

- **Effectiveness:** means that the users can do the tasks without making mistakes. This suggests that the user is not likely to request help.
- **Efficiency:** this attribute suggests that the users can complete the tasks in a reasonable time and effort.
- **Satisfaction:** the most important attribute which reflects the desirability of a product. It determines the extent to which the user finds the product to be effective and efficient.

Table 7 provides an overview of usability definitions by Nielsen, Quesenbery and other usability metrics by Schneiderman and matches their usability dimensions to those of the ISO.

Table 7: Overview of usability dimensions

ISO 9241-11	Schneiderman	Nielsen	Quenesbery
Efficiency	Speed of performance	Efficiency	Efficient
	Time to learn	Learnability	Ease to learn
Effectiveness	Retention over time Rate of errors by users	Memorability Errors/Safety	Effective Error tolerant
Satisfaction	Subjective satisfaction	Satisfaction	Engaging

Table 8 shows a direct usability criterion of the eight suggested Two-factor authentication methods. It represents the requirements of each method from usability point of view. More usable method criterion in this table means a better usability.

Based on industry standards, previous studies and life Two-factor authentication systems analysis. The usability criteria in the table are nine major criteria will directly affect the usability of Two-factor authentication for the user. Points will be calculated for each method based on its usability value. One point for a positive usability criterion of the suggested method, zero point for negative and half point for in between the usability criterion of the method. Highest total points for each suggested method means higher usability value. The usability criteria are:

- a- Requirement of special hardware for the user. That is not including mobile phones. One point if not required
- b- Requirement of special reader for the user. One point if not required
- c- Requirement of special software or driver for the user. One point if not required

- d- Requirement of training or usage instructions for the user. One point if not required
- e- Requirement of TFA configuration per the user account. One point if not required
- f- Ability of the user to edit the TFA configuration of his account. One point if the user able to edit the configuration
- g- Are the user able to access the portal using TFA from a smart phone or tablet PC. One point if the user able to
- h- The mobility and correlation of TFA solution to the user. One point if the suggested method are strongly correlated to the user
- i- The loss probability of the TFA solution token. One point if the suggested method loss probability is low.

As shown in the table 8. The Email message method gains the higher usability value with 6.5 out of 9 usability points. The mobile phone SMS and fingerprint become second with 5.5 out of 9 usability points each. Eye retina method and disconnected hardware token methods gain 5 points each while the Mobile phone push and software token methods gain 4.5 points each. The least usable method according to the table and studied criteria was the connected hardware token which is gained only 2 usability points out of 9.

Table 8: Direct usability criterion of the eight suggested methods

Method Criterion	Disconnected Hardware Token	Connected Hardware Token	Mobile Phone SMS	Mobile Phone Software token	Mobile Phone Push	E-mail Message	Biometric (Finger print)	Biometric (Eye retina)
Special end user Hardware	Required	Required	Not required	Not required	Not required	Not required	Not required	Not required
Special end user Reader	Not required	Required	Not required	Not required	Not required	Not required	Required	Required
Special software/Driver	Not required	Required	Not required	Required	Required	Not required	Required	Required
End user training/Special instructions	Not required	Not required	Required	Required	Required	Required	Not required	Not required
Configuration by end user	Not required	Not required	Required	Required	Required	Required	Not required	Not required
End user can edit configuration	No	No	Yes	Yes	Yes	Yes	No	No
Access the portal without PC (Only with smart phone)	Yes	No	Yes	Yes	Yes	Yes	Only on modern Smart phones	No
Mobility with end user (Correlation)	Low	Low	Moderate	Moderate	Moderate	High	High	High
Loss portability	High	High	High	High	High	Moderate	Low	Low
Total points	5	2	5.5	4.5	4.5	6.5	5.5	5

The figure 8 shows the total usability value of the eight suggested Two-factor authentication methods. It represents the value of each method from usability point of view. The higher usability method criterion in this graph means a better usability value.

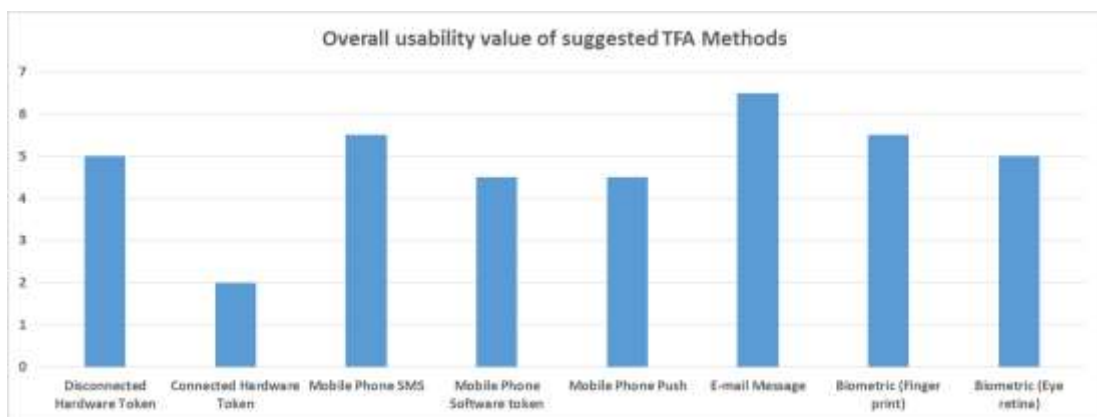


Figure 8: Total usability value of the eight suggested methods

5.1.3. Standardization

ISO identified Multi-factor Authentication as an Authentication with at least two independent authentication factors [ISO/IEC 19790].

5.1.4. One Time Passwords implementation versus other existing methods

The cheapest way would be generating a One-time password and then delivering it on a piece of paper ^[8], which is already known by someone who generates the OTPs on a device. The reason for this is these systems avoids the costs of SMS messaging. Even though delivering the OTPs by this way is cheap, it is not feasible because of the time to deliver the password to the user is too long. OTP technology is a sequential password system and is the only password system proved non-decrypted in theory ^[6].

Compared to hardware tokens, as far as one has a phone or a mobile device, it eliminates the need of carrying an extra item that would be of no use other than generating the one-time passwords ^[7]. In terms of costs, also using a phone as a token provides with the best convenience that it is not necessary to deliver devices to each end-user. For most users, a mobile phone can be trickle-charged to save the charging for at least some time for a day, but most proprietary tokens cannot be trickle-charged. However, most proprietary tokens have tamper-proof features.

Even though OTPs are most secured than the normal static passwords, the users of OTP systems are still vulnerable to MITM attacks. The OTPs should not be shared with the others and the use of an OTP in layered security is safer instead of using the OTP alone, achieving layered

security can be done by using an OTP in combination with a password that is memorable to the user ^[27].

The benefit of using layered security is that a single sign-on in combination with one master password is safer than using only one layer of security during the sign-on. The following table shows how Two-factor authentication performs better than the other existing systems in terms of cost, complexity and protection.

Table 9: how Two-factor authentication with OTP performs better than the other existing systems

Method	Password	Digital Certificates/PKI	OTP + Password
Advantages	Widely used and supported by the largest number of applications	Bi-directional authentication	Two-factor authentication compatible with password based infrastructure: zero client footprint option
	Technology easily understood by users	Can provide two-factor. Non-repudiation	
Disadvantages	Relies on human protection and management of the secret.	Certificate management cost can be prohibitive for large user base.	Requires possession of OTP generation software/hardware or access to a secondary channel for OTP transmission
		Heavy footprint to manage on client.	
		Not compatible with small devices. Requires distribution of certificate/smart card to client.	
Key Vulnerabilities	Brute force	User override of warnings Client insertion (reduced)	Man-in-the-middle/client insertion
	Man-in-the- middle/client insertion		Phishing (reduced to one time action)
	Phishing		
	Over the shoulder Keystroke loggers		
Applicability	Lower risk environments	Highly secure environments	B2C Commerce Enterprise Security
	Legacy environments	Monetary or legal transactions where non- repudiation is a required feature	VPN
	No network usage or protected network usage	Environments where mutual authentication is required.	Environments not suited for PKI (e.g. password based application infrastructure)

5.2. Online survey

An online digital survey created and distributed to the public to gain information from a random sample of people to collect required information that helps in identifying the importance, acceptance and most-liked methods that a normal person may prefer to use as a second authentication method. The online survey created and distributed via service provided by the www.esurveycrator.com website.

There is 187 person participated in the survey. Ninety three percent of them (174 person) has completed the survey successfully and counted in the final survey results.

The survey was designed to be answered by normal, ordinary and even not qualified or technology involved people. It consists of thirteen

question. Three of them are general questions, Email, gender and qualification. Four questions were for the general internet usage by the participants. The last section of the survey contains six questions that focus on the feeling of importance of securing sensitive online data. Acceptance of such technology and most liked method that the end user welcomed to use.

5.2.1. Online survey results

There are 143 Male and 31 Females participates in the survey. Below are the rest of the results of the survey:

Participant ages:

Table 10: Online survey participants age range

Age range	Persons participated
18 – 25 year	39
26 – 33 year	54
34 – 40 year	48
41 – 48 year	21
49 – 56 year	9
57 – 64 year	3
More than 64 years	0
Total	174

Qualification:

Table 11: Online survey participants qualification

Qualification	Persons participated
Below average education	2
average education	7
High school	53
High diploma	44
Bachelor degree	65
Graduate studies	3
Total	174

Internet usage:

Table 12: Online survey participants daily internet usage

Internet usage	Persons participated
Less than 30 minutes	27
30 Minutes – 1 Hour	31
1 Hour - 2 Hours	21
2 Hour - 4 Hour	38
More than 4 hours	57
Total	174

Internet services required confidential data, security and mobile phone usage:

Out of 174 participating persons, 33% (58 person) said that they are using internet services that uses confidential data or runs sensitive transactions like internet banking. While a 60% of them (104 person) said

they are not feeling secure by protect their data by username and password only and 98% of them are using mobile phone services

Additional hardware token:

54% of the participants (94 person) welcomed to carry additional hardware token to protect their access to e government web portal while the rest was not welcomed to carry it or afraid of losing the token

Preferred second factor authentication method:

Regards the suggested Two-factor authentication methods to the users, the user was able to choose more than one method to help determine the most welcomed method for the users. This survey question result is below

Table 13: Online survey preferred second factor authentication

Method	Participate votes
Disconnected Hardware Token	24
Connected Hardware Token	43
Mobile Phone SMS	112
Mobile Phone Software token	105
Mobile Phone Push	67
Email Message	59
Biometric (Finger print)	135
Biometric (Eye retina)	90

As noticed, the biometrics highly voted from the participants, 135 votes for fingerprint and 90 for Eye retina. As the methods using the mobile

phone as Two-factor authentication channel becomes second. The next question is critical to determine which one of them is able to implement for the users.

The question was about willing of users to buy additional hardware required by biometric methods for scan fingerprint or eye retina. It was dramatically reduced the opportunities to use biometrics as only 42% of the participants (73 person) welcomed to buy additional hardware to scan biometrics while 58% (101 person) denied that. That makes biometrics clearly not an option to implement in e-government web portal access, as it is not usable if the user does not have the required hardware.

The last two questions, help determine the acceptance of additional procedures required to use hardware or software token on their personal computers or smart phones and if it is important for the user to access the e-government web portal from a smart phone or tablet PC which is mandatory by nowadays standards.

Only 37% (65 person) welcomed to install additional software or drivers to their personal computers or smart phones to gain access to e-government web portal while the rest denied that. In addition, 99% (172 person) said they need to access e-government web portal from their smart phones or tablet PCs

The survey was a helpful tool to build a view of what the end users think and feel about the secure accessing internet services that uses confidential data and what they prefer and acceptance to use Two-factor authentication to access e-government web portal. That helps a lot to reach the results of this dissertation.

5.3. Two-factor authentication methods test

There is a number of companies that offer Two-factor authentication solutions for integration in websites and Internet portals as a Cloud Two-

factor authentication service that removes the hassle of build a special infrastructure to implement Two-factor authentication solution in the web portal for fixed yearly, monthly or even per user fees. For a security and cost reasons, the cloud Two-factor authentication solution is not recommended because of confidentiality of data and to host all the system resources locally. However, these services used throughout this dissertation to test the process time and delivery assurance of the second factor process, which should be strict as it should not have any delay or loss of information.

To study the process, two cloud Two-factor authentication service providers services in two different geographic locations in Libya (Tripoli city and Benghazi city) tested during this thesis preparation to use the test output and verify the difference between the suggested Two-factor authentication methods and help choose the best one for e-government web portal.

The delivery assurance here indicates if the user successfully enters his username/password and get a response from the second authentication method (SMS, Email, etc...). if the user successfully enters his username/password and didn't get any response from the second authentication process for any reason that means a failure in the login process and he should try again from the beginning or try a backup method if exists.

The processing time means the time required between the successful inputs of username/password and get a response from the second authentication method (SMS, Email, etc...). a shorter time leads to a better experience of Two-factor authentication and smooth login process

The methods tested are:

- a) Mobile Phone SMS
- b) Mobile software token
- c) Mobile push notification
- d) Email Message

The second factor process delivery assurance and time during the process depends upon many factors based on the used method. As an example, in SMS method, the network traffic and mobile coverage may delay the SMS or cause a failed transmission. However, this method still better than the Email message as it comes with immediate notification directly to the mobile phone once received rather than check the incoming mails via web browser or Email client and keep checking until it arrives.

5.3.1. Test results

Each tested methods went through 50 sample login in each geographical location while monitoring and record the delivery assurance and processing time each time. That means 100 login using each method and 400 sample login in total. Below are the test results for delivery assurance and delivery time for each tested method.

a- Software token:

Delivery assurance and processing time:

The software token is a previously installed and configured software on a smart phone and it has a high delivery assurance and zero processing time as it is working in the background on the smart phone and generates a new OTP every 60 seconds that can be used any time just after opened the software token application. When the user successfully enters his valid username/password to login to the system, he just needs to open the software token application and enters the appeared OTP in the token to the e-government web portal login page to complete the login process.

The drawback of this method comes from the need of smart phone to work. If the user has a normal old-fashioned mobile phone, he simply could not use the software token, as mentioned before, it is originally a mobile application that has to be installed and configured previously on a smart phone

b- Mobile phone SMS:

Delivery assurance

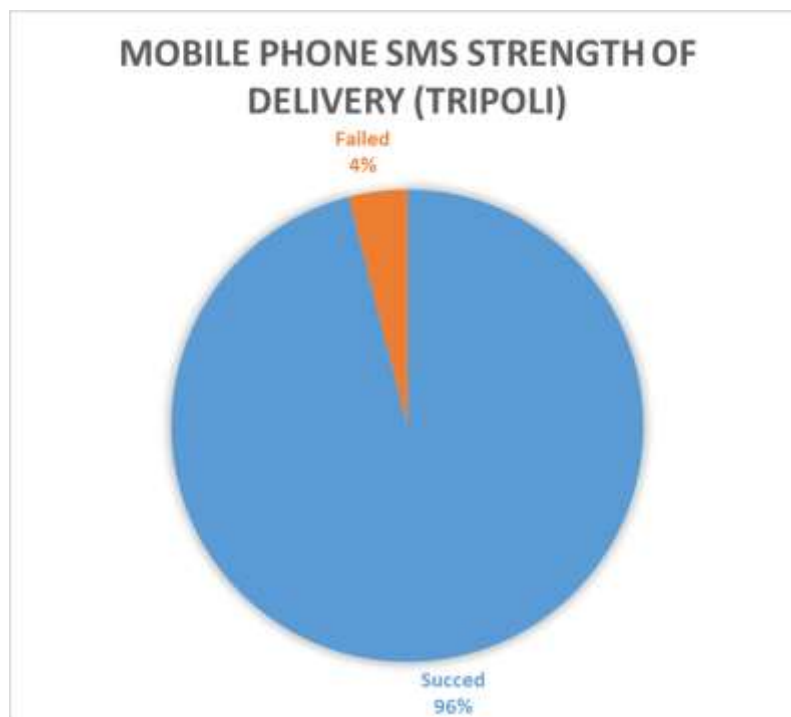


Figure 9: Online survey SMS delivery assurance (Tripoli)

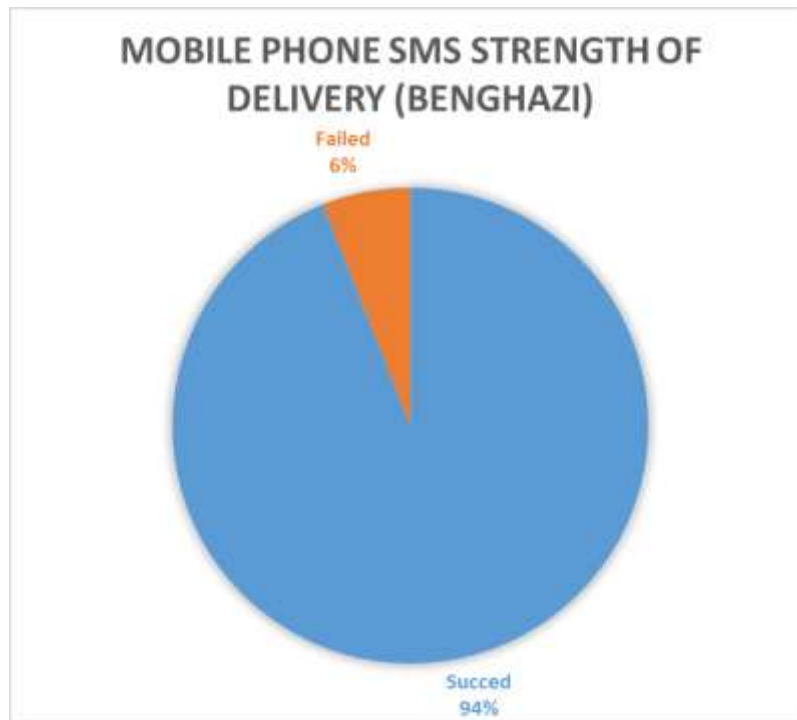


Figure 10: Online survey SMS delivery assurance (Benghazi)

Mobile phone SMS Processing time:

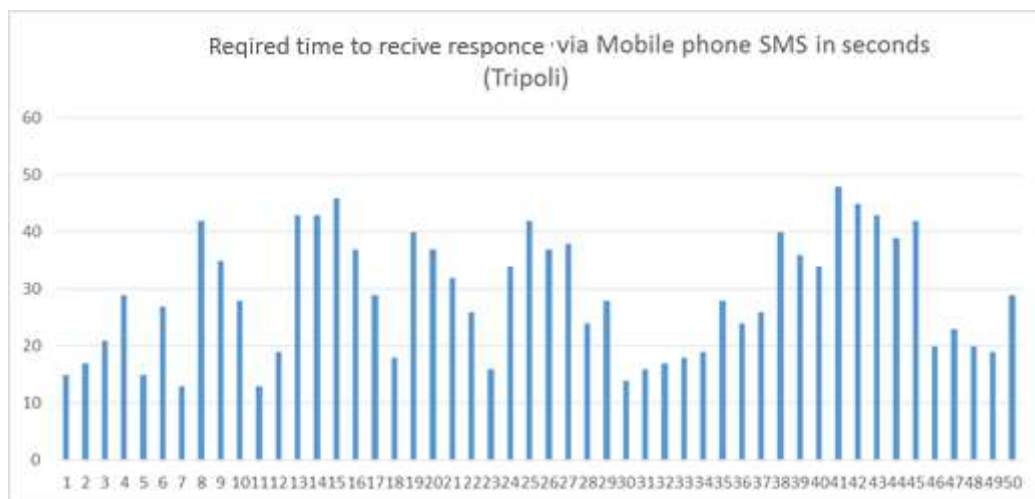


Figure 11: Online survey SMS processing time (Tripoli)

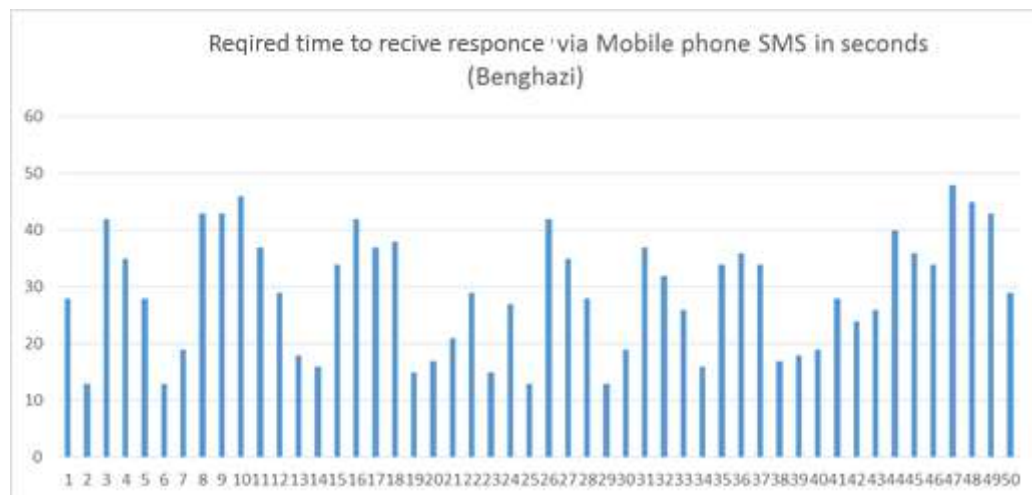


Figure 12: Online survey SMS processing time (Benghazi)

The excellence of the mobile phone SMS method comes from the fact that almost everyone is using the mobile phone services and this method can work on any mobile network and any mobile phone device from second generation to the fourth generation without any need of internet connection, special software or even a smart phone. Even if it has a little drawback in delivery assurance and takes maximum 50 seconds to receive the message. In final compromise that is not a big issue unless there is no mobile phone service in the area the user trying to login to the system from it.

c- Mobile push:

Delivery assurance

While the mobile push has optimum delivery assurance without any loss in the process. We should know that there is a big drawback in mobile push method. That drawback is that the mobile push method does not work if the user does not have a wireless internet connection or mobile broadband for any reason. This drawback would limit the access to the portal and should be taken in consideration when choosing the best TFA method to implement for e-government web portal access. Also, as the software token, it is originally a mobile

application that has to be installed and configured previously on the smart phone

Mobile push Processing time

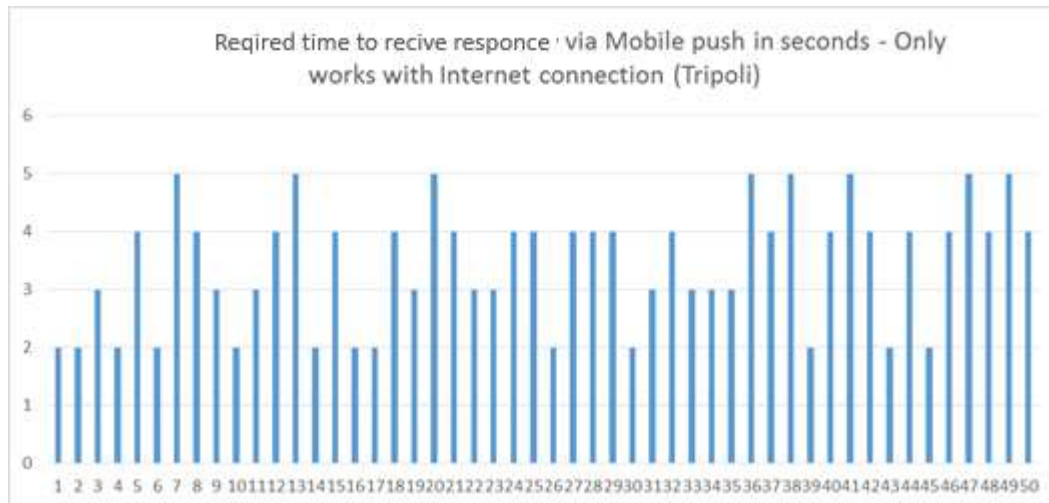


Figure 13: Online survey Mobile push processing time (Tripoli)

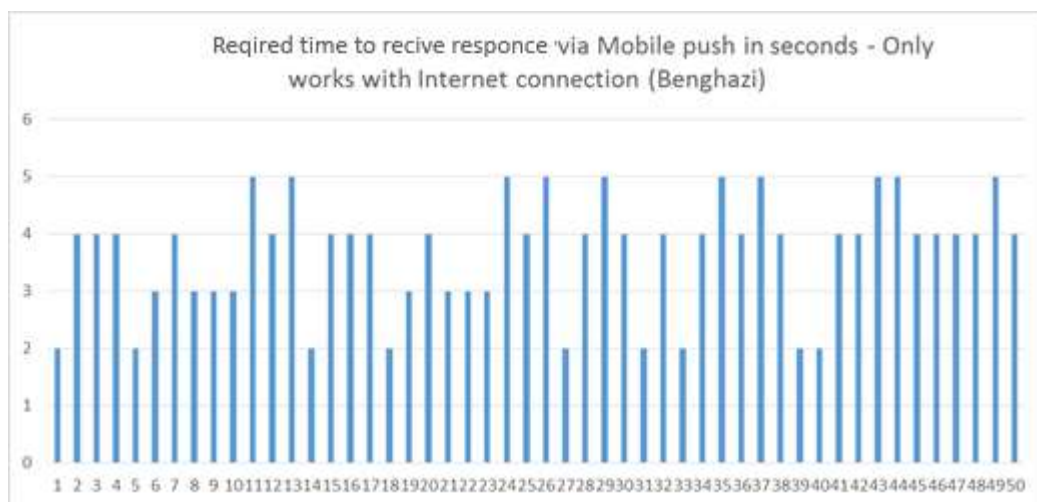


Figure 14: Online survey Mobile push processing time (Benghazi)

d- Email message

Delivery assurance of Email system is very high unless the received Email considered spam by the Email system the user is

using it. In this case the user should manually configure the Email system to don't filter the Emails received from the e-government web portal system and move it to spam or junk folders rather than the inbox. Otherwise, the Email message method has an optimum delivery assurance.

Email message Processing time

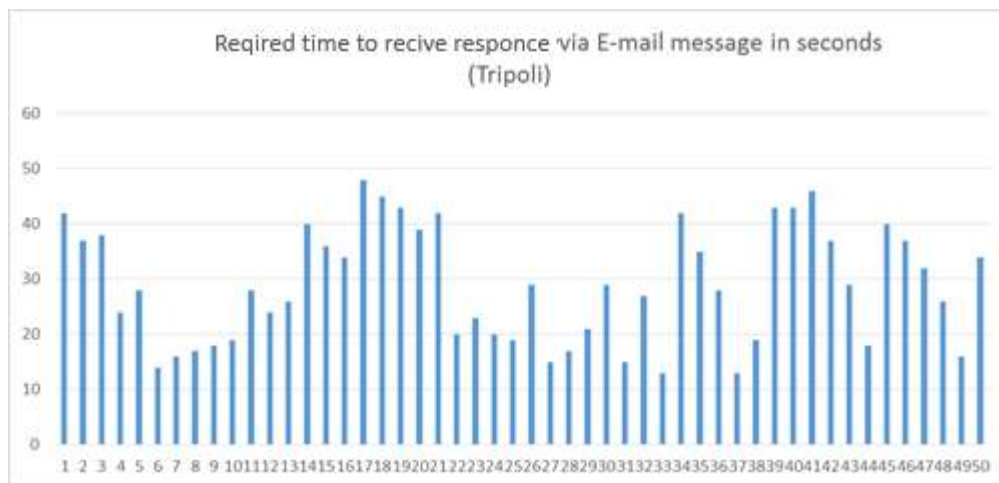


Figure 15: Online survey Email message processing time (Tripoli)

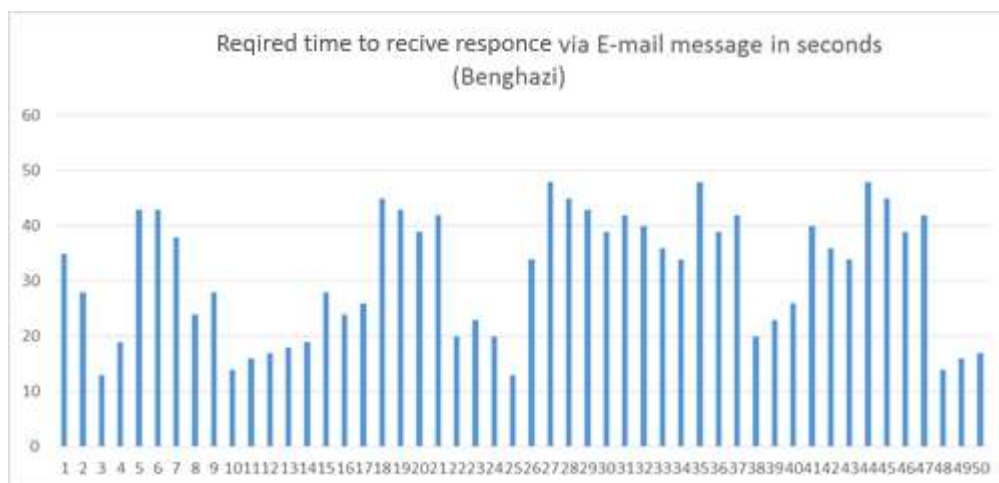


Figure 16: Online survey Email message processing time (Benghazi)

Biometrics and hardware tokens have a very good delivery assurance and low process time, but it has other drawbacks in usability, cost and other discussed requirements of Two-factor authentication.

The two cloud Two-factor authentication service companies used throughout this dissertation to test and study the second factor process is:

- Duo Security - <https://www.duosecurity.com/>
- Secure Envoy - <https://www.securenvoy.com/>

6. Proposed authentication system and implementation

This chapter proposes a Two-factor authentication system for e-government web portal that is able to withstand the most popular, previously identified online authentication attacks in previous chapters while maintaining acceptable levels of usability and acceptability. It also proposed a backup method of Two-factor to use it in case of unavailability of the primary method and implementation of the proposed solution.

Based on chapter 5, a clear identification of each Two-factor authentication pros and cons can help in decide the main and backup Two-factor authentication methods that can satisfy the e-government web portal needs.

Figure 17 shows a chart of the overall value of Two-factor authentication methods from e-government web portal point of view based on previous work on chapter 5.

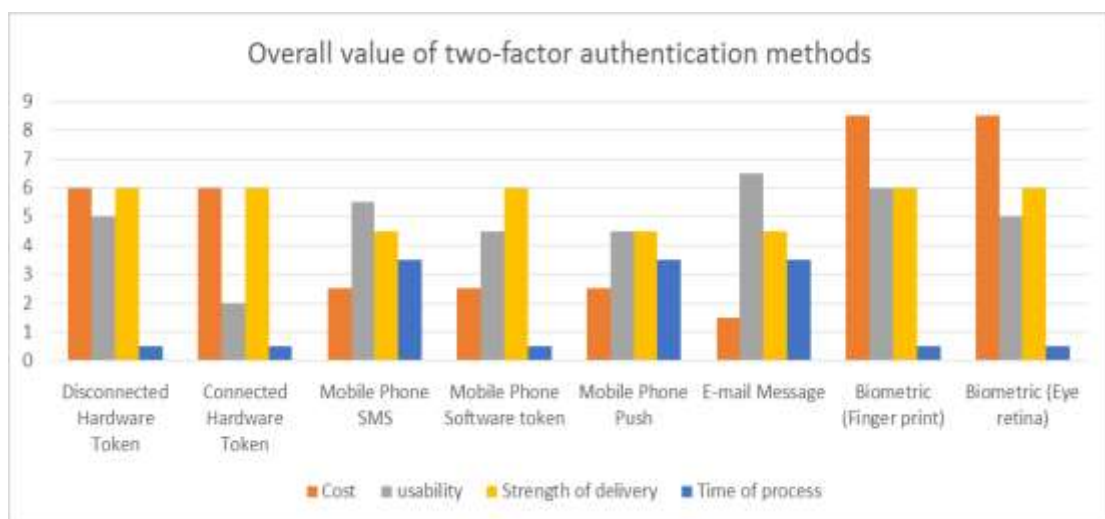


Figure 17: a chart of the overall value of Two-factor authentication methods

Hardware tokens: The downside of the Two-factor authentication security process is that new hardware tokens need to be ordered, then

issued and this can cause slowdowns and problems for the e-government portal operators and end users, who is waiting to gain access to their own private data via this authentication procedure. The tokens are also usually small and easily lost so causing more problems for everyone when end users requesting new ones.

Biometrics: On the other hand. While the biometrics have many advantages like ease of use and nothing to forget or lose. The implementation of biometrics in Two-factor authentication in wide enterprise e-government portal facing a lot of problems for the system operators such as when they create a new account and scan the required biometric data from the account user and assign it to it. Furthermore, end user may resist or do not accept to read his biometric data from the system operators and make it accessible in such a system.

6.1. Proposed main authentication method

This dissertation looks forward to resolving discussed e-government web portal authentication problems in the previous chapters and propose a high security authentication system.

By utilizing mobile phone SMS technology. With over 8 million mobile phones in use in Libya, according to local mobile operators (Libyana and Almadar), turning a phone into an authentication device quickly solves the need and additional cost and delays of sending out hardware tokens.

The mobile phone SMS (Short Messages System) is used to send randomly generated time based One-Time-Password as a second authentication factor that the user should enter it after he successfully enters his correct national ID and passport. A one-time password (OTP) is a password that is valid for only one login session or transaction. OTP

avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid.

SMS is a ubiquitous communication channel, being directly available in nearly all mobile handsets, SMS has a great potential to reach all consumers with a lower total cost to implement. However, the cost of text messaging for each OTP may not be acceptable to some users, but for a governmental portal, it has a very good value as it serves a large number of users.

SMS information set: Beside the one-time password, the system sends the following information set in the SMS. The SMS information set contains:

- Session ID (each login attempt has its own session ID that has assigned OTP)
- Login request time
- Login request location (the system determines it by IP address)
- Browser type
- Operating system platform

The system sends the information set with the OTP in the text of SMS to make sure that the user is aware of the login he or she is verifying. This is vital to avoid any possibility of man-in-the-middle or man-in-the-browser and real-time phishing/pharming attacks

Libyan government national ID is a unique number for each citizen that never changes during his life, and it already exists and the Libyan government relies on it in citizen's governmental transactions like electronic passports. The suggested solution use that Libyan government national ID as a username, and an account password to initiate the login process.

To protect the users from key-logging and similar attacks. The password are only writable by the portal's built-in on-screen keyboard. The system also allow only three wrong password login attempts before locks the account for five minutes to prevent password discovery attacks and non-repudiation protection.

In the final step in the system's authentication process. The system uses an image-based authentication technology and displays 12 pictures from 12 different categories (National, ancients, desert, animals, flowers, cars, electronics, furniture, buildings, tools, people and food). To finish the authentication process, the user should select a photo that belongs to the category that assigned to his account during the account creation. This step adds an additional layer of protection to the authentication process that helps reduce attacks may happen after the theft of the device and compromise the password by the attacker.

After the user successfully enters the correct information in each step, the e-government web portal system determines if the information submitted is valid or not. If all and only all information in each step were valid, it gives the authorized access to the e-government web portal resources, thereby allowing the user to have access to his account, preview information and perform any necessary queries and transactions. Otherwise, it blocks the access attempt.

Every successful and failed login attempt information set sent to account owner default mobile phone via SMS and default Email address beside the status of login (successful or failed).

This confirmatory feedback feature is helping in detect tampering and illegal login attempts. This will allow the account owner to take required action or actions and report such an incident quickly to the e-government authority.

6.2. Proposed alternative authentication method to be used as a backup

Any good system should have a high level of usability, minimum effort of administration and of course with a good plan for emergencies. In e-government web portal authentication process, assuring a hassle-free access to the system for the end user and system administrators in case of emergency is mandatory.

First. The emergency in any Two-factor authentication process is always happening when the user lost one of his authentication factors. Until now, this dissertation reached a point that the best Two-factor authentication method for e-government web portal is to use National ID as a user ID with password to initiate the authentication process and generate a one-time password sent via mobile SMS valid only for the associated process for a short period (Time based OTP). Login attempt detail sent alongside the OTP and final image based authentication step. To achieve a successful authentication process, the user should have his valid National ID and account password with his mobile phone and know the image based authentication category has been associated with his account previously. While he has these requirements, he can successfully authenticate easily with his account in the e-government web portal.

Password recovery: In case the user lost the account password. A procedure contains a few steps should be implemented to recover the lost password without any interaction of the system administrators. These procedural steps are to ensure that the real account associated user only can recover his password. These procedure steps are the following.

- The system allows only three wrong password attempt before it deactivates the account for five minutes to prevent password discovery attacks and non-repudiation protection.
- The user will ask to renew his password by clicking a link on the page. He will be redirected to be asked a three questions like a birth date or mother's name. These questions will be displayed a one question per page and will not redirect to the next question until a correct answer submitted.
- After answering the three questions correctly, the system will generate a new random password and asks the user about the user's Email address that has configured previously in the system to send the new password.
- The user will use the new randomly generated password to access the portal for one time only because he will be forced to change it during the login process.
- If the user fails to successfully implement this password recovery procedure. He should directly contact the e-government web portal support authority to recover his account.

That scenario and steps are implemented in case the user lost or cannot access his e-government web portal account by the password he knows.

Backup second authentication channel: In case the user lost his mobile phone by stealing, damage, or just he cannot reach his mobile phone. User should follow another procedure per the following steps:

- Once the user successfully submits the correct user ID/password, and the system accepted it. Another page which requesting to enter the OTP that the system should send it via mobile SMS to the user. Login via another method link on that page always appears to the user to help in case he cannot receive the OTP via his registered SMS mobile phone.
- By clicking log in via another method link. The user will be directed to another page asked about how to receive the OTP. He can choose a registered Email address to send an Email message contains the OTP, or an alternative mobile phone number to send an SMS containing the OTP.
- If the user fails to successfully implement this alternative login procedure. He should directly contact the e-government web portal support authority to gain access to his account.

The reason of using Email message as a backup second authentication channel to deliver the OTP is because the same results we reach it in choosing the best TFA method previously. Figure 18 shows a brief conclusion from the results of chapter five.

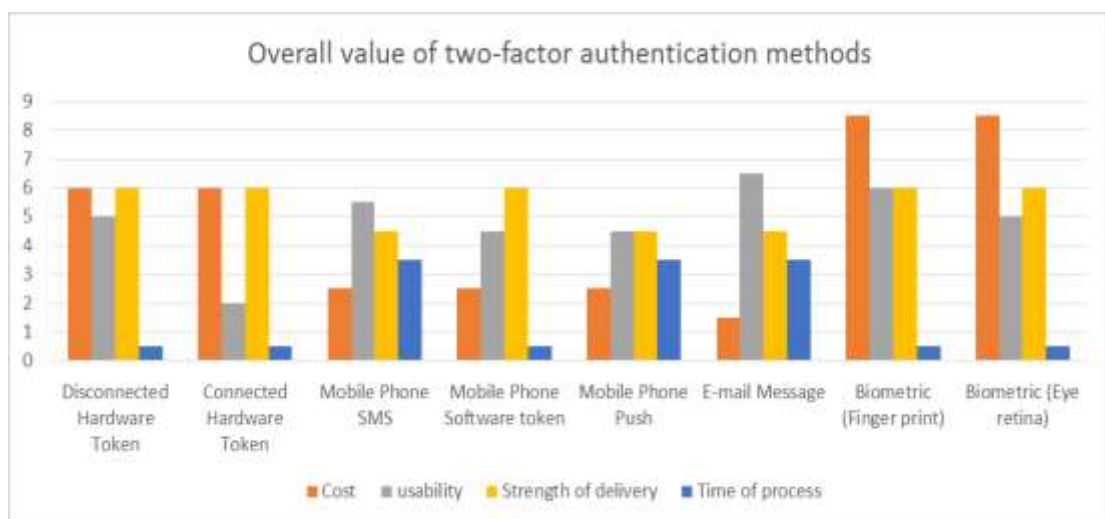


Figure 18: a chart of the overall value of Two-factor authentication methods

The suggested solution has the following benefits:

- High security multi-step Two-factor authentication system uses National ID and password that only writable by built-in on-screen keyboard, one-time password that the system generates it and send it with a custom information set (session ID, login request time, login request location, used browser and OS details) via a user's desired channel (SMS or Email) and finally an image category recognition step.
- Overcomes the drawbacks of traditional Two-factor authentication systems.
- Provides a cost-effective, user-friendly and high security authentication.
- Uses the mobile phone SMS as the user's second authentication channel.
- Uses the Email system as a backup second authentication channel.
- Uses an image based authentication in the last step.
- Easy to use for any regular user with no additional use of hardware or special training.
- Easy to deploy solution for large enterprise.
- Mutually-authenticated and speaks over SHA-2 256bit Transport Layer Protocol (TLS) encrypted channels between client and server.
- Does not rely on username/password authentication that is not secure anymore.

The suggested multi-step Two-factor authentication solution provided to check the identity of the e-government web portal user. It provides a cost-effective solution to provide the e-government web portal resources with a top secure authentication system.

Through the internet browser, a user request permission to access the e-government web portal resources, the user should have an account with an assigned mobile phone number and Email address.

The suggested solution does not rely on traditional User ID and password. It uses Libyan government national ID that belongs to the national government database and contain all personal info of the citizens. Libyan government national ID is a unique number for each citizen that never changes during his life that is already existing and the Libyan government rely on it in citizen's governmental transactions like electronic passports. A password is also required to initiate the login process. The rest of the steps is to prove user identity and serves as added layers of security that protects and enriches the e-government authentication process.

The suggested solution in this dissertation overcomes the security limitations of traditional Two-factor authentication systems and vulnerabilities of mobile device.

6.3. Proposed solution implementation

In order to verify and prove the capabilities of the proposed solution login process. The proposed solution login process implemented and hosted online to give access to the supervisor and examiners to verify it. The proposed solution implementation link is: <http://hajmsc.demo.ly/>.

Technologies used in solution implementation:

- Programming Language: PHP
- Database: MySQL
- Template: Bootstrap
- SMS gateway integrated through API.

Source code and additional information included in appendix D

Implementation screenshots: The following figures shows the implemented login process steps of the suggested solution.

In the first step show in figure 19. The user should enter the login details (National ID and account password) to start the login process. The following steps are to prove the ownership of the entered National ID

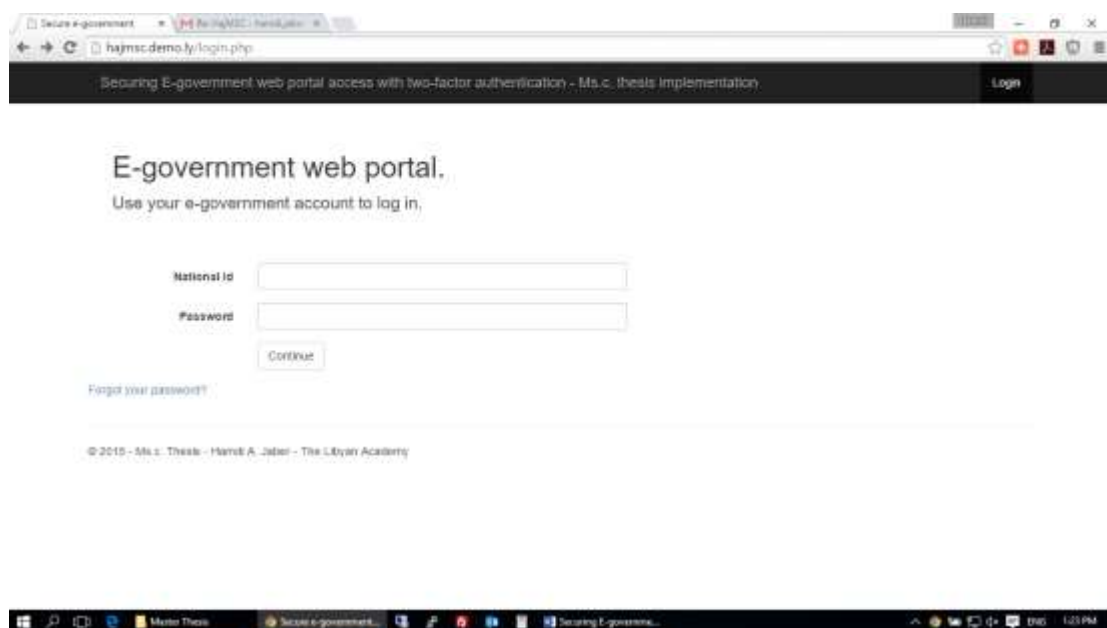


Figure 19: initial login step

In the second step shown in figure 20. The user should choose the desired mobile phone number to receive the one-time password. The mobile numbers should be registered in the system previously during account creation and before activating the account. In addition, the user can modify it any time after a successful login. The system in that step has already generated a session ID and displayed it to the user to help verify the current login process.

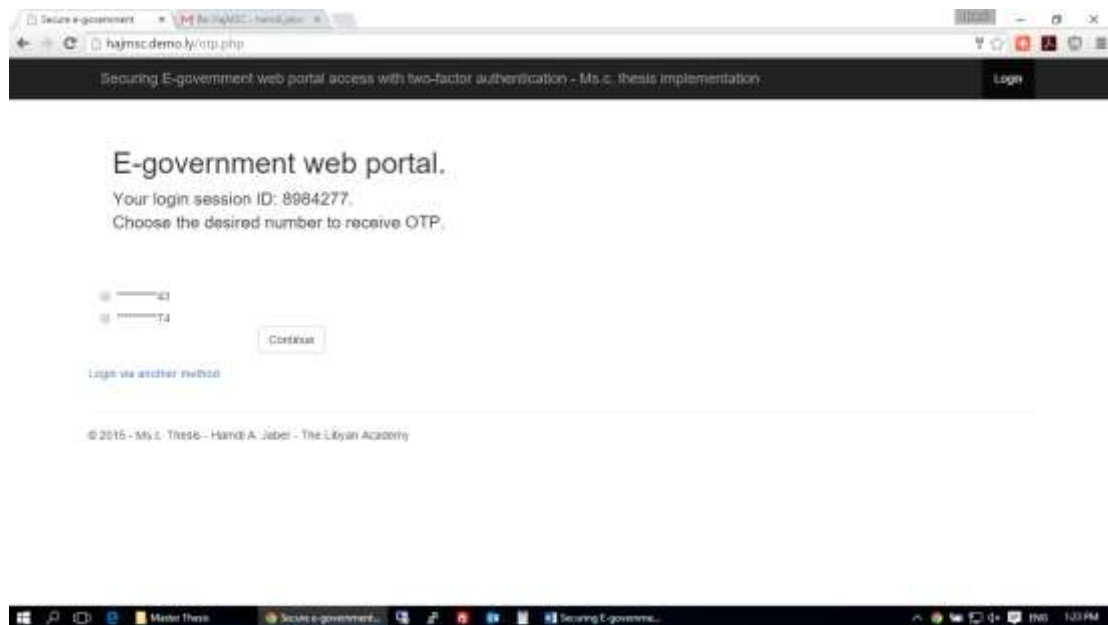


Figure 20: choosing mobile number to receive OTP

In the third step shown in figure 21. The system has generated and sent the one-time password and the login session information set to the user mobile via SMS service.

The login session information set is helping the user to verify the login session he is approving it and help detect tampering and illegal login attempts.

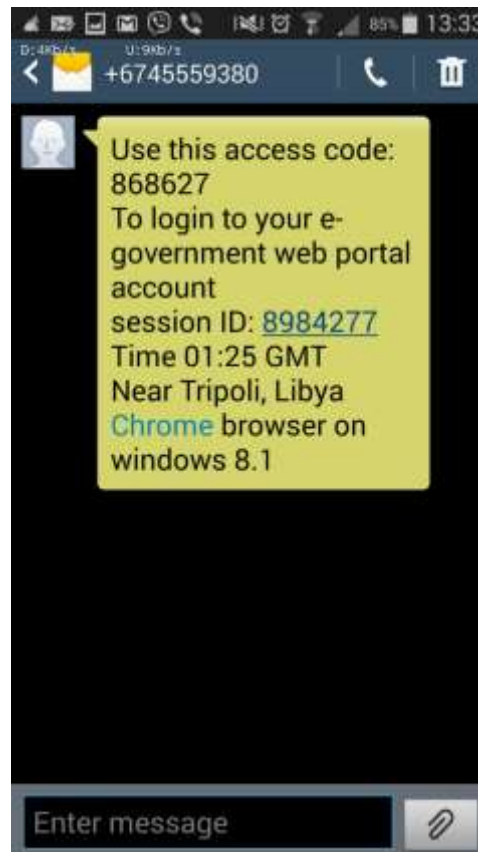


Figure 21: received SMS message contains OTP and login details

In the fourth step shown in figure 22. The user has to enter the received OTP into the system to continue login process.

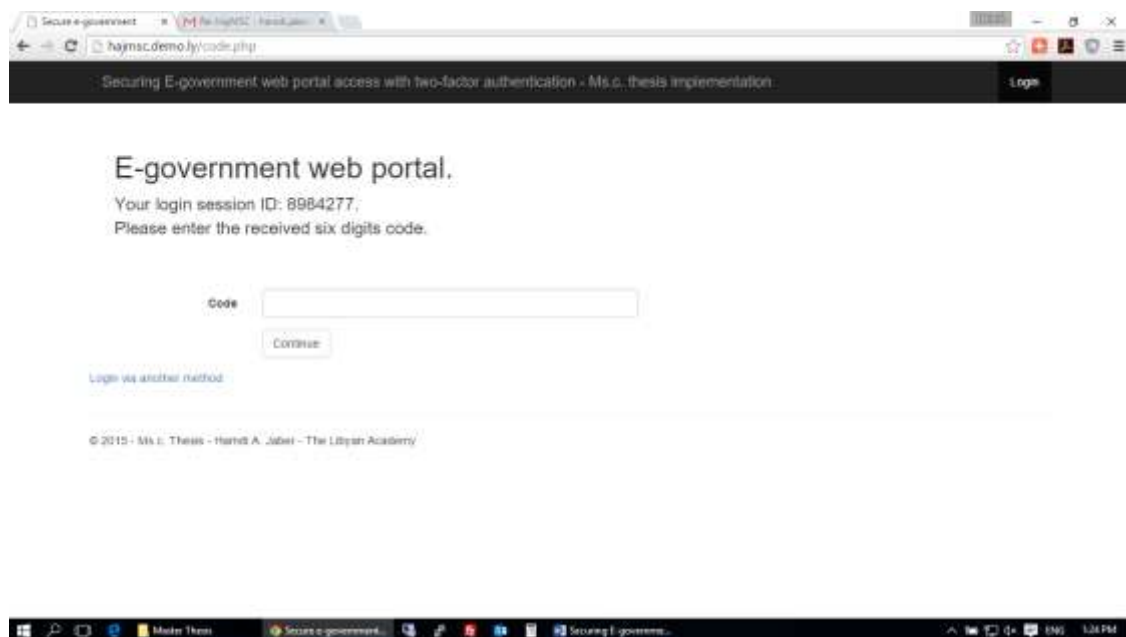


Figure 22: entering the received one-time password

In the fifth step shown in figure 23. The system displays 12 pictures from 12 different categories (National, ancients, desert, animals, flowers, cars, electronics, furniture, buildings, tools, people and food). To finish the authentication process, the user should select a photo that belongs to the category that assigned to his account during the account activation. Just a click on the desired photo will proceed to the next step.

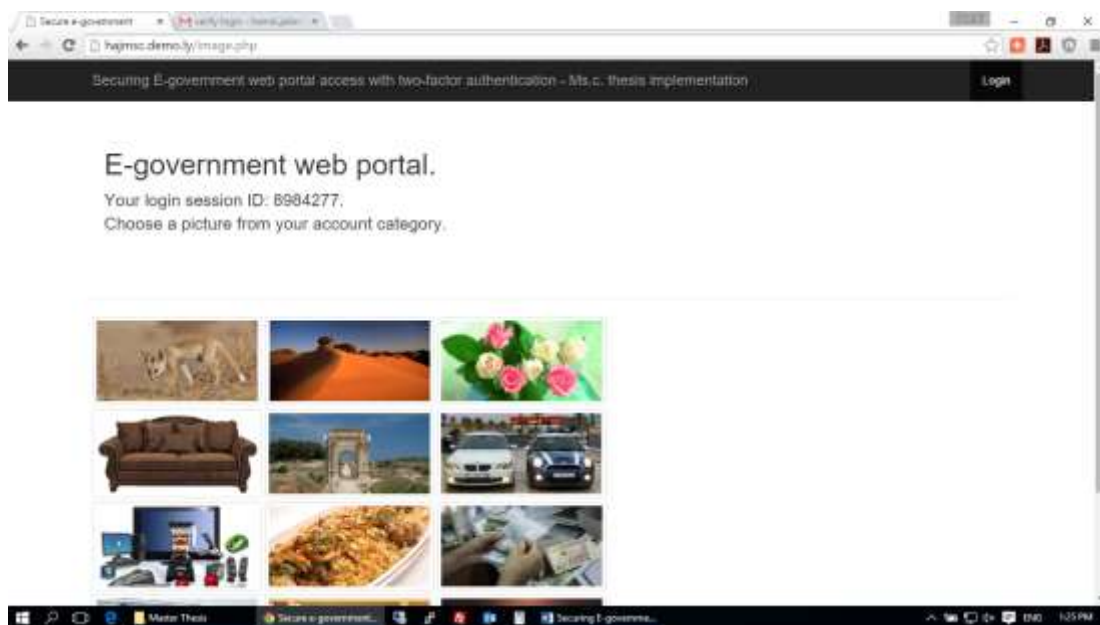


Figure 23: image based authentication step

If every previous step done correctly, the user will login securely to the e-government web portal as shown in figure 24. The user now can access the e-government web portal information and databases. Perform his governmental transactions, queries, and benefit of other services that the e-government web portal provides.

In the suggested system. During a successful login, and through the account options page. The user can change the account password, change or add up to three mobile numbers. Change or add up to three Email addresses. Change the photo category of image based authentication step.

These options can be changed and modified any time after a successful login to the system.

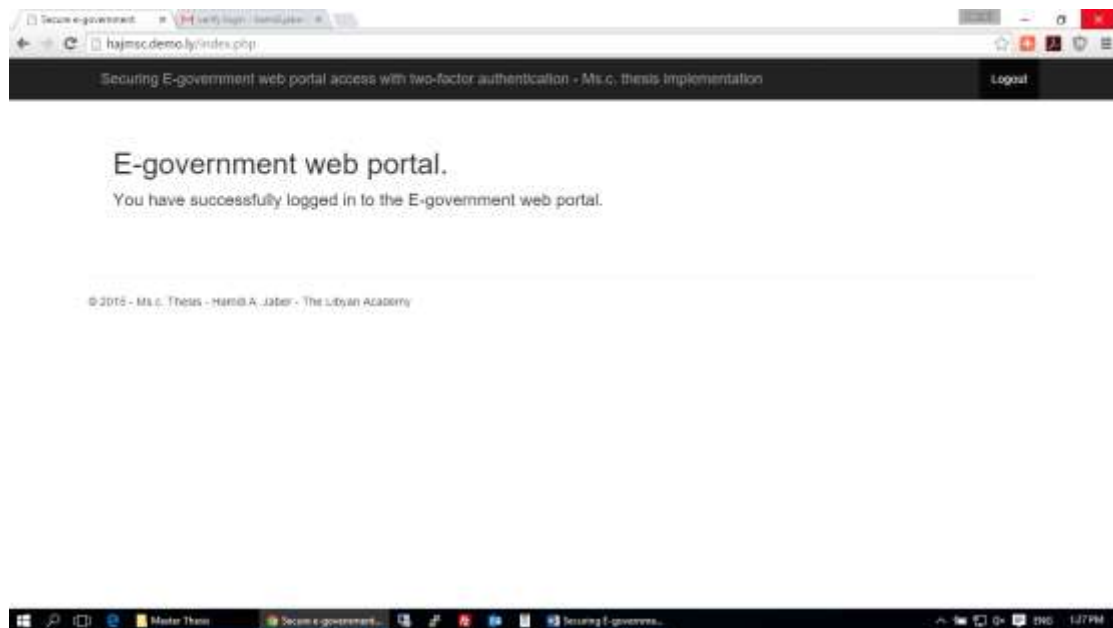


Figure 24: successful login to the system

Every successful and failed login attempt information set sent to account owner default mobile phone via SMS and default Email address beside the status of login (successful or failed).

This confirmatory feedback feature is helping in detect tampering and illegal login attempts. This will allow the account owner to take required action or actions and report such an incident quickly to the e-government authority helpdesk.



Figure 25: confirmatory feedback SMS message

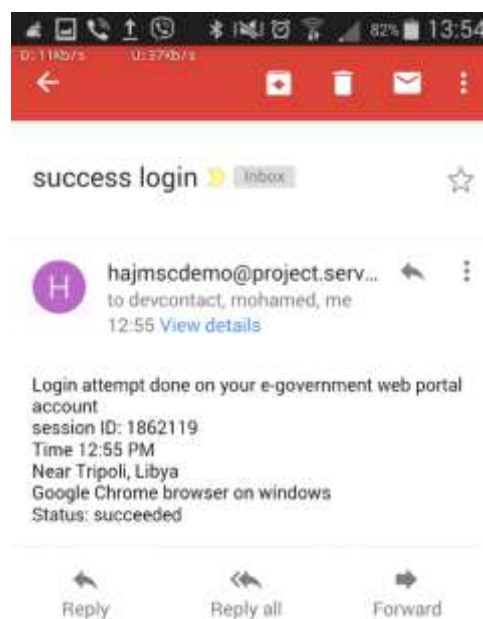


Figure 26: Successful login confirmatory Email

In addition, it is recommended in this dissertation designed system to configure the system to accept two mobile phones and two Email addresses for each account to increase usability by giving the user the chance to choose the desired channel to deliver the OTP (SMS or Email) and to which configured mobile number or Email address through the login process. As a result, the user will be free to access his account in case of problems with the operators of his mobile phone line (e.g. an unpaid bill) or limited access to Email service.

Additional implementation figures:

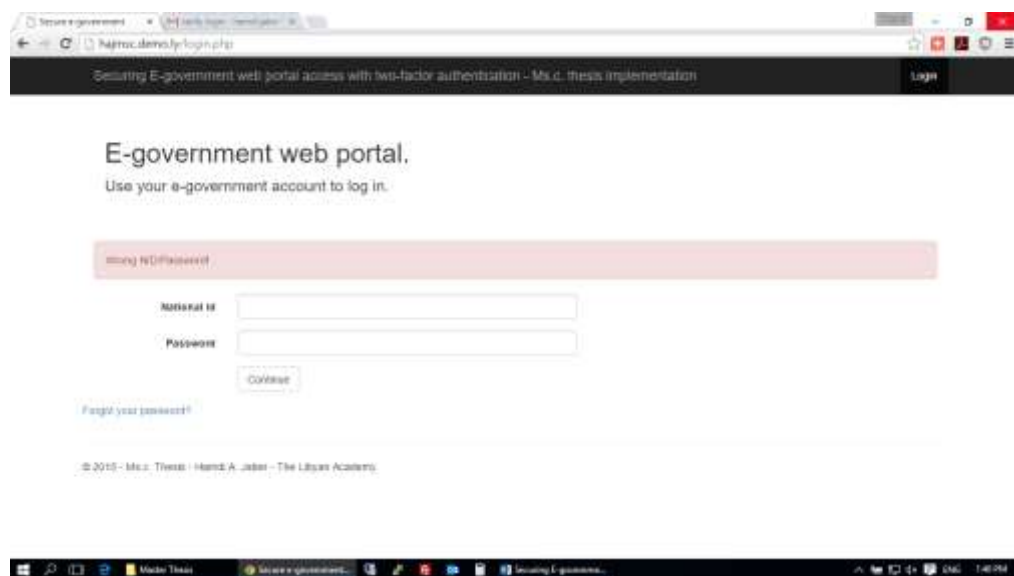


Figure 27: Wrong NID/Password entered

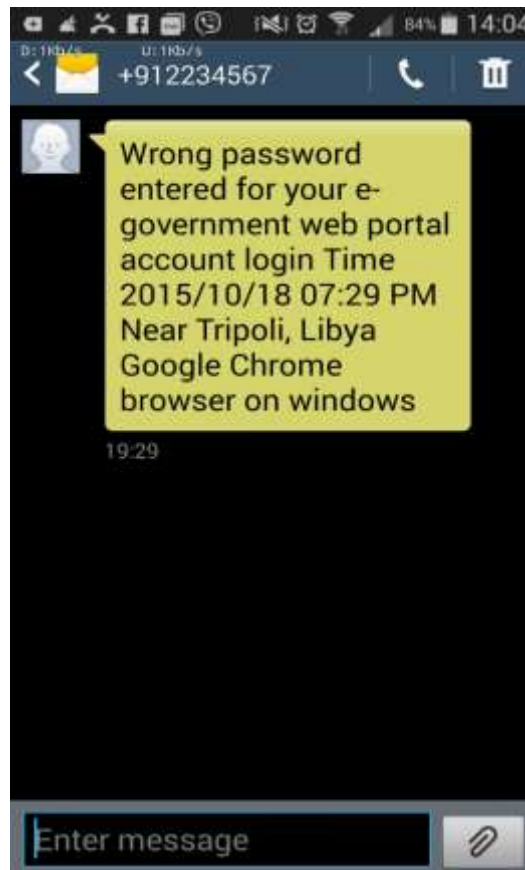


Figure 28: Wrong password alert SMS

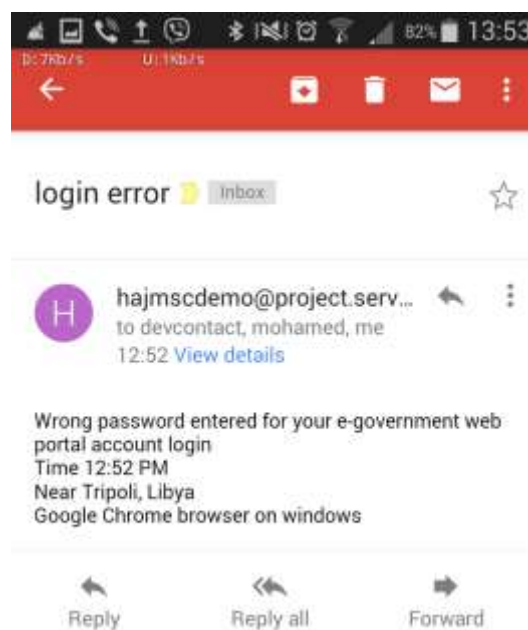


Figure 29: Wrong password alert Email

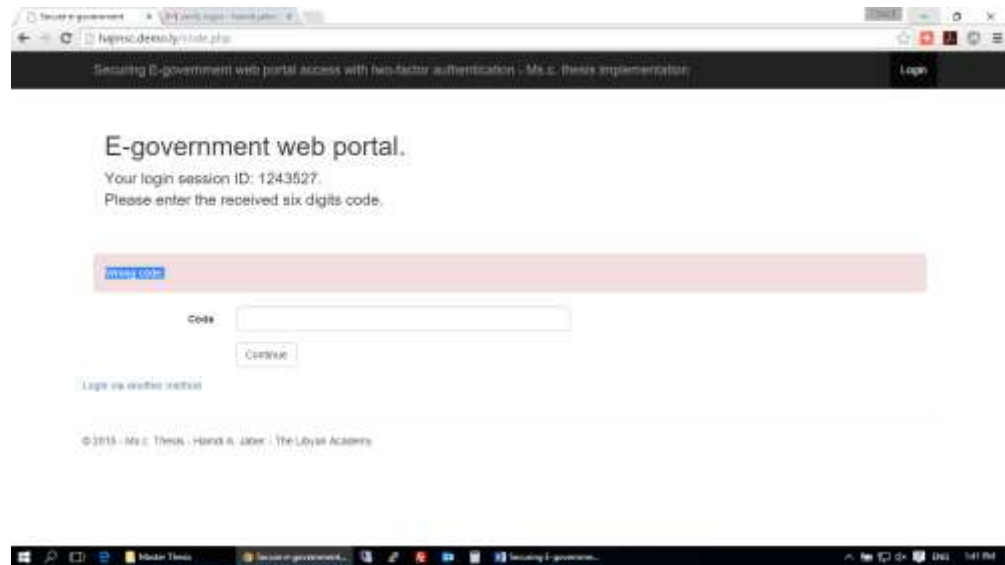


Figure 30: Wrong access code entered

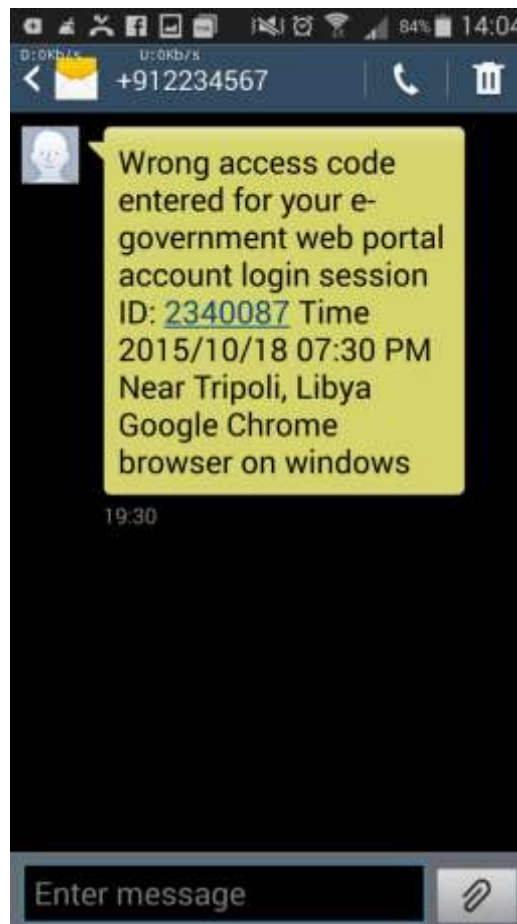


Figure 31: Wrong access code alert SMS

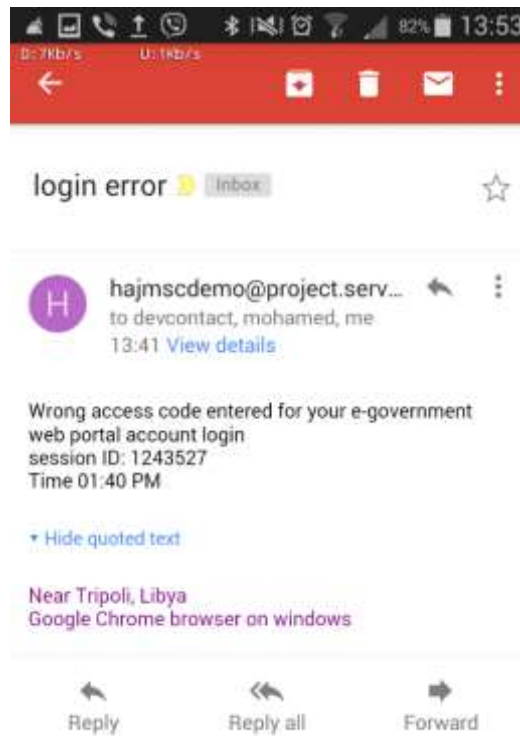


Figure 32: Wrong access code alert Email

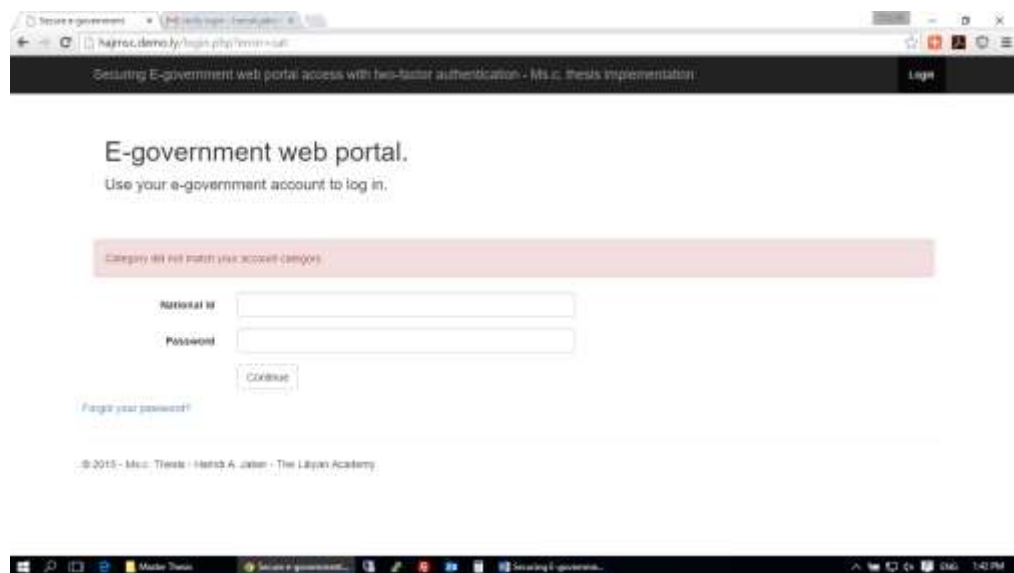


Figure 33: Image category mismatch

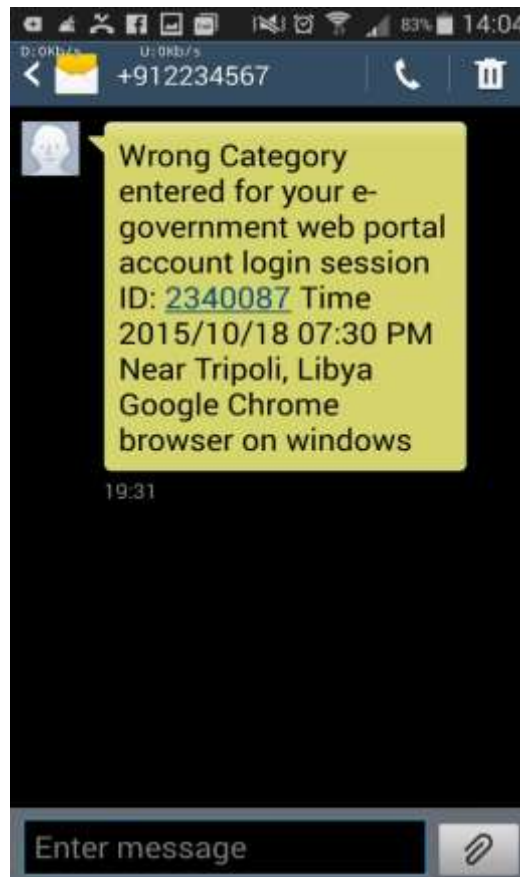


Figure 34: Image category mismatch alert SMS

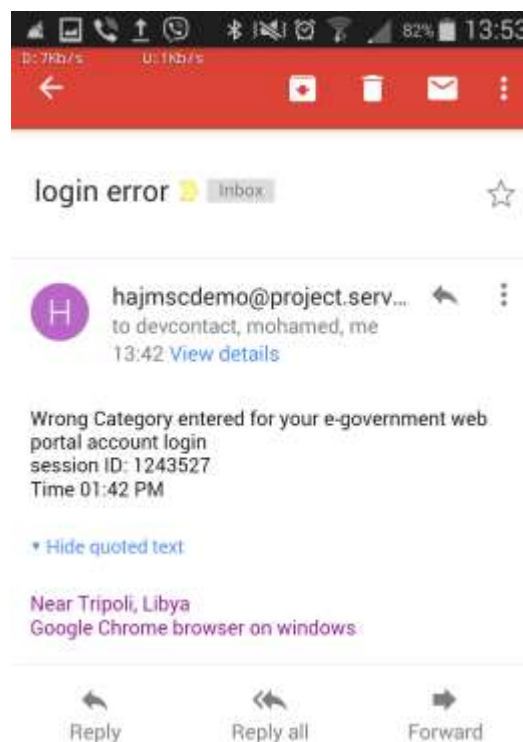


Figure 35: Image category mismatch alert Email

7. Dissertation Results

This chapter presents the results of the dissertation that came with a solution that protects the access to e-government web portal with advanced Two-factor authentication that is able to protect the system from the most popular, previously identified online attacks. The suggested solution designed based on the evaluation of the data gathered through the previous chapters of this thesis.

7.1. Introduction

While the security and usability working against each other in IT world, and the value of data in the e-government web portal require a high level of security, which make the traditional Two-factor authentication not secure enough, and the large number of e-government web portal users from different educational background makes the need of usability is high. This dissertation worked on that fact and produced a high security authentication system strongly resist all known authentication threats while maintaining high usability, allows ease of use to the system users.

7.2. Results summary

This dissertation gives a solution that protects the e-government web portal authentication from security threats using strong multi-step Two-factor authentication. The suggested solution is:

- High security multi-step Two-factor authentication system uses National ID and password that only writable by built-in on-screen keyboard, one-time password that the system generates it and send it with a custom information set (session ID, login request time, login request location, used browser and OS details) via a user's desired channel (SMS or Email) and finally an image category recognition step.

- Overcomes the drawbacks of traditional Two-factor authentication systems.
- Provides a cost-effective, user-friendly and high security authentication.
- Uses the mobile phone SMS as the user's second authentication channel.
- Uses the Email system as a backup second authentication channel
- Uses an image based authentication in the last step.
- Easy to use for any regular user with no additional use of hardware or special training.
- Easy to deploy solution for large enterprise
- Mutually-authenticated and speaks over SHA-2 256bit Transport Layer Protocol (TLS) encrypted channels between client and server
- Does not rely on username/password authentication that is not secure anymore.

The suggested multi-step Two-factor authentication solution provided to check the identity of the e-government web portal user. It provides a cost-effective high security authentication solution to access the e-government web portal resources. Through the internet browser, a user request permission to access the e-government web portal resources, the user should have an account with an assigned mobile phone number and Email address. When a login attempt occur, the system generates one-time password valid for a short period of time (Time based OTP) assigned to that specific login process by session ID, and send it to the user by either SMS text message or Email based on what the user choose during the login request. Beside the one-time password, the system sends a custom information set in the SMS. The information set contains: the login session ID, login request time, login request location, used browser and

OS details. The user has to enter the received one-time password into the web-browser to move to the final image based authentication step, which displays 12 pictures from 12 different categories (flowers, cars, electronics, etc.). To finish the authentication process, the user should select a photo that belongs to the category that assigned to his account during the account creation.

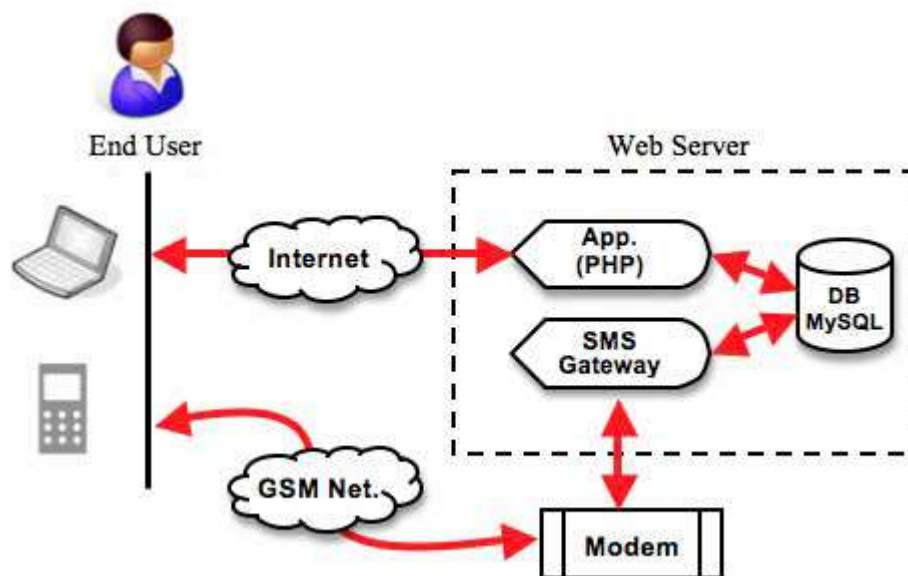


Figure 36: main authentication method

If the user successfully enters the correct information in each step, the e-government web portal system determines if the information submitted is valid or not and move forward to the next authentication step. If all and only all information in each step were valid, it gives the authorized access to the e-government web portal resources, thereby allowing the user to have access to his account, view information and perform any necessary queries and transactions. Otherwise, it blocks the access attempt.

As mentioned in chapter 6. Every successful and failed login attempt information set sent to account owner default mobile phone via SMS and

default Email address beside the status of login (successful or failed). This confirmatory feedback feature is helping in detect tampering and illegal login attempts. This will allow the account owner to take required action or actions and report such an incident quickly to the e-government authority helpdesk.

The suggested solution does not rely on traditional User ID and password. It uses Libyan government national ID that belongs to the national government database and contain all personal info of the citizens. Libyan government national ID is already exists unique number for each citizen that never changes during his life and the Libyan government rely on it in citizen's governmental transactions like electronic passports. A password is also required to initiate the login process. The rest of the steps is to prove user identity and serves as added layers of security that protects and enriches the e-government authentication system.

7.3. Security limitations that are solved by the proposed solution

The suggested solution in this dissertation overcomes the security limitations of Two-factor authentication systems. The following points are to explore the traditional Two-factor authentication system security limitations and vulnerabilities of mobile devices that the suggested solution to overcome it.

- **Untrustworthy Interface**
- **Theft/Loss of the Device**
- **Man-in-the-middle-attacks**
- **Cryptographic attacks**
- **Eavesdropping**

Moreover, human vulnerability factors like compromised password also covered by the suggested solution as it is designed to resist not only listed limitations.

There is mobile phone SMS Two-factor authentication limitations that this dissertation overcome by the Email message as a backup Two-factor authentication method. These limitations are:

- The user cannot login to the system if the GSM gateway service provider's servers are down where he could not receive the OTP even though he is a genuine user.
- The user cannot receive the OTP via mobile SMS when the user's mobile network service provider terminates the connection due to the delay in bill payments
- The user cannot receive the OTP via mobile SMS when the user is in a poor signal of the network area.
- Theft/steal of the mobile phone device of the user

That was mandatory to ensure that the user can gain access to the system and overcome these mobile phone SMS Two-factor authentication limitations.

7.4.E-government web portal user account creation and first login steps

In addition to the normal mandatory documents, procedures and paperwork that's beyond the scope of this dissertation as it only focusing on technical IT aspects. When the e-government web portal system administrator creates a new user account for an ordinary citizen, he and the account user should follow these steps:

- The user name will be the national ID number, which is already exists unique number for each citizen and the Libyan government relies on it in citizen's governmental transactions like electronic passports.

- A randomly system generated password will be the password of the account. The system will force the user to change the password during his first login to the system.
- For security reasons, the account will remain disabled until the account user came in person to the e-government portal service desk. The system administrator should add at least one mobile number, and one Email address belongs to the account owner in order to activate the account. In addition, the user will choose a photo category to use it in the image based authentication step. There are 12 available different categories. National, ancients, desert, animals, flowers, cars, electronics, furniture, buildings, tools, people and food.
- Once the system administrator activates the account. An SMS and Email message contains the login credentials will be sent to the account user immediately. The randomly generated account password will be valid for only the first login. During this login, the user will be forced to change his password.
- When the account user opens the e-government web portal home page. He will login using the credentials sent to him during the account activation.
- In the first step login page, the user asked to enter his national ID and account password to proceed to the next page.
- If the national ID is belongs to an existing account and the password entered correctly. The system will direct the user to the second login page. In the second step login page, the user will choose the desired registered mobile phone number to send the OTP to it via SMS (as the system can register more than one mobile phone number per account). Only the last two digits are displayed to the user (Like *****43). After that, the user will be directed to the third login page that asked for the login session OTP that the system will send it to the user via SMS.

- The system generate and send the login session OTP to the user via SMS. The message will contain beside the one-time password the session ID, login request time, login request location, and used browser and OS details.
- The user enter the received OTP in the third login page and proceeds. If entered correctly, the user will be forwarded to the image based authentication final step when the system displays 12 pictures from 12 different categories (National, ancients, desert, animals, flowers, cars, electronics, furniture, buildings, tools, people and food). To finish the authentication process, the user should select a photo that belongs to the category that assigned to his account during the account activation.
- If every previously stated step done correctly, the user will be logged in securely to the e-government web portal but after he forced to change the account password with his own created rather than the system-generated password. As mentioned before the system forces the user to change the randomly generated password during the first login only.
- After successful password change, the user now can access the e-government web portal information and databases. Perform his governmental transactions, queries, and benefit of other services that the e-government web portal provides. The governmental transactions the user takes after successful login to the system are beyond the scope of this dissertation.
- During a successful login, and through the account options page. The user can change the account password, change or add up to three mobile numbers. Change or add up to three Email addresses. Change the photo category of image based authentication step. These options can be changed and modified any time after a successful login to the system.

The above scenario is the normal scenario for the system accounts creation and users login, use and modify the account login information (Password, Mobile number and Email address. Image recognition category).

Figure 37 shows the account creation and normal login process flow chart.

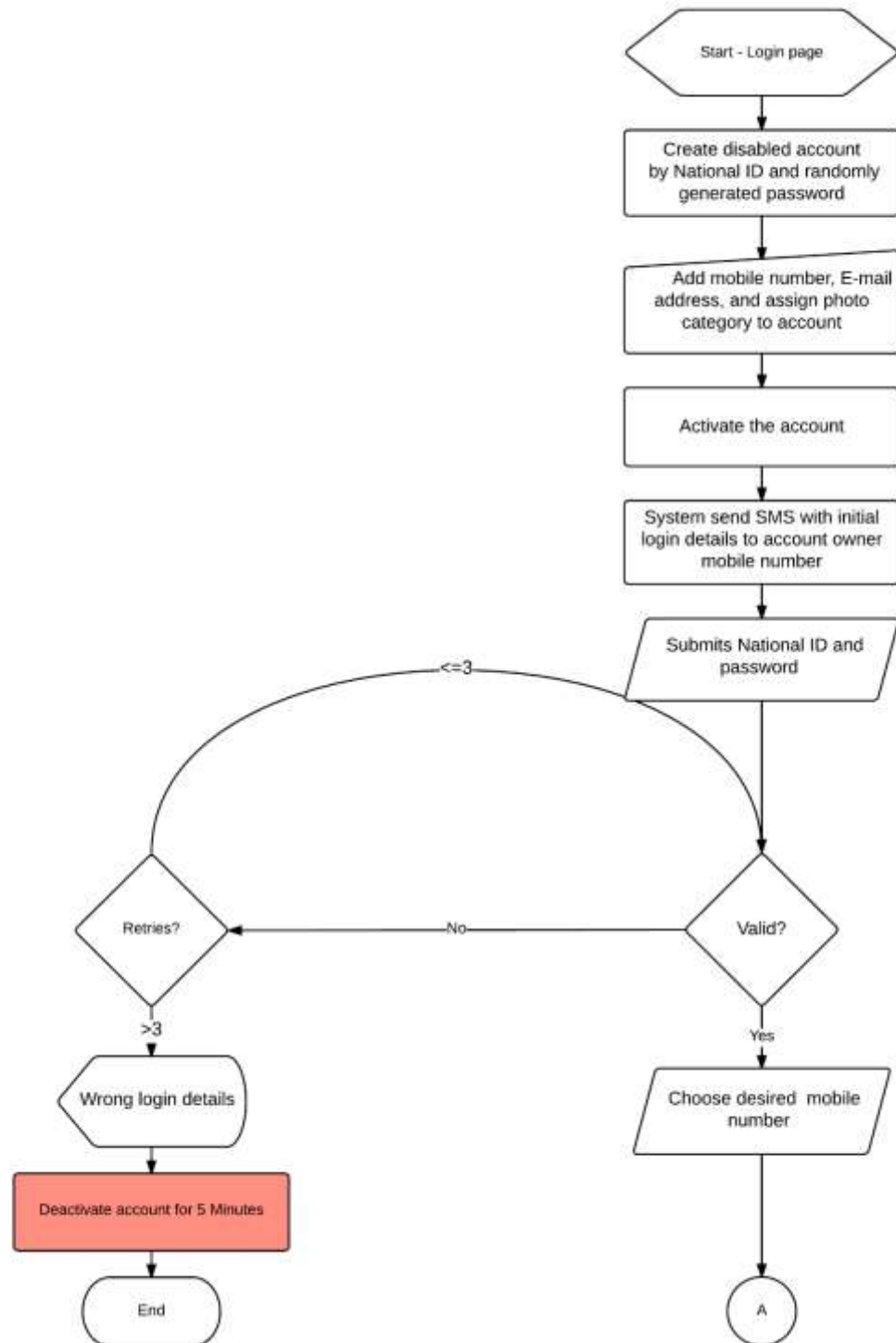


Figure 37: Account creation and normal login process flow chart.

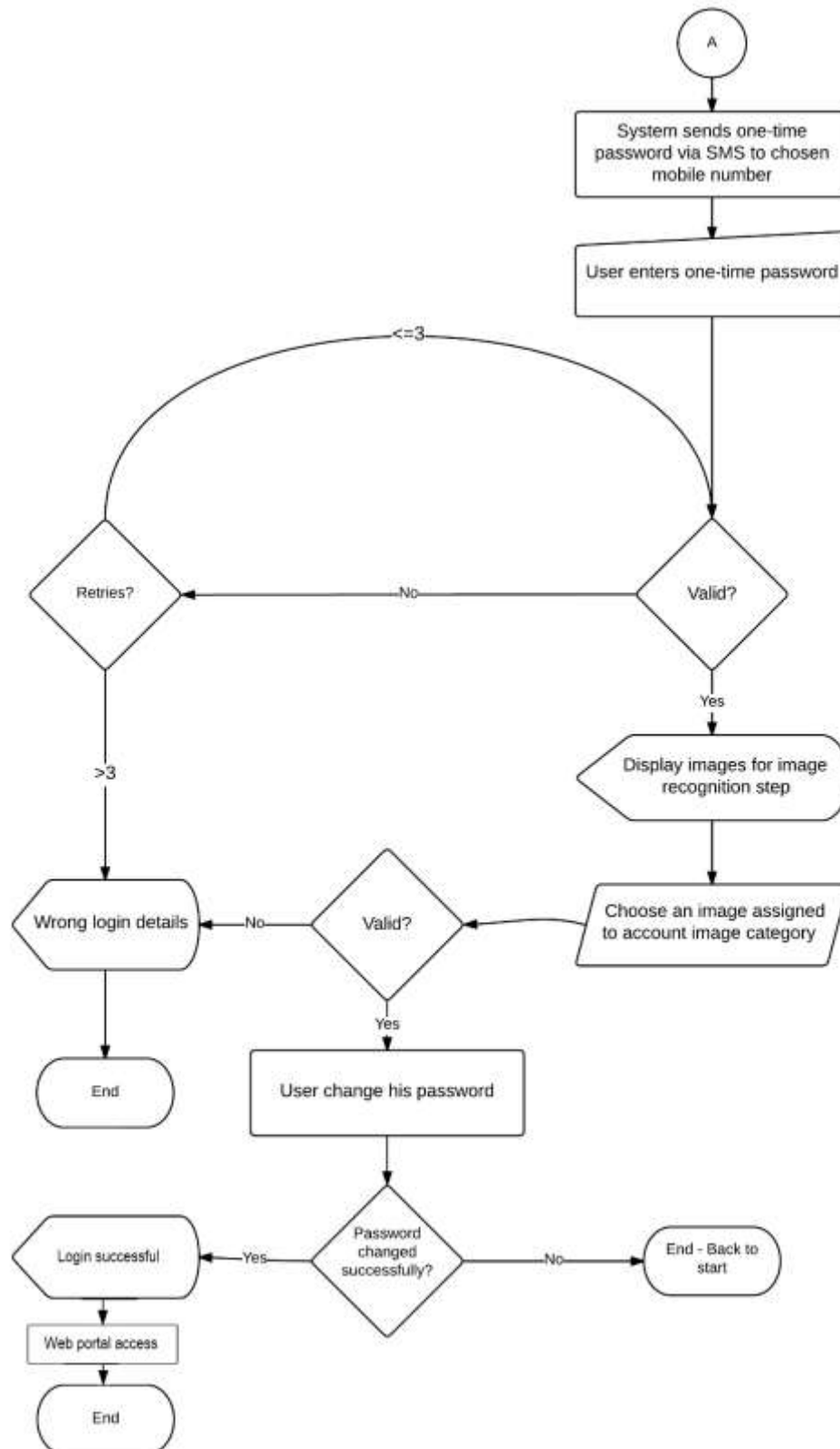


Figure 37: Account creation and normal login process flow chart.

7.5.E-government web portal normal login steps

The normal login steps are slightly different from the first login of the new account process. The account user should follow these steps to login to the system:

- When the account user opens the e-government web portal home page and in the first step login page, the user prompted to enter his national ID and account password to proceed to the next page.
- If the national ID and password correct. The system will direct the user to the second login page. In the second step login page, the user will choose the desired registered mobile phone number to send the OTP to it via SMS (as the system can register more than one mobile phone number per account). Only the last two digits are displayed to the user (Like *****43). After that, the user will be directed to the third login page that asked for the login session OTP that the system will send it to the user via SMS. If the user configured more than one mobile number. He can choose which number he prefers to deliver the OTP.
- The system generate and send the login session OTP to the user via SMS. The message will contain beside the one-time password the session ID, login request time, login request location, and used browser and OS details.
- The user enter the received OTP in the third login page and proceeds. In addition, the user can request to re-send the OTP by clicking a button in case he does not receive it on time. If OTP entered correctly, the user be will processed into the image based authentication final step where the system displays 12 pictures from 12 different categories (National, ancients, desert, animals, flowers, cars, electronics, furniture, buildings, tools, people and food). To finish the authentication process, the user should select a photo that

belongs to the category that assigned to his account during the account activation.

- If every previous step done correctly, the user will be logged in securely to the e-government web portal and can access the e-government web portal information and databases.
- During a successful login, and through the account options page. The user can change the account password, change or add up to three mobile numbers. Change or add up to three Email addresses. Change the photo category of image based authentication step. These options can be changed and modified any time after a successful login to the system.

Figure 38 shows the normal login process flow chart.

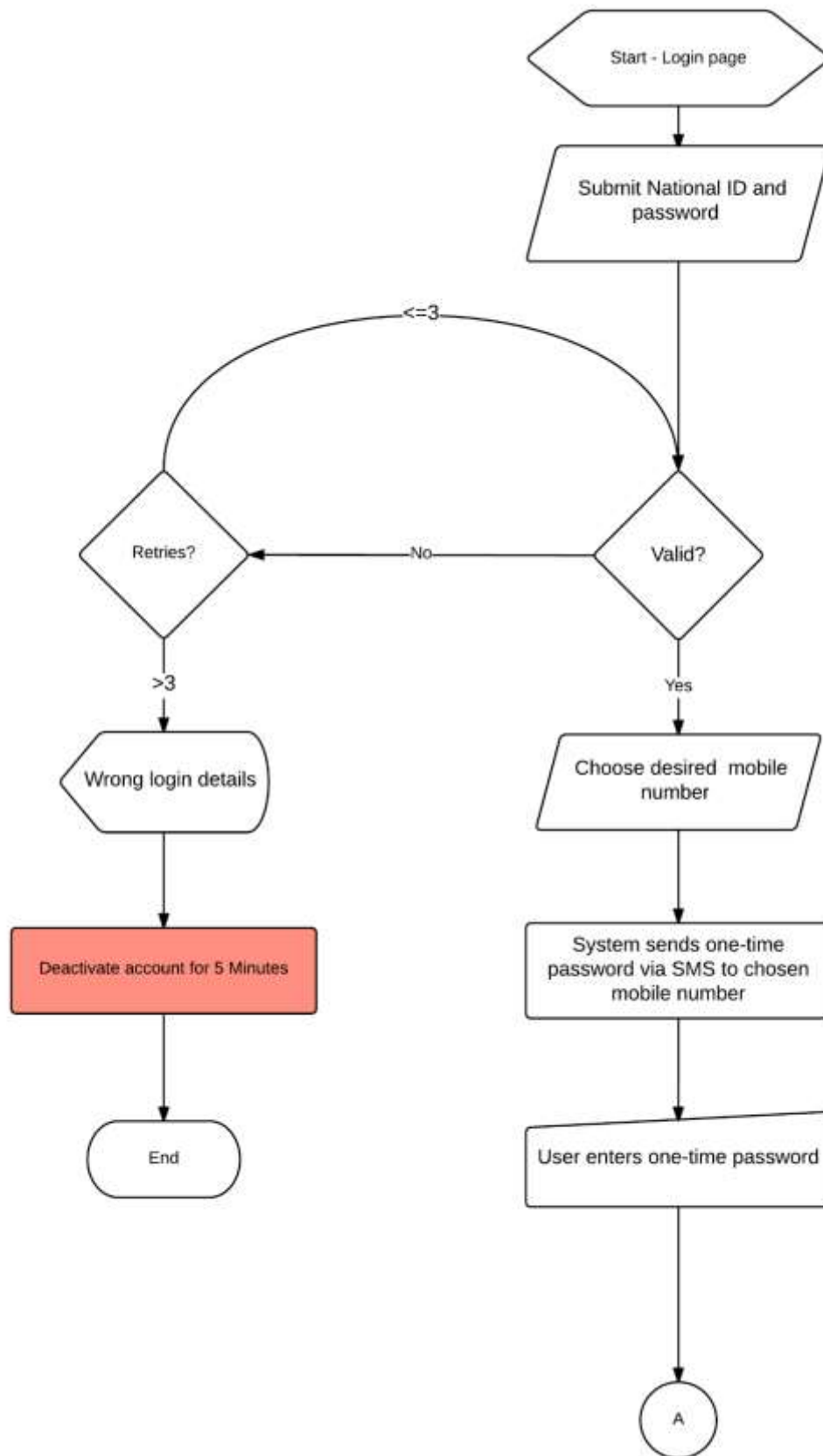


Figure 38: Normal login process flow chart.

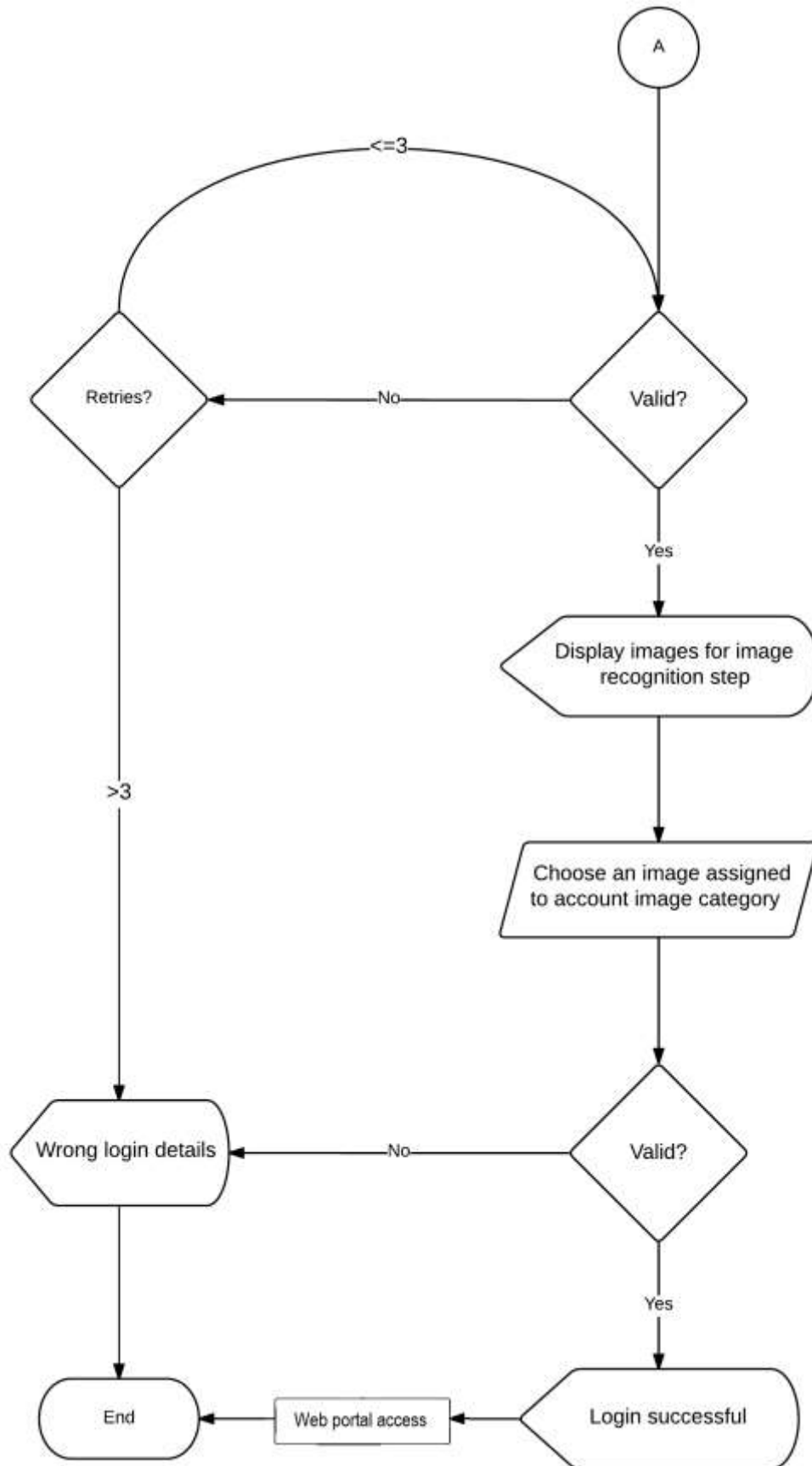


Figure 38: Normal login process flow chart.

7.6. Emergency user account login steps

In case of emergency that prevent the user from login to his account like forgotten password, SMS delays, mobile phone theft, etc. User should go through emergency steps based on the emergency scenario:

- **Password lost/forgot:** While the user still in the first login page that asked for the user ID and password. The user will click a link in that page to let the system knows that he lost his password. He will be redirected to be asked a three questions like a birth date or mother's name. These questions will be displayed a one question per page and will not redirect to the next question until a correct answer submitted. After answering the three questions correctly, the system will generate a new random password and asks the user about the user's Email address that has configured previously in the system to send the new password. The user will use the new randomly generated password to access the portal for one time only because he will be forced to change it during the login process.
- **Mobile phone lost/SMS delays:** while the user in the second login page that asked the user to choose the desired mobile number to receive OTP, a login via another method link on that page always appears to the user. By clicking login via another method link. The user will be directed to another page asked about how to receive the OTP, he can choose a registered Email address to send an Email message contains the OTP, or an alternative mobile phone number to send an SMS containing the OTP. Then the system will send the OTP to the desired communication channel alongside login session information set. Then the user will continue the login process normally with image based authentication step. Once the user has logged in successfully to the system, he can take any required actions to protect his account, like removing a stolen mobile number from registered mobile numbers in account options page.

In any other case that prevent the user from gaining access to the e-government web portal and the backup methods did not help the user to do so. The account owner should contact the e-government portal service desk in person. The service desk will be able after the user proves his identity to recover the account and let him access his account as normal.

Figures 39 and 40 shows the emergency user account login steps flow charts in case of Password lost/forgot and Mobile phone lost/SMS delays.

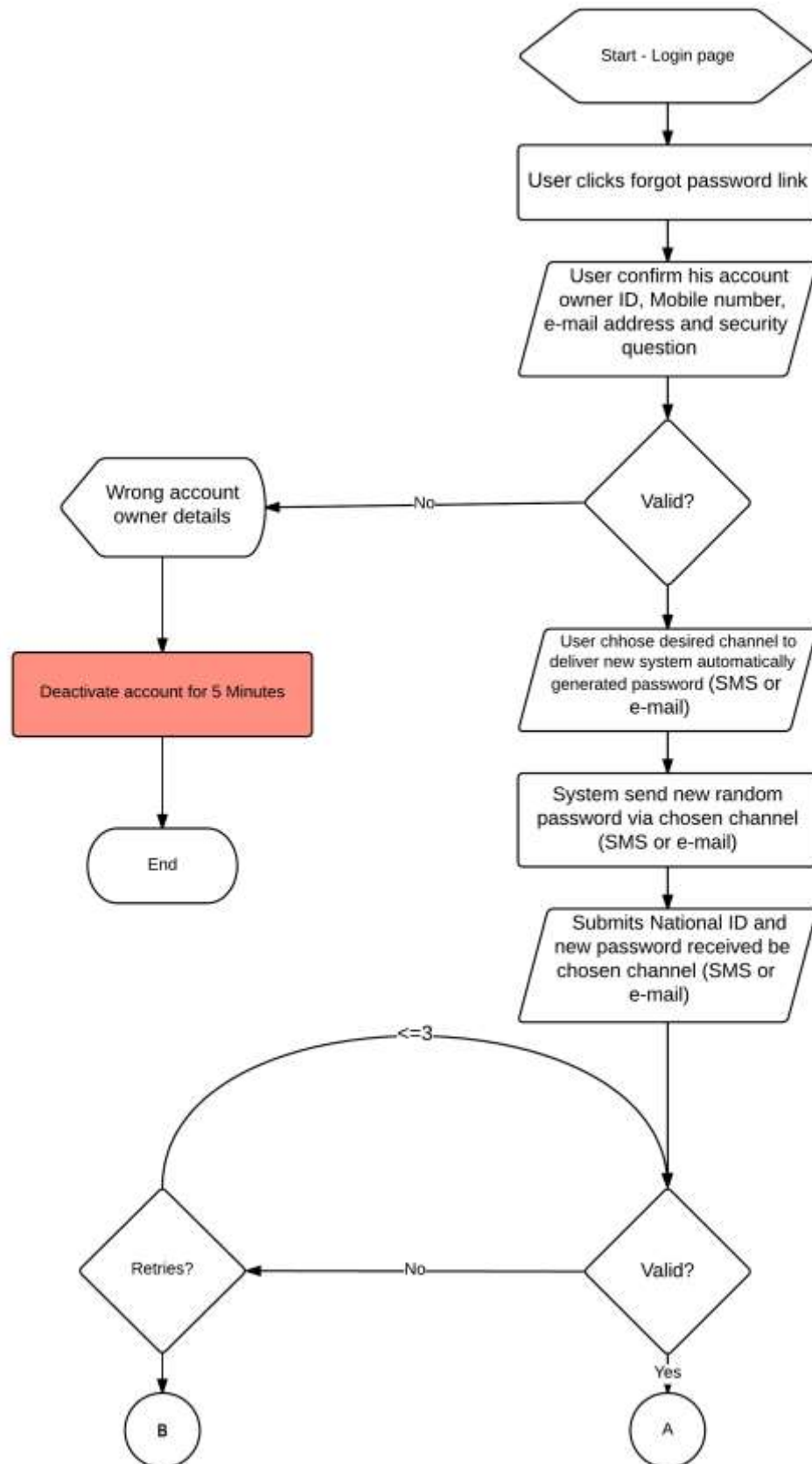


Figure 39: Emergency account login steps - Password lost/forgot flow chart

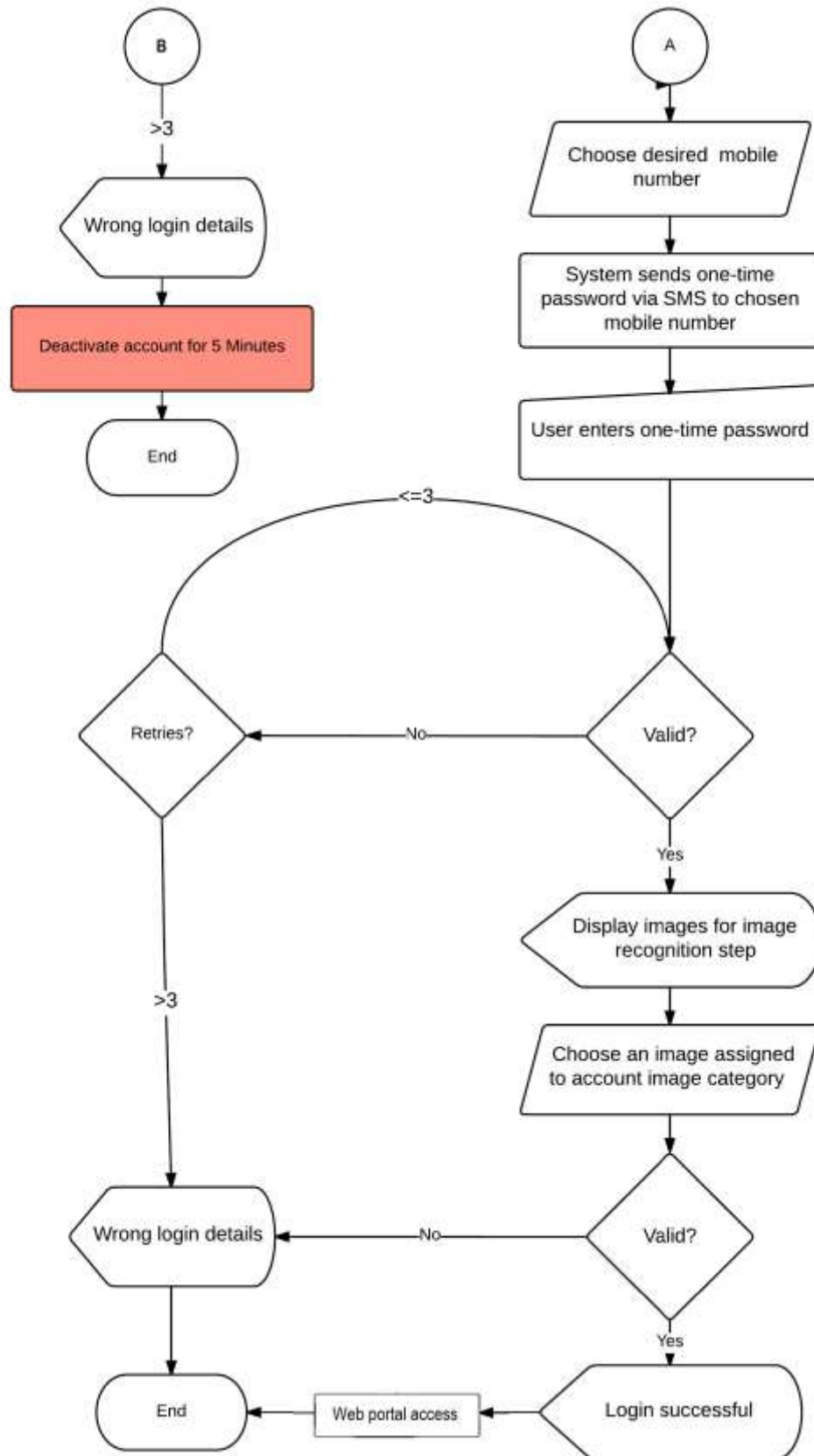


Figure 39: Emergency account login steps - Password lost/forgot flow chart

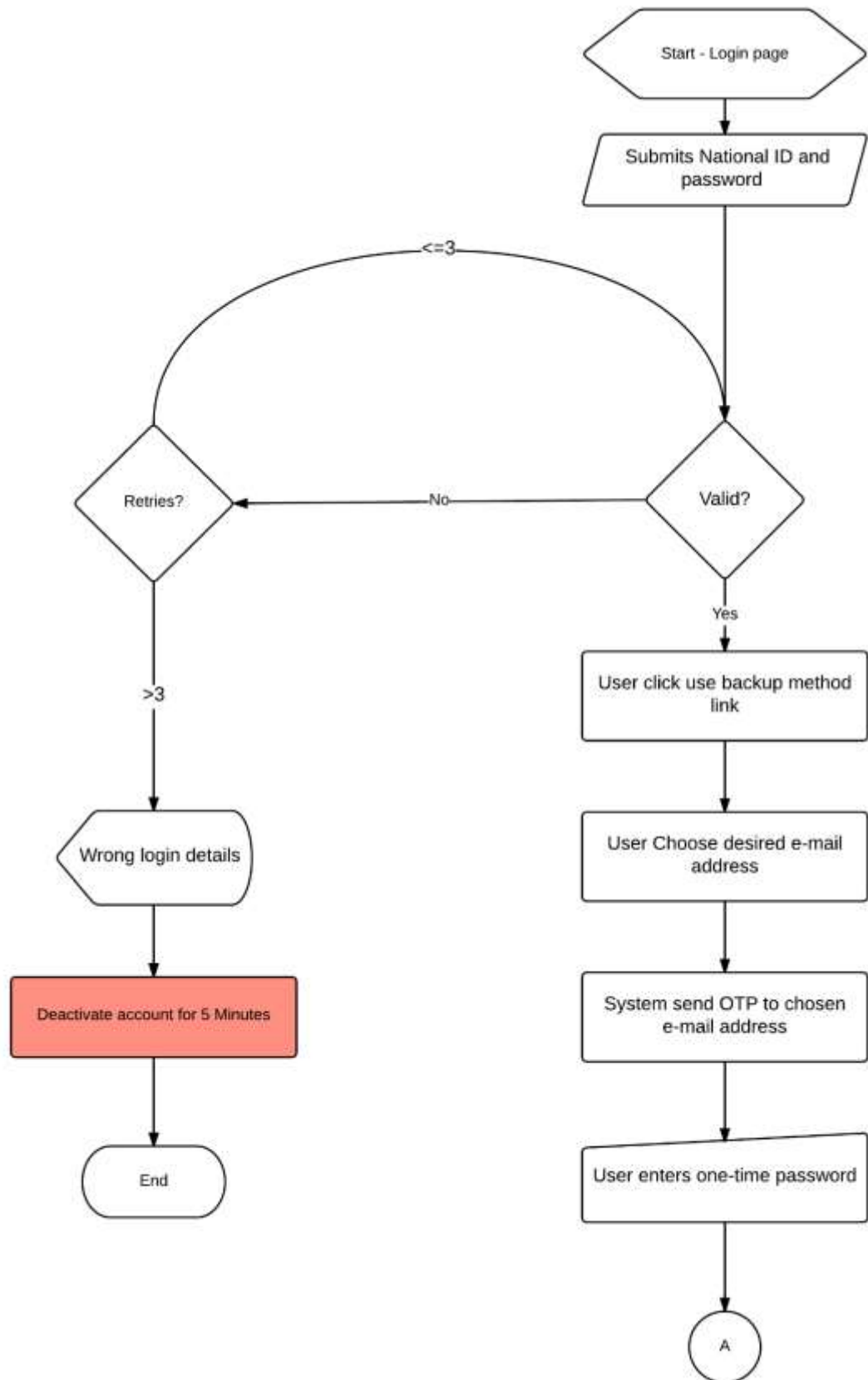


Figure 40: Emergency account login steps - Mobile phone lost/SMS delays flow chart

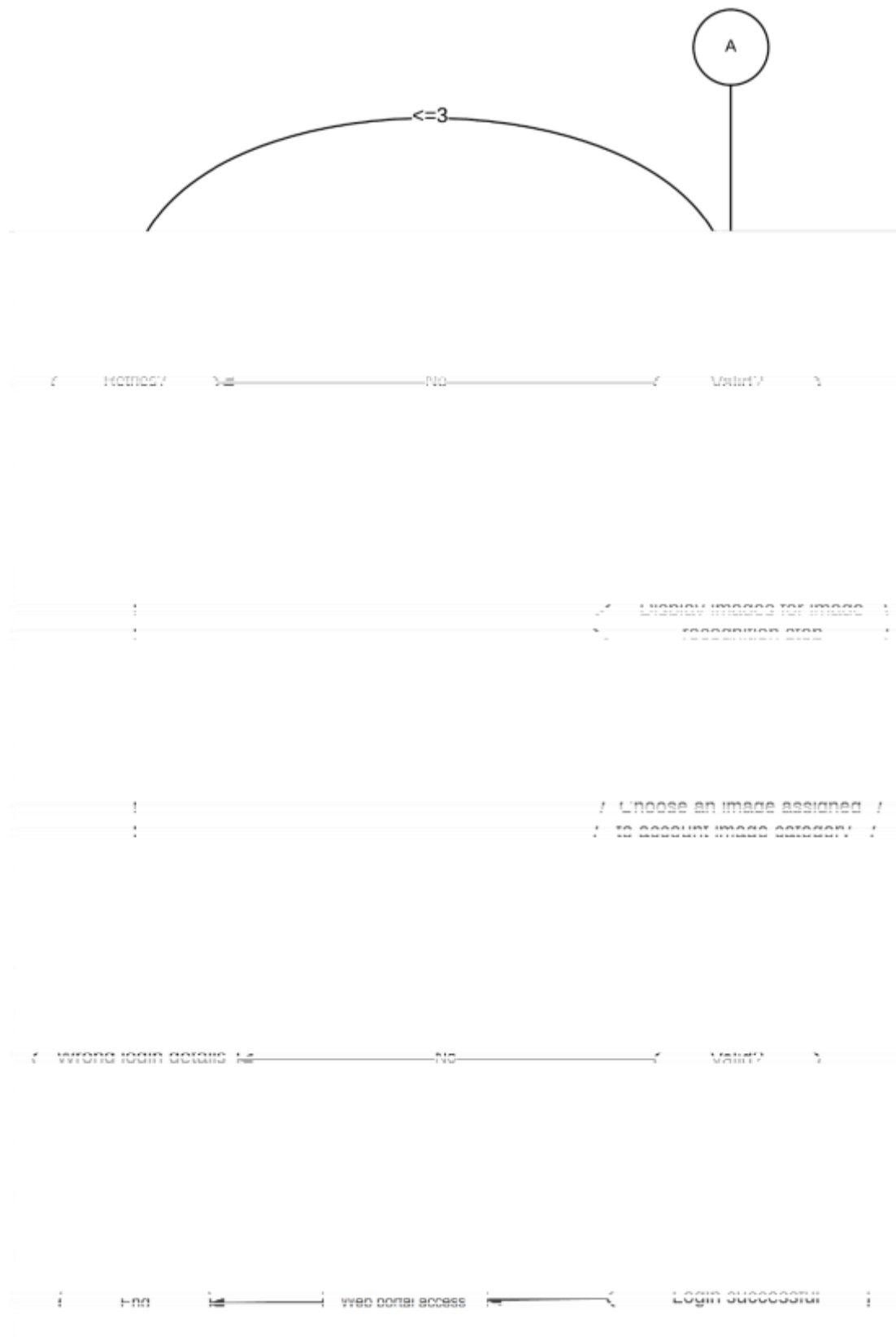


Figure 40: Emergency account login steps - Mobile phone lost/SMS delays flow chart

8. Conclusion

This chapter gives a brief conclusion of the dissertation, including objectives, contributions and future work

8.1. Introduction

The recent advances in communication and Internet technology have made online services more widely accessible. This has encouraged enterprises around the world, including governmental sector, to utilize online services for new opportunities. E-government web portal services offered by governments was one of these services. E-government web portal offered citizens usable and accessible ways of doing governmental transactions and queries from home or work. Other technologies like 3G/LTE networks, have allowed citizens to access their e-government accounts and accomplish transaction requests using portable devices like mobile phones, tablets and notebooks.

On the other hand, these technological advances, along with the rich and sensitive information exchanged between the citizens and their e-government service providers have attracted internet users with other agendas, using their skills and developing new techniques to penetrate e-government user accounts and use it illegally.

This dissertation proposed a multi-step Two-factor authentication mechanism that combines the strength of the three popular authentication approaches: multilevel, multi-channel, and multi-factor. These three authentication approaches were merged to form an authentication mechanism that can better protect e-government user accounts against most known attacks including phishing and MITM. Also gives protection from using a compromised account credentials.

Technical comparisons and tradeoffs, a cloud Two-factor authentication web-application, a custom online survey participated by 173 different user used to support the evaluation of the dissertation statement:

“It is possible to design a low-cost, easy to distribute authentication mechanism that uses Two-factor authentication to resist attacks more effectively than most commonly used Two-factor authentication mechanisms, and will be also usable and acceptable to ordinary users of Libyan e-government web portal.”

8.2. Research Objectives and Contributions

The general research topic addressed by this dissertation was whether the security of e-government web portal user accounts authentication could be increased while maintaining or also increasing usability. The specific dissertation statement as mentioned before being “It is possible to design a low-cost, easy to distribute authentication mechanism that uses Two-factor authentication to resist attacks more effectively than most commonly used Two-factor authentication mechanisms, and will be also usable and acceptable to ordinary users of Libyan e-government web portal”. The main research objectives defined in this dissertation were as follows:

- **Objective 1:** Review the most commonly used authentication classes, authentication mechanisms, and authentication attacks.
- **Objective 2:** Review the usability and acceptability aspects of authentication mechanisms and the evaluation techniques used to decide high secure and easy to use Two-factor authentication solution for Libyan e-government portal.
- **Objective 3:** With respect to e-government web portal needs, discuss some of the currently used authentication mechanisms and identify their weaknesses, showing how they fail to protect customer accounts against different attacks identified in objective1.

- **Objective 4:** Propose an authentication solution that addresses the security and usability problems identified and listed in objective 2. Theoretically evaluate the security of this solution and identify all features needed for implementation.

To meet these objectives, three authentication factors were identified to be used as a second authentication channel: knowledge-based, possession-based and biometric-based. Eight authentication methods belong to these factors were compared to identify the advantages and disadvantages of each. Finally, various attack methods that target these authentication mechanisms were discussed based on the communication component they target. These core communication components are the online service provider, communication channel and the end user.

The status of e-government web portal was discussed. The needs of authentication mechanism setup depending on the risk associated with the services offered and usability needs. In order to evaluate mechanisms, further discussions identified the points of failure. Which is: The organization IT environment, the target user skills, adopt a risk-based approach and finally avoid unnecessary cost and complexity

Proposing a new multi-step, multi-channel Two-factor authentication system. This was intended to increase security while maintains the usability of the proposed solution. It further utilized an emergency authentication mechanism by Email message that can be triggered in case the secondary channel device (the mobile phone) is unavailable to complete the authentication process. Finally, a list of other features and guidelines were included to complement and facilitate the actual implementation of the proposed Two-factor authentication solution.

The usability and acceptability of the proposed solution were evaluated based on technical comparisons and tradeoffs and inviting random sample of citizens to answer an online survey were used to collect feedback from the participants. These data were analyzed to identify the factors affecting the adoption of Two-factor authentication in Libyan e-government web portal and help to improve the usability and acceptability of the proposed solution.

The risks exposed to the e-government web portal system access can be mitigated the proposed solution. The approach discussed throughout this dissertation concluded to use the Libyan citizens National ID with a password that followed by OTP and login session details sent via mobile phone SMS and finally an Image-based authentication step to authenticate the user. Furthermore, a backup method is used for emergencies by sending the OTP via Email message. A confirmatory feedback SMS and Email message contains a login session details will be sent to the account owner after every success or failed login process. The authentication steps belongs to two different authentication factors. The proposed authentication mechanism uses encrypted TLS 256bit web communication protocol and has the capacity to provide the required information security as per the modern industry standards against illegal authentication threats.

8.3.Future Work

This dissertation has contributed to multi-step, multi-channel usable and improved security Two-factor authentication system for Libya e-government web portal. It also raised new research directions. The following points discuss these research opportunities in more detail.

8.3.1. More Usable Channels

Mobile devices have proven to be a usable complementary channel for online authentication. Other possible usable communication channels can also be used to support Two-factor authentication. These channels need

to be tested for usability and security when used with other conventional authentication mechanisms. This includes chatting software (live contact services) that can be used in Two-factor authentication. People can be allowed to set preferences on these services to receive their OTPs.

8.3.2. Two-factor authentication for the disabled people

Disabled users might find it difficult to utilize Two-factor authentication for their e-government transactions. The proposed Two-factor authentication system needs further investigation to see how it can be improved to meet the requirements of different disabilities.

8.4.A Final Word

This dissertation proposed an advanced multi-step, multi-channel Two-factor authentication system that improves authentication security of Libyan e-government web portal while maintaining usability. It also showed how the proposed authentication system could protect system user accounts from most known illegal access attacks that other Two-factor authentication mechanisms fails to address it.

The proposed solution and recommendations provided in this dissertation gives a guidelines to implement a strong authentication system for the Libyan e-government web portal. Providing high security and high usability authentication system.

References

- [1] *Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment*, August 15, 2006
- [1] *Design of Two-Way One-Time-Password Authentication Scheme Based On True Random Numbers*. Second International Workshop on Computer Science and Engineering 2009.
- [2] Long M. Blumenthal, U. Manageable *One-Time Password for Consumer Applications*. Consumer Electronics, 2007. ICCE 2007.
- [3] Do van Thanh Jorstad, I.Jonvik, and T.Do Van Thuan. *Strong Authentication with Mobile Phone as Security Token, Mobile Adhoc and Sensor Systems*, 2009. IEEE 6th International Conference.
- [4] Michael Pearce, Ray Hunt, Sherali Zeadally. *Assessing and Improving Authentication Confidence Management*, University of Canterbury, New Zealand and University of the District of Columbia.
- [5] Roberto Di Pietro, Gianluigi Me, Maurizio A.Strangio. *A Two –Factor Mobile Authentication Scheme for Secure Financial Transactions*. International Conference on Mobile Business 2005.
- [6] Aloul F, Zahidi S, El-Hajj W. *Two Factor Authentication Using Mobile Phones*, IEEE/ACS International Conference on Computer Systems and Applications.
- [7] Harris, J.A. *A One Time Password Scheme* .International conference on Parallel Processing Workshops, 2002 .Proceedings.
- [8] *Electronic Authentication Guideline*. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63.
- [9] *Password Standard*, State Services Commission New Zealand.
- [10] T. D. K. D. Wanli Ma, Campbell J. *Password Entropy and Password Quality*. In *Network and System Security (NSS)*, 2010 4th International Conference. Sept. 2010.

- [11] A. R. G. A. Yan J., Blackwell A. *Password memorability and security: empirical results* In *Security & Privacy*, IEEE (Volume:2 , Issue: 5). Sept.-Oct. 2004.
- [12] A. Allan. *Passwords Are Near the Breaking Point*. Technical report, Gartner, December 2004.
- [13] *Frequently Asked Questions on FFIEC Guidance on Multi-factor Authentication*, February 22, 2009.
- [14] RSA Security. *RSA mobile and RSA Securid*. December 2002.
- [15] *HOTP: An HMAC-Based One-Time Password Algorithm*. RFC 4226.
- [16] *TOTP: Time-Based One-Time Password Algorithm*. RFC 6238.
- [17] Angela Moscaritolo (2011-07-12). *Zeus for Android steals one-time banking passwords*. SC Magazine.
- [18] *Authentication in an Internet Banking Environment*. URL http://www.ffiec.gov/pdf/authentication_guidance.pdf.
- [19] *Security Requirements for Cryptographic Modules*. Federal Information Processing Standards Publication 140-2.
- [20] B. Nanus and L. Farr, *Some cost contributors to large-scale programs*, in The Spring Joint Computer Conference, 1964, p. 239.
- [21] D. A. Garvin, *What does Product Quality Really Mean?*, MIT Sloan Management Review, vol. 26, p. 18, 1984.
- [22] J. Nielsen, *Usability engineering*. Boston Academic Press, 1993.
- [23] W. Quesenbery, *Storytelling for User Experience: Crafting Stories for Better Design*, 1 ed.: Rosenfeld Media, 2010.
- [24] ISO, *"Ergonomic requirements for office work with visual display"*
- [25] *The Identity Lifecycle, Part 1* (Brent Williams, 2010)
- [26] A.medrano, *Online Banking Security-Layers of protection* available at <http://ezinearticles.com/?Online-Banking-Security---Layers-of-Protection&id=1353184>

- [27] Barkan, Elad; Eli Biham; Nathan Keller (2003). *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*, Cryptome 2003: 600–16.
- [28] *Reliance spells end of road for ICT amateurs*, May 07, 2013, The Australian.
- [29] *Understanding cyber security online threat*. URL <http://www.evolllution.com/opinions/cybersecurity-understanding-online-threat/>.
- [30] *An Investigation into the Usability and Acceptability of Multi-channel Authentication*. Ph.D. dissertation by Mohamed Ali Al-Fairuz. University of Glasgow
- [31] *The drawbacks of Two-factor authentication*. URL <http://searchitchannel.techtarget.com/tip/The-drawbacks-of-two-factor-authentication>
- [32] *Two-factor authentication is a false sense of security*. URL <http://venturebeat.com/2013/05/01/two-factor-authentication/>
- [33] Harris, Shon, *All-in-one CISSP Exam Guide*, 6th Edition. McGraw Hill Osborne, Emeryville, California, 2012.
- [34] *Attribute Based Access Control (ABAC) overview*. National Institute of Standards and Technology. URL <http://csrc.nist.gov/projects/abac/>
- [35] *Image based authentication*. URL <http://www.slideshare.net/ahlamansari/image-based-authentication>

APPENDIX A Online survey questions

استطلاع للرأي حول استخدام المصفحة المزودة للولوج لخدمات الحكومة الإلكترونية هي أهدأ

استطلاع الإنترنت

0 %

استطلاع للرأي حول استخدام المصفحة المزودة للولوج لخدمات الحكومة الإلكترونية في ليبيا

نوع الإلكتروني

الجنس *

ذكر ☐

أنثى ☐

العمر *

18 - 25 سنة ☐

26 - 33 سنة ☐

34 - 40 سنة ☐

41 - 48 سنة ☐

49 - 56 سنة ☐

57 - 64 سنة ☐

أكثر من 64 سنة ☐

الموطن الأصلي *

أتردد، الإجابات ...

ما هو العمل القومي لاستخدامك لخدمة الإنترنت *

أقل من 30 دقيقة ☐

من 30 دقيقة إلى ساعة ☐

من ساعة إلى ساعتين ☐

من ساعتين لأربع ساعات ☐

أكثر من أربع ساعات ودياً ☐

هل تستخدم خدمات تعدد على شبكات حرة مثل الفيسبوك الإلكترونية *

نعم ☐

لا ☐

هل تتجه بالآمان عند حماية الخدمات الإلكترونية عن طريق إسم مستخدم وكلمة مرور فقط *

نعم ☐

لا ☐

هل تستخدم خدمات الهاتف النقال أكثر من الشبكات الشخصية بشكل أساسي *

نعم ☐

لا ☐

<https://www.esurveycrator.com/s/43b6afe>

1/2

استطلاع الرأي حول استخدام التكنولوجيا المدمجة لتوزيع الخدمات الحكومية الإلكترونية في ليبيا

ما هو إخطاؤك عن حمل أداة إلكترونية لتأمين دخولك على بوابة الحكومة الإلكترونية *

- ☐ دائم مبداهي في تأمين الدخول فالتابع من ذلك .
- ☐ لا أجد ذلك فلهذا يكون حرجا للخدمات

ملا لتفني أدوات إلكترونية لتأمين دخولك على بوابة الحكومة الإلكترونية *

- ☐ أداة تقوم بتوليد رقم سري
- ☐ أداة تقوم بتوصيلها بجهاز كمبيوتر
- ☐ خدمة ترسل القصير بالهاتف النقال
- ☐ برنامج يوافق التالي يقوم بتوليد رقم سري للدخول
- ☐ تديره ببرنامج من طريق هاتفك النقال يكون أو رفض الدخول لشخص
- ☐ رسالة بريد إلكتروني
- ☐ استخدام بصمة الإصبع
- ☐ استخدام بصمة العين

هل ترغب بشراء معدات إلكترونية نظرية بصمتك الإصبع أو بصمة العين لتأمين دخولك على بوابة الحكومة الإلكترونية *

- ☐ نعم
- ☐ لا

هل تستخدم هاتفك النقال أو حاسوبك الشخصي للدخول إلى بوابة الحكومة الإلكترونية *

- ☐ نعم
- ☐ لا

هل ترغب بتطبيق برامج أو تعريفات إلكترونية في حاسوبك أو هاتفك النقال كتمديد في تأمين دخولك على بوابة الحكومة الإلكترونية *

- ☐ نعم
- ☐ لا

مؤلف الاستبيان: Hamdi Ahmed, hamdi.ahmed@gmail.com

Online surveys for free! Quick and easy with www.surveymonkey.com

APPENDIX B Online survey detailed results

استطلاع للرأي حول استخدام المصادقة المزدوجة للولوج للخدمات الحكومية الإلكترونية في ليبيا

1. البريد الإلكتروني *

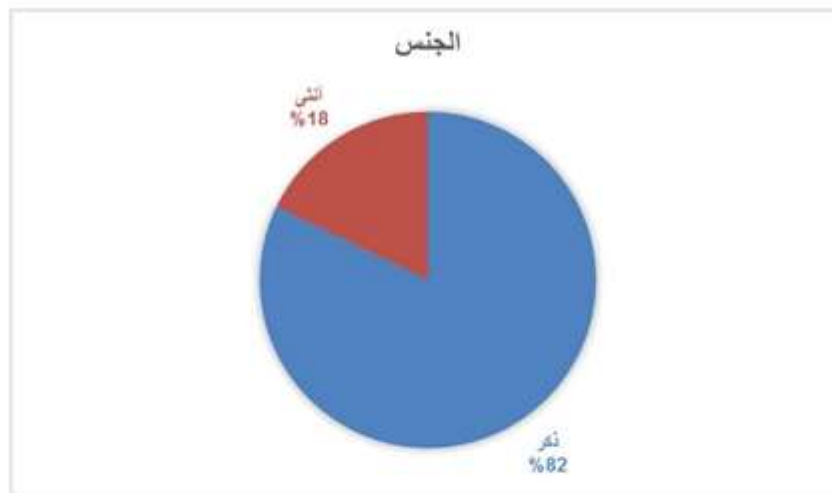
عدد المشاركين: 86

2. الجنس *

عدد المشاركين: 174

ذكور: 143 (82.18%)

إناث: 31 (17.81%)



3. العمر *

عدد المشاركين: 174

سنة 18 - 25: 39 (22.41%)

سنة 26 - 33: 54 (31.03%)

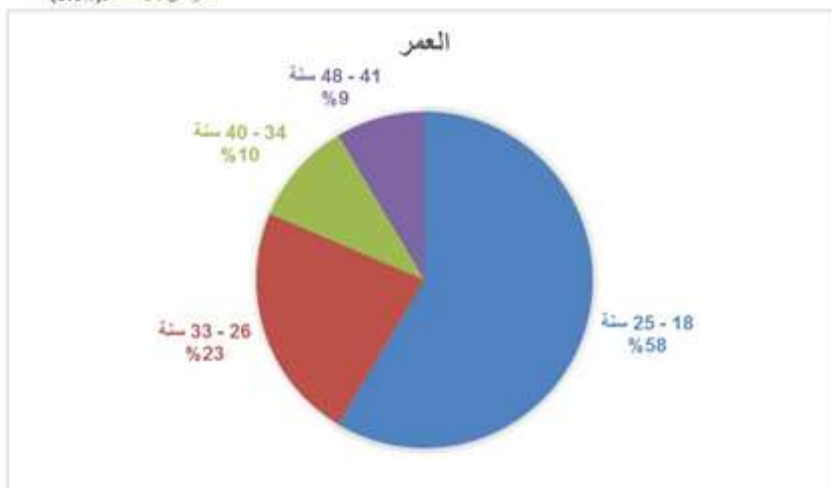
سنة 34 - 40: 48 (27.58%)

سنة 41 - 48: 21 (12.06%)

سنة 49 - 56: 9 (5.17%)

سنة 57 - 64: 3 (1.72%)

أكثر من 64 سنة: 0 (0.0%)



4. المؤهل العلمي *

عدد المشاركين: 174

تحت المتوسط: (1.14%) 2

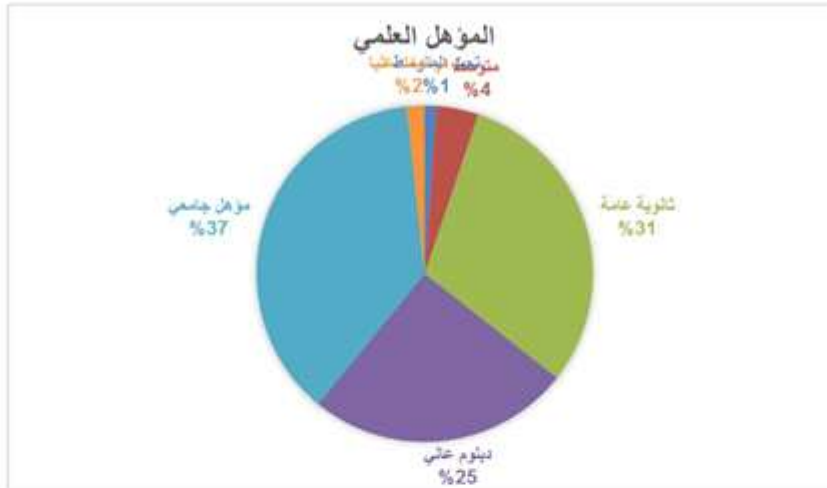
متوسط: (4.02%) 7

ثانوية عامة: (30.45%) 53

دبلوم عالي: (25.28%) 44

مؤهل جامعي: (37.35%) 65

دراسات عليا: (1.72%) 3



5. المعدل اليومي لاستخدام الإنترنت *

عدد المشاركين: 174

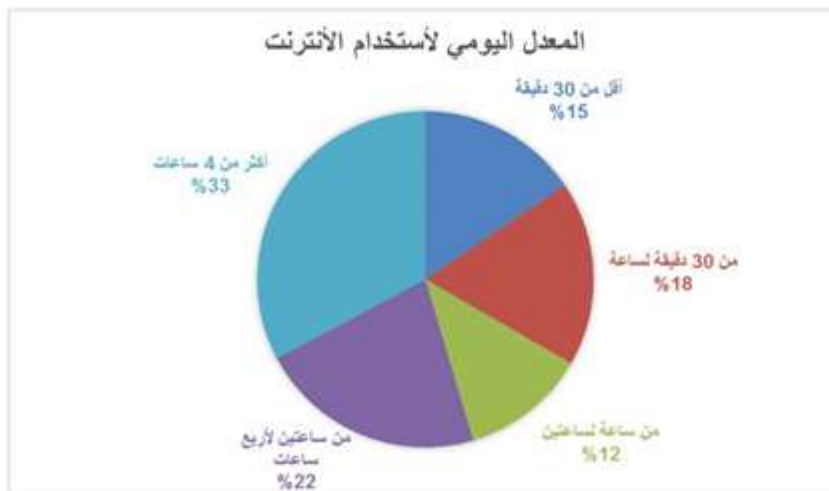
أقل من 30 دقيقة: (15.51%) 27

من ساعة إلى 30 دقيقة: (17.81%) 31

من ساعة إلى ساعتين: (12.06%) 21

من ساعتين لأربع ساعات: (21.83%) 38

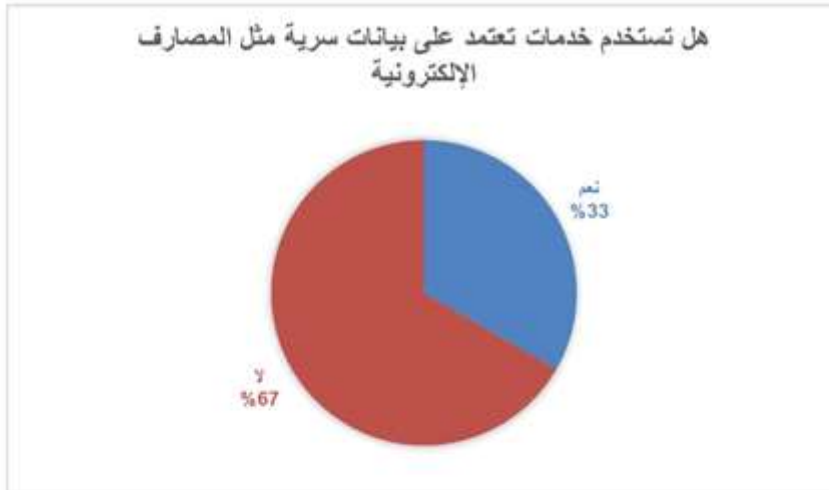
من ساعتين لأربع ساعات: (32.75%) 57



6. هل تستخدم خدمات تعتمد على بيانات سرية مثل المصارف الإلكترونية *

عدد المشاركين: 174

نعم: 58 (33.33%)
لا: 116 (66.66%)

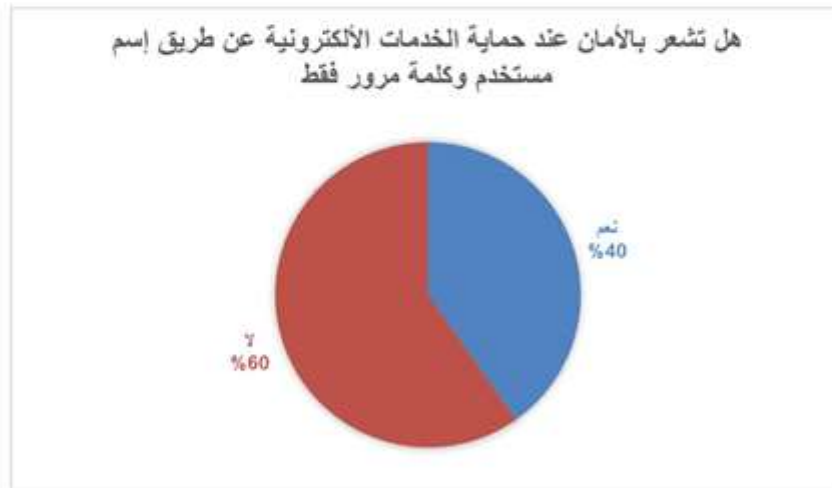


7. هل تشعر بالأمان عند حماية الخدمات الإلكترونية عن طريق اسم مستخدم وكلمة مرور فقط *

عدد المشاركين: 174

نعم: 70 (40.22%)

لا: 104 (59.77%)

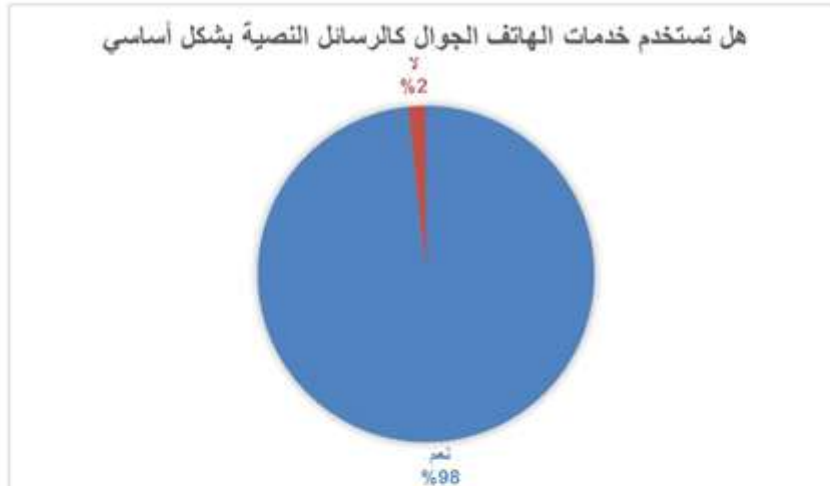


8. هل تستخدم خدمات الهاتف الجوال كالرسائل النصية بشكل أساسي *

عدد المشاركين: 174

نعم: 171 (98.27%)

لا: 3 (1.72%)

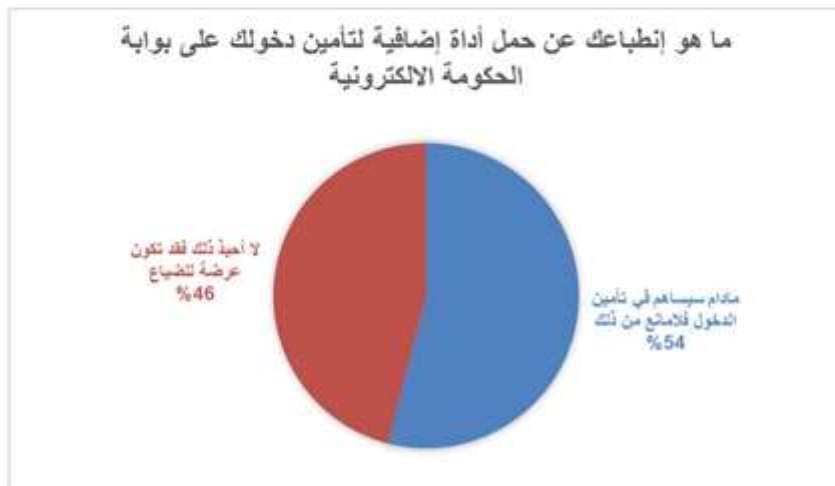


9. ما هو انطباعتك عن حمل أداة إضافية لتأمين دخولك على بوابة الحكومة الإلكترونية *

عدد المشاركين: 174

مادام سيساهم في تأمين: 94 (54.02%)

الدخول فلا مانع من ذلك



ماذا تفضل كأداة إضافية لتأمين دخولك على بوابة

الحكومة الإلكترونية *

174 : عدد المشاركين

أداة تقوم بتوليد رقم سري: 24 (13.79%)

أداة تقوم بتوصيلها بجهاز الكمبيوتر: 43 (24.71%)

خدمة الرسائل القصيرة: 112 (64.36%)

بإلحاق التذا

توليد بملفك الذي يقوم بتوليد رقم سري للدخول: 105 (60.34%)

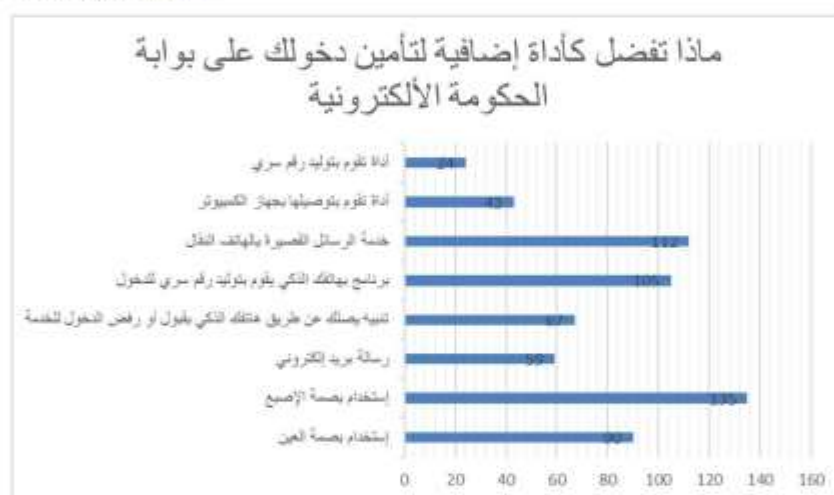
تلبية بملفك عن طريق: 67 (38.50%)

ملفك الذي يقول أو رفض الدخول للخدمة

رسالة بريد إلكتروني: 59 (33.90%)

استخدام بصمة الإصبع: 135 (77.58%)

استخدام بصمة العين: 90 (51.72%)

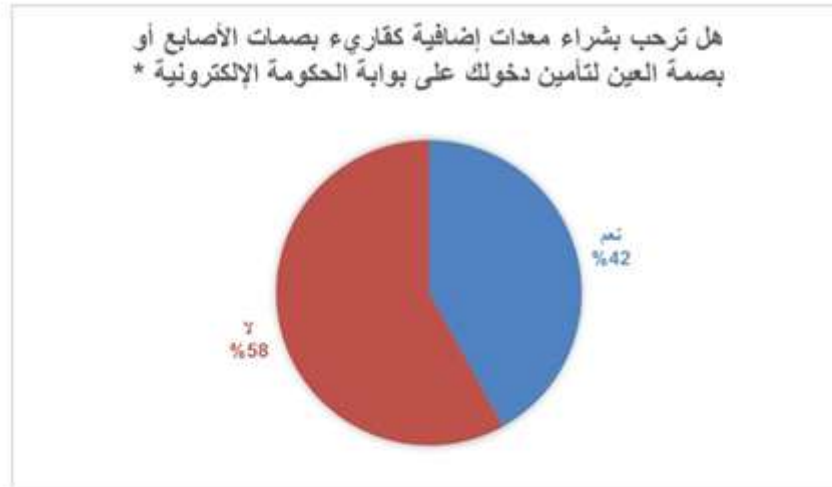


11. هل ترحب بشراء معدات إضافية كقارئ بصمات الأصابع أو بصمة العين لتأمين دخولك على بوابة الحكومة الإلكترونية * 11.

عدد المشاركين: 174

نعم: 73 (41.95%)

لا: 101 (58.04%)

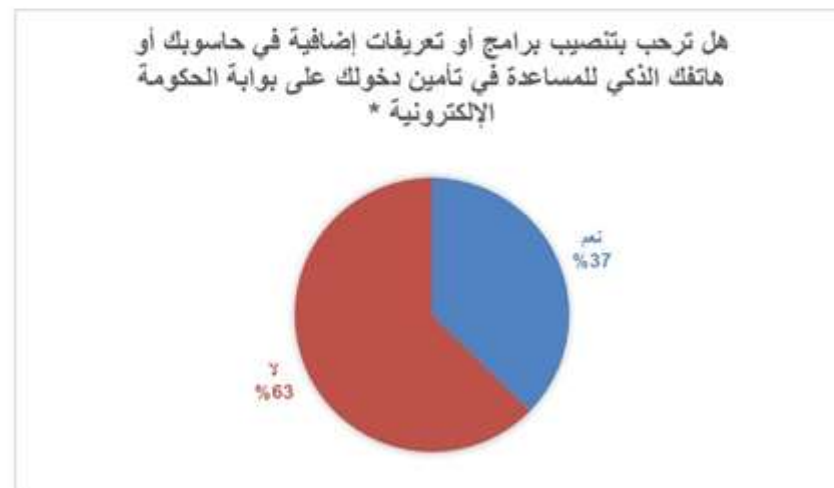


12. هل ترحب بتنصيب برامج أو تعريفات إضافية في حاسوبك أو هاتفك الذكي للمساعدة في تأمين دخولك على بوابة الحكومة الإلكترونية * 12.

عدد المشاركين: 174

نعم: 65 (37.36%)

لا: 109 (62.64.0%)



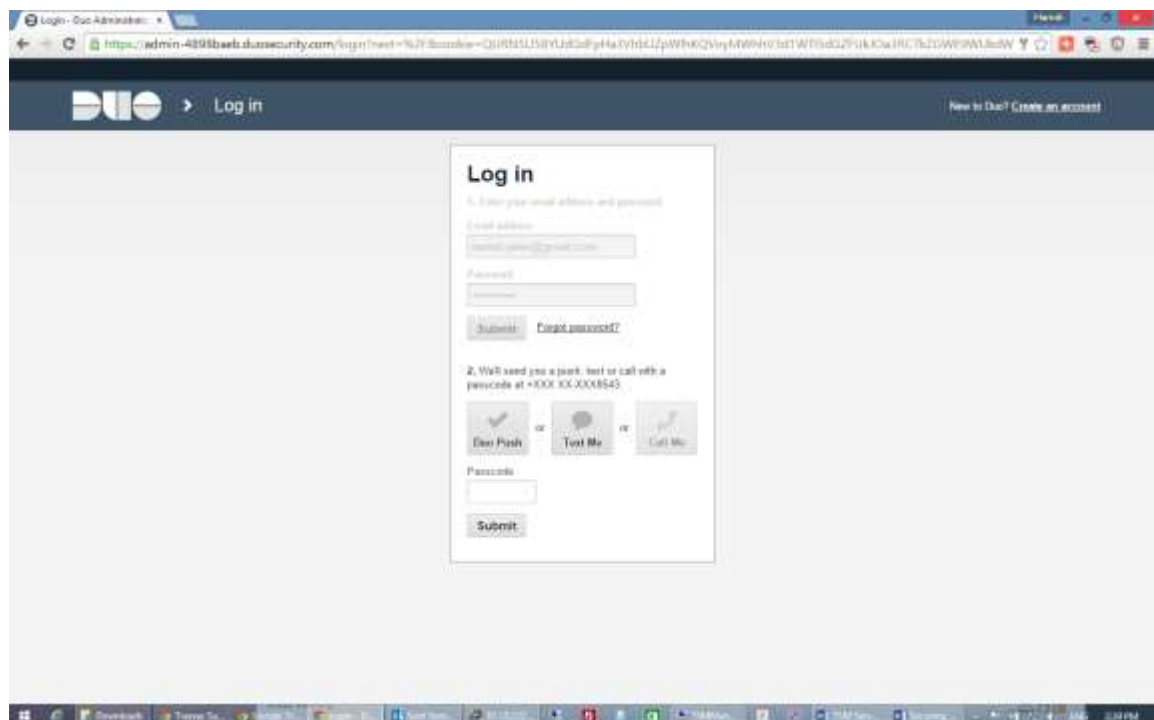
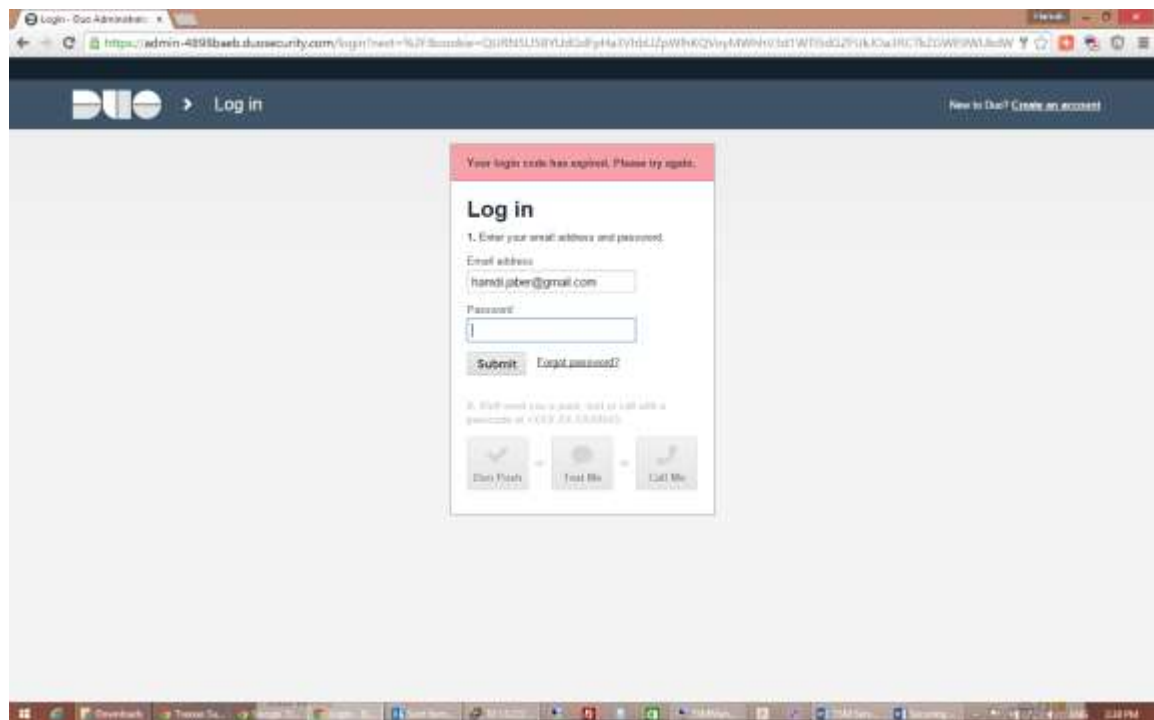
هل تستخدم هاتفك الذكي أو حاسوبك اللوحي للدخول إلى بوابة الحكومة الإلكترونية ؟ 13.

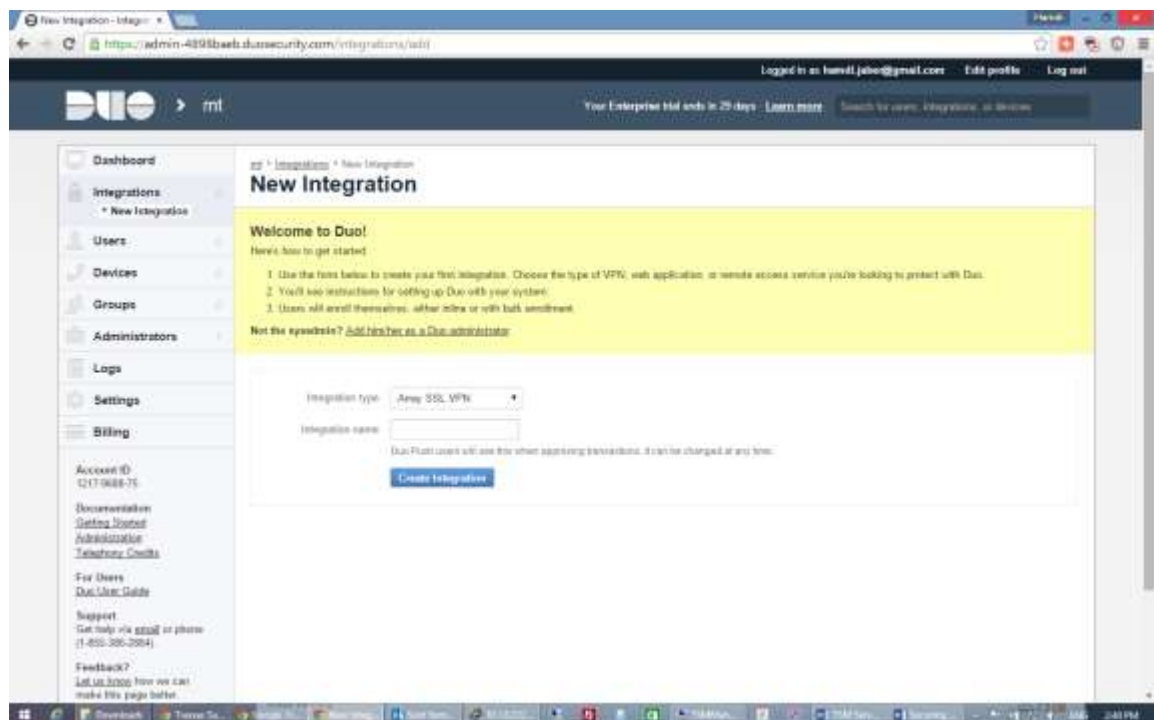
عدد المشاركين 174

نعم: 172 (98.85%)

لا: 2 (1.14%)

APPENDIX C Testing sample screen shots of SMS method (Lack of information in SMS is noticeable)





APPENDIX D Implementation source code

Index.php:

```
<?php
require_once dirname( __FILE__ ) . '/inc/db.inc.php';
session_start();
if (!isset($_SESSION['loggedin'])) {
header('Location: login.php');
exit();
}
?><!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">
<title><?php echo $htmlTitle;?></title>
<!-- Bootstrap core CSS -->
<link href="css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="css/starter-template.css" rel="stylesheet">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">
<div class="container">
<div class="navbar-header">
<button type="button" class="navbar-toggle collapsed" data-
toggle="collapse"
data-target="#navbar" aria-expanded="false" aria-controls="navbar">
<span class="sr-only">Toggle navigation</span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="navbar-brand" href="#"><?php echo $pageTitle;?></a>
</div>
<div id="navbar" class="collapse navbar-collapse">
<ul class="nav navbar-nav navbar-right">
<li class="active"><a href="logout.php">Logout</a></li>
</ul>
</div><!-- /.nav-collapse -->
</div>
</nav>
<div class="container">
<div class="starter-template">
<h1>E-government web portal.</h1>
<p class="lead">
You have successfully logged in to the E-government web portal.
</p>
</div>
<div class="row">
<hr>
<?php echo $pageFooter;?>
</div>
</div><!-- /.container -->
<!-- Bootstrap core JavaScript
===== -->
<!-- Placed at the end of the document so the pages load faster -->
```

```

<script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"
></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>

```

Code.php:

```

<?php
require_once dirname( __FILE__ ) . '/inc/db.inc.php';
require_once dirname( __FILE__ ) . '/inc/messages.inc.php';
require_once dirname( __FILE__ ) . '/inc/browser_detection.php';
require_once dirname( __FILE__ ) . '/inc/functions.php';
session_start();
$error = '';
$session_id = '';
$numbers = array();
$user = array();
if (isset($_SESSION['uid'])) {
    $sql = 'SELECT * FROM users WHERE id=:id';
    $sth = $dbh->prepare($sql);
    $sth->execute(array('id' => $_SESSION['uid']));
    if($row = $sth->fetch(PDO::FETCH_ASSOC)) {
        $user = $row;
        $session_id = $_SESSION['sessid'];
        $no1_digits = substr($row['number1'], -2, 2);
        $no2_digits = substr($row['number2'], -2, 2);
        $numbers[1] = '*****' . substr($row['number1'], -2, 2);
        $numbers[2] = '*****' . substr($row['number2'], -2, 2);
    }
} else {
    header('Location: login.php');
    exit();
}
//echo $_SESSION['code'];
if (isset($_POST['actCode'])) {
    $code = $_POST['code'];
    if ($code == $_SESSION['code']) {
        $_SESSION['otp_done'] = true;
        header('Location: image.php');
        exit();
    } else {
        $number = $user['number1'];
        $ua = getBrowser();
        $message = $messages['otp_wrong'];
        $message = str_replace('%SESSID%', $session_id, $message);
        $message = str_replace('%TIME%', date('h:i A'), $message);
        $message = str_replace('%BROWSER%', $ua['name'], $message);
        $message = str_replace('%OS%', $ua['platform'], $message);
        if ($user['Emails'] != '') {
            mail($user['Emails'], 'login error', $message);
        }
        sendSMS($number, $message);
        $error = 'Wrong code.';
    }
}
?><!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">

```

```

<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">
<title><?php echo $htmlTitle;?></title>
<!-- Bootstrap core CSS -->
<link href="css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="css/starter-template.css" rel="stylesheet">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">
<div class="container">
<div class="navbar-header">
<button type="button" class="navbar-toggle collapsed" data-
toggle="collapse"
data-target="#navbar" aria-expanded="false" aria-controls="navbar">
<span class="sr-only">Toggle navigation</span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="navbar-brand" href="#"><?php echo $pageTitle;?></a>
</div>
<div id="navbar" class="collapse navbar-collapse">
<ul class="nav navbar-nav navbar-right">
<li class="active"><a href="login.php">Login</a></li>
</ul>
</div><!--/.nav-collapse -->
</div>
</nav>
<div class="container">
<div class="starter-template">
<h1>E-government web portal.</h1>
<p class="lead">
Your login session ID: <?php echo $session_id;?>.<br>
Please enter the received six digits code.
</p>
</div>
<?php if ($error != ''){?>
<div class="alert alert-danger"><?php echo $error; ?></div>
<?php } ?>
<form class="form-horizontal" method="post" action="">
<div class="form-group">
<label for="code" class="col-sm-2 control-label">Code</label>
<div class="col-sm-5">
<input type="text" class="form-control" id="code" name="code"
maxlength="6">
</div>
</div>
<div class="form-group">
<div class="col-sm-offset-2 col-sm-10">
<input type="submit" class="btn btn-default" value="Continue"
name="actCode">
</div>
</div>
<div class="form-group">
<a href="javascript:void;">Login via another method</a>
</div>
</form>
<div class="row">

```

```

<hr>
<?php echo $pageFooter;?>
</div>
</div><!-- /.container -->
<!-- Bootstrap core JavaScript
===== -->
<!-- Placed at the end of the document so the pages load faster -->
<script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"
></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>

```

Otp.php:

```

<?php
require_once dirname( __FILE__ ) . '/inc/db.inc.php';
require_once dirname( __FILE__ ) . '/inc/messages.inc.php';
require_once dirname( __FILE__ ) . '/inc/browser_detection.php';
require_once dirname( __FILE__ ) . '/inc/functions.php';
session_start();
$error = '';
$session_id = '';
$numbers = array();
$user = array();
if (isset($_SESSION['uid'])) {
    $sql = 'SELECT * FROM users WHERE id=:id';
    $sth = $dbh->prepare($sql);
    $sth->execute(array(':id' => $_SESSION['uid']));
    if($row = $sth->fetch(PDO::FETCH_ASSOC)) {
        $user = $row;
        $session_id = $_SESSION['sessid'];
        $no1_digits = substr($row['number1'], -2, 2);
        $no2_digits = substr($row['number2'], -2, 2);
        $numbers[1] = '*****' . substr($row['number1'], -2, 2);
        $numbers[2] = '*****' . substr($row['number2'], -2, 2);
    }
} else {
    header('Location: login.php');
    exit();
}
if (isset($_POST['actOtp'])) {
    if (isset($_POST['number'])) {
        $number_key = filter_var($_POST['number'], FILTER_SANITIZE_NUMBER_INT);
        $field = 'number' . $number_key;
        if ($user) {
            $number = $user[$field];
            $ua = getBrowser();
            $code = rand('123456', '987654');
            $_SESSION['code'] = $code;
            $_SESSION['number'] = $number;
            //ToDo: send SMS to $number, and save it to session
            $message = $messages['otp'];
            $message = str_replace('%CODE%', $code, $message);
            $message = str_replace('%SESSID%', $session_id, $message);
            $message = str_replace('%TIME%', date('h:i A'), $message);
            $message = str_replace('%BROWSER%', $ua['name'], $message);
            $message = str_replace('%OS%', $ua['platform'], $message);
            if ($user['Emails'] != '') {
                mail($user['Emails'], 'verify login', $message);
            }
        }
    }
}

```

```

}
sendSMS($number, $message);
header('Location: code.php');
exit();
}
} else {
$error = 'Please select a number.';
}
}
?><!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">
<title><?php echo $htmlTitle;?></title>
<!-- Bootstrap core CSS -->
<link href="css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="css/starter-template.css" rel="stylesheet">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">
<div class="container">
<div class="navbar-header">
<button type="button" class="navbar-toggle collapsed" data-
toggle="collapse"
data-target="#navbar" aria-expanded="false" aria-controls="navbar">
<span class="sr-only">Toggle navigation</span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="navbar-brand" href="#"><?php echo $pageTitle;?></a>
</div>
<div id="navbar" class="collapse navbar-collapse">
<ul class="nav navbar-nav navbar-right">
<li class="active"><a href="login.php">Login</a></li>
</ul>
</div><!--/.nav-collapse -->
</div>
</nav>
<div class="container">
<div class="starter-template">
<h1>E-government web portal.</h1>
<p class="lead">
Your login session ID: <?php echo $session_id;?>.<br>
Choose the desired number to receive OTP.
</p>
</div>
<?php if ($error != ''){?>
<div class="alert alert-danger"><?php echo $error; ?></div>
<?php } ?>
<form class="form-horizontal" method="post" action="">
<?php
foreach ($numbers as $k => $v){
?>
<div class="radio">
<label>

```

```

<input type="radio" name="number" id="number<?php echo $k;?>"
value="<?php
echo $k;?>">
<?php echo $v;?>
</label>
</div>
<?php
}
?>
<div class="form-group">
<div class="col-sm-offset-2 col-sm-10">
<input type="submit" class="btn btn-default" value="Continue"
name="actOtp">
</div>
</div>
<div class="form-group">
<a href="javascript:void;">Login via another method</a>
</div>
</form>
<div class="row">
<hr>
<?php echo $pageFooter;?>
</div>
</div><!-- /.container -->
<!-- Bootstrap core JavaScript
===== -->
<!-- Placed at the end of the document so the pages load faster -->
<script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"
></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>

```

Image.php:

```

<?php
require_once dirname( __FILE__ ) . '/inc/db.inc.php';
require_once dirname( __FILE__ ) . '/inc/messages.inc.php';
require_once dirname( __FILE__ ) . '/inc/browser_detection.php';
require_once dirname( __FILE__ ) . '/inc/functions.php';
session_start();
if (!isset($_SESSION['otp_done'])) {
header('Location: login.php');
exit();
}
$session_id = '';
$user = array();
if (isset($_SESSION['uid'])) {
$sql = 'SELECT * FROM users WHERE id=:id';
$stmt = $dbh->prepare($sql);
$stmt->execute(array(':id' => $_SESSION['uid']));
if($row = $stmt->fetch(PDO::FETCH_ASSOC)) {
$user = $row;
$session_id = $_SESSION['sessid'];
}
} else {
header('Location: login.php');
exit();
}
if (isset($_GET['cat'])) {

```

```

if ($_GET['cat'] == $user['category']) {
    $number = $_SESSION['number'];
    $ua = getBrowser();
    $message = $messages['done'];
    $message = str_replace('%SESSID%', $session_id, $message);
    $message = str_replace('%TIME%', date('h:i A'), $message);
    $message = str_replace('%BROWSER%', $ua['name'], $message);
    $message = str_replace('%OS%', $ua['platform'], $message);
    if ($user['Emails'] != '') {
        mail($user['Emails'], 'success login', $message);
    }
    sendSMS($number, $message);
    $_SESSION['loggedin'] = true;
    header('Location: index.php');
    exit();
} else {
    $number = $user['number1'];
    $ua = getBrowser();
    $message = $messages['cat_wrong'];
    $message = str_replace('%SESSID%', $session_id, $message);
    $message = str_replace('%TIME%', date('h:i A'), $message);
    $message = str_replace('%BROWSER%', $ua['name'], $message);
    $message = str_replace('%OS%', $ua['platform'], $message);
    if ($user['Emails'] != '') {
        mail($user['Emails'], 'login error', $message);
    }
    sendSMS($number, $message);
    header('Location: login.php?error=cat');
    exit();
}
}
}
?><!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">
<title><?php echo $htmlTitle;?></title>
<!-- Bootstrap core CSS -->
<link href="css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="css/starter-template.css" rel="stylesheet">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">
<div class="container">
<div class="navbar-header">
<button type="button" class="navbar-toggle collapsed" data-
toggle="collapse"
data-target="#navbar" aria-expanded="false" aria-controls="navbar">
<span class="sr-only">Toggle navigation</span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="navbar-brand" href="#"><?php echo $pageTitle;?></a>
</div>
<div id="navbar" class="collapse navbar-collapse">
<ul class="nav navbar-nav navbar-right">

```

```

<li class="active"><a href="login.php">Login</a></li>
</ul>
</div><!--/.nav-collapse -->
</div>
</nav>
<div class="container">
<div class="starter-template">
<h1>E-government web portal.</h1>
<p class="lead">
Your login session ID: <?php echo $session_id;?>.<br>
Choose a picture from your account category.
</p>
</div>
<hr>
<?php if ($error != ''){?>
<div class="alert alert-danger"><?php echo $error; ?></div>
<?php } ?>
<div class="row">
<div class="col-xs-7 cat-images">
<?php
foreach ($cats as $cat) {
?>
<a href="image.php?cat=<?php echo $cat; ?>">

</a>
<?php
}
?>
</div>
</div>
<div class="row">
<hr>
<?php echo $pageFooter;?>
</div>
</div><!-- /.container -->
<!-- Bootstrap core JavaScript
===== -->
<!-- Placed at the end of the document so the pages load faster -->
<script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"
></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>

```

Login.php:

```

<?php
require_once dirname( __FILE__ ) . '/inc/db.inc.php';
require_once dirname( __FILE__ ) . '/inc/messages.inc.php';
require_once dirname( __FILE__ ) . '/inc/browser_detection.php';
require_once dirname( __FILE__ ) . '/inc/functions.php';
session_start();
$error = '';
$loginError = false;
if (isset($_GET['clear'])) {
unset($_SESSION['tries']);
}
if (isset($_GET['error']) && $_GET['error'] == 'cat') {
$_SESSION = array();
$error = 'Category did not match your account category.';
}

```

```

if (isset($_POST['actLogin'])) {
    $nid = $_POST['nid'];
    $password = $_POST['password'];
    $sql = 'SELECT * FROM users WHERE nid=:nid';
    $sth = $dbh->prepare($sql);
    $sth->execute(array(':nid' => $nid));
    if($row = $sth->fetch(PDO::FETCH_ASSOC)) {
        if ($password == $row['password']) {
            $_SESSION['uid'] = $row['id'];
            $_SESSION['sessid'] = rand(1234567, 9876543);
            header('Location: otp.php');
            exit();
        } else {
            $loginError = true;
            $number = $row['number1'];
            $ua = getBrowser();
            $message = $messages['password_wrong'];
            $message = str_replace('%TIME%', date('h:i A'), $message);
            $message = str_replace('%BROWSER%', $ua['name'], $message);
            $message = str_replace('%OS%', $ua['platform'], $message);
            if ($row['Emails'] != '') {
                mail($row['Emails'], 'login error', $message);
            }
            sendSMS($number, $message);
        }
    } else {
        $loginError = true;
    }
    if ($loginError) {
        $error = 'Wrong NID/Password!';
        $_SESSION['tries'] = isset($_SESSION['tries']) ? $_SESSION['tries'] + 1 : 1;
        if ($_SESSION['tries'] >= 3) {
            $error = 'Exceeded login tries. Your account will be locked for 5 minutes. (<a href="?clear">Request Clear</a>)';
        }
    }
}

?><!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">
<title><?php echo $htmlTitle;?></title>
<!-- Bootstrap core CSS -->
<link href="css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="css/starter-template.css" rel="stylesheet">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">
<div class="container">
<div class="navbar-header">
<button type="button" class="navbar-toggle collapsed" data-
toggle="collapse"
data-target="#navbar" aria-expanded="false" aria-controls="navbar">
<span class="sr-only">Toggle navigation</span>

```

```

<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="navbar-brand" href="#"><?php echo $pageTitle;?></a>
</div>
<div id="navbar" class="collapse navbar-collapse">
<ul class="nav navbar-nav navbar-right">
<li class="active"><a href="login.php">Login</a></li>
</ul>
</div><!--/.nav-collapse -->
</div>
</nav>
<div class="container">
<div class="starter-template">
<h1>E-government web portal.</h1>
<p class="lead">Use your e-government account to log in.</p>
</div>
<?php if ($error != ''){?>
<div class="alert alert-danger"><?php echo $error; ?></div>
<?php } ?>
<form class="form-horizontal" method="post" action="login.php">
<div class="form-group">
<label for="nid" class="col-sm-2 control-label">National Id</label>
<div class="col-sm-5">
<input type="text" class="form-control" id="nid" name="nid" required>
</div>
</div>
<div class="form-group">
<label for="inputPassword3" class="col-sm-2 control-label">Password</label>
<div class="col-sm-5">
<input type="password" class="form-control" id="inputPassword3"
name="password"
</div>
</div>
<div class="form-group">
<div class="col-sm-offset-2 col-sm-10">
<input type="submit" class="btn btn-default" value="Continue"
name="actLogin">
</div>
</div>
<div class="form-group">
<a href="javascript:void;">Forgot your password?</a>
</div>
</form>
<div class="row">
<hr>
<?php echo $pageFooter;?>
</div>
</div><!-- /.container -->
<!-- Bootstrap core JavaScript
===== -->
<!-- Placed at the end of the document so the pages load faster -->
<script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"
></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>

```

Logout.php:

```
<?php
session_start();
$_SESSION = array();
session_destroy();
header('Location: login.php');
exit();
```

Functions.php:

```
<?php
function sendSMS($number, $message) {
include __DIR__ . '/../classes/GatewayFactory.php';
include __DIR__ . '/../classes/Gateway_RouteSMS.php';
$gatewayOption = 'RouteSMS';
$gateway = \MassSMS\GatewayFactory::build($gatewayOption,
'121.241.242.114', '8080', 'libs-ashgal', '3e^ui!TV');
$parms = array();
$parms['delivery'] = true;
$parms['type'] = 0;
$parms['destination'] = $number;
$parms['source'] = '%gateway%';
$parms['message'] = $message;
$results = $gateway->send_sms($parms);
error_log(print_r($results, true), 3, __DIR__ . '/sms.log');
}
```

Messages.inc.php:

```
<?php
$messages['password_wrong'] = <<<MSG
Wrong password entered for your e-government web portal account login
Time %TIME%
Near %location%
%BROWSER% browser on %OS%
MSG;
$messages['otp'] = <<<MSG
Use this access code: %CODE%
To login to your e-government web portal account
session ID: %SESSID%
Time %TIME%
Near %location%
%BROWSER% browser on %OS%
MSG;
$messages['otp_wrong'] = <<<MSG
Wrong access code entered for your e-government web portal account
login
session ID: %SESSID%
Time %TIME%
Near %location%
%BROWSER% browser on %OS%
MSG;
$messages['cat_wrong'] = <<<MSG
Wrong Category entered for your e-government web portal account login
session ID: %SESSID%
Time %TIME%
Near %location%
%BROWSER% browser on %OS%
MSG;
$messages['done'] = <<<MSG
Login attempt done on your e-government web portal account
```

```
session ID: %SESSIONID%
Time %TIME%
Near %location%
%BROWSER% browser on %OS%
Status: succeeded
MSG;
```

DB.inc.php:

```
<?php
if ($_SERVER['HTTP_HOST'] == 'localhost') {
define('DB_HOST', 'localhost');
define('DB_NAME', 'private_tfadissertation');
define('DB_USER', 'root');
define('DB_PASS', '123456');
} else {
define('DB_HOST', 'localhost');
define('DB_NAME', 'hajmscde_sitedb');
define('DB_USER', 'hajmscde_siteusr');
define('DB_PASS', 'd)dM$uGJny#');
}
$dbh=null;
try{
$dbh = new PDO('mysql:host='.DB_HOST.';dbname='.DB_NAME, DB_USER,
DB_PASS);
//Enable Error Reporting for PDO
//ToDo: remove when done
$dbh->setAttribute( PDO::ATTR_ERRMODE, PDO::ERRMODE_WARNING
);//PDO::ERRMODE_EXCEPTION/ERRMODE_WARNING
$dbh->exec('SET CHARACTER SET utf8'); //Confirm UTF8 charset
} catch(PDOException $e) {
trigger_error('Error: '.$e->getMessage());
}
$debug_Email = 'devcontact@Email.ly';
$cats = array('animals', 'desert', 'flowers', 'furniture', 'tourism',
'cars', 'electronics',
'food', 'money', 'clothes', 'medicine', 'legal');
$htmlTitle = 'Secure e-government';
$pageTitle = 'Securing E-government web portal access with Two-factor
authentication - Ms.c.
dissertation implementation';
$pageFooter = '&copy; 2015 - Ms.c. Dissertation - Hamdi A. Jaber - The
Libyan Academy';
```

Browser detection.php:

```
<?php
function getBrowser()
{
$u_agent = $_SERVER['HTTP_USER_AGENT'];
$bname = 'Unknown';
$platform = 'Unknown';
$version= "";
//First get the platform?
if (preg_match('/linux/i', $u_agent)) {
$platform = 'linux';
}
elseif (preg_match('/macintosh|mac os x/i', $u_agent)) {
$platform = 'mac';
}
elseif (preg_match('/windows|win32/i', $u_agent)) {
```

```

$platform = 'windows';
}
// Next get the name of the useragent yes seperately and for good
reason
if(preg_match('/MSIE/i',$u_agent) && !preg_match('/Opera/i',$u_agent))
{
$name = 'Internet Explorer';
$sub = "MSIE";
}
elseif(preg_match('/Firefox/i',$u_agent))
{
$name = 'Mozilla Firefox';
$sub = "Firefox";
}
elseif(preg_match('/Chrome/i',$u_agent))
{
$name = 'Google Chrome';
$sub = "Chrome";
}
elseif(preg_match('/Safari/i',$u_agent))
{
$name = 'Apple Safari';
$sub = "Safari";
}
elseif(preg_match('/Opera/i',$u_agent))
{
$name = 'Opera';
$sub = "Opera";
}
elseif(preg_match('/Netscape/i',$u_agent))
{
$name = 'Netscape';
$sub = "Netscape";
}
// finally get the correct version number
$known = array('Version', $sub, 'other');
$pattern = '#(?:<browser>' . join('|', $known) .
')[/ ]+(?:<version>[0-9.|a-zA-Z.]*)#';
if (!preg_match_all($pattern, $u_agent, $matches)) {
// we have no matching number just continue
}
// see how many we have
$i = count($matches['browser']);
if ($i != 1) {
//we will have two since we are not using 'other' argument yet
//see if version is before or after the name
if (stripos($u_agent, "Version") < stripos($u_agent, $sub)) {
$version= $matches['version'][0];
}
else {
$version= $matches['version'][1];
}
}
else {
$version= $matches['version'][0];
}
// check if we have a number
if ($version==null || $version=="") {$version="?";}
return array(
'userAgent' => $u_agent,
'name' => $name,

```

```

'version' => $version,
'platform' => $platform,
'pattern' => $pattern
);
}

```

Gateway RouteSMS.php:

```

<?php
namespace MassSMS;
class Gateway_RouteSMS {
private $server;
private $port;
private $username;
private $password;
public function __construct($server, $port, $username, $password){
$this->server = $server;
$this->port = $port;
$this->username = $username;
$this->password = $password;
}
public function send_sms($params){
//Delivery Report
$delivery = '0';
if(isset($params['delivery']) && $params['delivery']){
$delivery = '1';
}
//Message Type
$message_type = '2';//Unicode
if (isset($params['type'])) {
}
//Destination: multiple numbers separated by url-encoded commas
if(is_array($params['destination'])){
$params['destination'] = implode( urlencode( ',' ),
$params['destination']);
}
//Message: Unicode
$params["message"] = $this->_smpp_unicode($params["message"]);
//2do: for english messages
$url = 'http://'.$this->server.':'.$this->port.'/bulksms/bulksms?';
$url .= 'username='.$this->username;
$url .= '&password='.$this->password;
$url .= '&type='.$message_type;
$url .= '&dlr='.$delivery;
$url .= '&destination='.$params['destination'];
$url .= '&source='.$params['source'];
$url .= '&message='.$params['message'];
//echo "$url<br>";
//$url="http://smpp2.routesms.com:8000/bulksms/bulksms?username="
.urlencode($params["username"]). "&password="
.urlencode($params["password"]).
"&type=".$msgtype."&dlr=1&destination=".urlencode($params["to"])."&sour
ce="
.urlencode($params["senderid"]). "&message=".$params["message"];
$data = $this->_get($url);
$sms_id = 0;
//2do: check for multiple numbers
if(isset($data['response'])){
#1701|<CELL_NO>:<MESSAGE ID>,etc,etc
$response = @explode( '|', $data["response"]);
//echo '<pre>'.print_r($response,true).'

```

```

if( $response[0] == '1701'){//Success
$sms_id = $response[2];
return array('success'=>true, 'sms_id'=>$sms_id);
} else {
return array('error'=>$data['response']);
}
} else {
return array('error'=>'No response!');
}
}

public function get_balance(){
$cookie_file = 'temp_'.md5(microtime());
$pg = 'http://'.$this->server.'/websms/login.php?name=libyanspidersms';
//http://121.241.242.114/websms/libyanspidersms
$useragent="Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1)
Gecko/20061204
Firefox/2.0.0.1";
$ch = curl_init();//Read Session
$cookiearr = array();
curl_setopt($ch, CURLOPT_URL, $pg);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_COOKIEJAR, $cookie_file);
curl_setopt($ch, CURLOPT_COOKIEFILE, $cookie_file);
$cd=curl_exec($ch);
curl_close($ch);
preg_match_all('|Set-Cookie: (.*)|U', $cd, $results);
$cookies = implode(';', $results[1]);
//print_r($cookies);
$postfields = array();
$postfields['txtUsername']=$this->username;//;
$postfields['txtPassword']=$this->password;//;
$postfields['txtResName']='libyanspidersms';
$postfields['txtResId'] = '42049';
$postfields['txtDistId'] = '-1';
$postfields['txtPageName']="login.psms";
$postfields['btnSubmit']='Login';
$ch = curl_init();//Login
$pg = "http://".$this->server."/RSmsPlus/websms/AjaxPage.php";
curl_setopt($ch, CURLOPT_URL, "http://".$this->
server."/RSmsPlus/websms/AjaxPage.php");
curl_setopt($ch, CURLOPT_COOKIEJAR, $cookie_file);
curl_setopt($ch, CURLOPT_COOKIEFILE, $cookie_file);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_REFERER, $pg);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_TIMEOUT, 100);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, $postfields);
$data=curl_exec($ch);
curl_close($ch);
$ch = curl_init(); //Read Balance
///websms/creditHistory.psms
//http://121.241.242.114/RSmsPlus/websms/creditHistory.psms
curl_setopt($ch, CURLOPT_URL,
"http://".$this->server."/RSmsPlus/websms/creditHistory.psms");
curl_setopt($ch, CURLOPT_REFERER, $pg);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_TIMEOUT, 100);

```

```

curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_COOKIEJAR, $cookie_file);
curl_setopt($ch, CURLOPT_COOKIEFILE, $cookie_file);
$data=curl_exec($ch);
curl_close($ch);
//echo htmlentities($data);
//print_r($data);
//Extract balance info
$results = array('error'=>'', 'credit'=>-1);
if(strpos($data, 'CreditUsed')!==false) {
$tmp1 = explode('CreditUsed', $data);
$tmp2 = explode('</table>', $tmp1[1]);
//echo $tmp2[0];
preg_match_all('/Credit Balance\:(.*) ([0-9.]+)/si', $tmp2[0],
$matches);
//print_r($matches);
if(!empty($matches)) {
$results['credit'] = $matches[2][0];
} else {
$results['error'] = 'Could not pull balance value!';
}
$values = array();
if ($results['error'] == '') {
$values["credits"] = $results['credit'];
} else {
$values["error"] = $results['error'];
$values["credits"] = -1;
}
} else {
$values = array('error'=>'Could not pull balance value!', 'credits'=>-1);
}
//print_r($matches);
//return $results;
//$rtval = smpp_lsReadBalance($params["username"],
$params["password"]);
unlink($cookie_file);
//print_r($values);
return $values;
}
private function _get($url) {
$ch = curl_init($url);
curl_setopt($ch, CURLOPT_TIMEOUT, 100);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$data=curl_exec($ch);
curl_close($ch);
$results['response'] = $data;
return $results;
}
private function _smpp_unicode($message) {
$hex1 = '';
if (function_exists('iconv')) {
$latin = @iconv('UTF-8', 'ISO-8859-1', $message);
if (strcmp($latin, $message)) {
$arr = unpack('H*hex', @iconv('UTF-8', 'UCS-2BE', $message));
$hex1 = strtoupper($arr['hex']);
}
}
if ($hex1 == '') {
$hex2 = '';
$hex = '';
}

```

```

for ($i = 0; $i < strlen($message); $i++) {
    $hex = dechex(ord($message[$i]));
    $len = strlen($hex);
    $add = 4 - $len;
    if ($len < 4) {
        for ($j = 0; $j < $add; $j++) {
            $hex = "0" . $hex;
        }
    }
    $hex2 .= $hex;
}
return $hex2;
} else {
return $hex1;
}
} else {
//print 'iconv Function Not Exists !';
}
}
}

```