



THE VERIFICATION FROM THE CITIZEN IN E-GOVERNMENT APPLICATIONS

BY

YASIR RASHEED ALI JASIM

A THESIS

**SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR MASTER DEGREE
IN
COMPUTER INFORMATION SYSTEM**

SUPERVISOR

Dr. HAZIM FARHAN

**DEPARTMENT OF COMPUTER INFORMATION
SYSTEM
FACULTY OF INFORMATION TECHNOLOGY**

MIDDLE EAST UNIVERSITY

**AMMAN-JORDAN
August, 2010**

AUTHORIZATION FORM

إقرار تفويض


أنا ياسر رشيد عالي جاسم أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي
للمكتبات أو المؤسسات أو الهيئات أو الأشخاص عند طلبها.

التوقيع: 

التاريخ: ٢٠١٠ / ٨ / ١٥

Authorization statement

I, Yasir Rasheed Ali Jasim, Authorize the Middle East University to supply
copies of my Thesis to libraries, establishments or individuals upon their
request.

Signature: 

Date: 15-8-2010

Middle East University


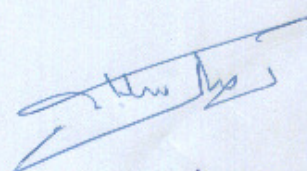
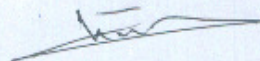
Examination Committee Decision

This is to certify that the thesis entitled "The Verification from the Citizen in E-government Applications" was successfully defended and approved on August 2th 2010.

Examination Committee Members

Signature

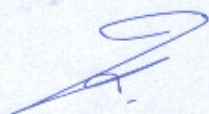
- 1- Dr. Hazim A. Farhan
Assistant Professor, Department of Computer
Information Systems, Faculty of Information Systems
& Technology (Middle East University)
- 2- Prof. Nidal F. Shilbayeh
Professor, Department of Computer Science,
Faculty of Information Systems & Technology
(Middle East University)
- 3- Dr. Rashid Al-Zubaidy
Assistant Professor, Department of Computer Science,
Faculty of Information Technology
(Philadelphia University)



DECLARATION

I do hereby declare the present research work has been carried out by me under the supervision of Dr. Hazim Farhan and this work has not been submitted elsewhere for any other degree, fellowship or any other similar title.

Signature:



Date:

15-8-2010

Yasir Rasheed Ali Jasim
Department of Computer Information System
Faculty of Information Technology
Middle East University

LIST OF FIGURES.....	IX
ABSTRACT.....	XI
ABSTRACT IN ARABIC.....	XII
CHAPTER 1: INTRODUCTION.....	1
1.1 Overview.....	2
1.2 E-government definitions and the service scenario.....	4
1.3 E-government and Security Importance	6
1.4 E-mail Systems and Threats	11
1.5 Problem Statement.....	16
1.6 Thesis Objective.....	17
1.7 Thesis Scope.....	18
1.8 Thesis Motivations.....	18
1.9 Thesis Limitations.....	19
1.10 Thesis Organization.....	19
CHAPTER 2: E-GOVERNMENT APPLICATIONS AND RELATED WORKS.....	21
2.1 Scope of E-government Applications.....	22
2.2 Functions of E-government Applications.....	24
2.3 Related Work.....	26
CHAPTER 3: SYSTEM ANALYSIS.....	37
3.1 Overview.....	38
3.2 Current System Scenarios.....	39
3.3 Security Importance.....	41
3.4 Phishing Scenarios.....	42
3.5 Phishers Events.....	43
3.6 The Problem Analysis.....	44
CHAPTER 4: DESIGNING THE PROPOSED SOLUTION.....	52

4.1 Overview.....	53
4.2 Designing the Proposed Solution.....	54
4.2.1 The Flowchart of the Proposed Design.....	63
4.2.2 Use Case Diagram of the Proposed System.....	64
4.3 New System Analysis.....	65
 CHAPTER 5: CONCLUSIONS AND FUTURE WORK.....	67
5.1 Conclusions.....	68
5.2 Future Work.....	69
 APPENDIX.....	70
APPENDIX A: An example of system proposed.....	71
APPENDIX B: Comparison of the Proposed Approach with the related works.....	75
 REFERENCES.....	76

LIST OF FIGURES

Figure 1.1 E-government Architecture.....	6
Figure 1.2 Phishers Attack Percentages around the World.....	15
Figure 2.1 Sender Verification	34
Figure 2.2 Sender Verification	34
Figure 3.1 The Structure of the Current System	39
Figure 3.2 Citizen Login E-government Site.....	39
Figure 3.3 A Citizen's Registration into the E-Government Database.....	40
Figure 3.4 Application Request.....	40
Figure 3.5 Citizen's Registration Form.....	41
Figure 3.6 Send E-mail Form	41
Figure 3.7 Fabrication.....	43
Figure 3.8 E-government Is Not Responsible for Other Websites.....	45
Figure 3.9 E-mail address	46
Figure 3.10 Shown Same Senders, Same Subject and Different Date.....	46
Figure 3.11 True Message of the Sender.....	47
Figure 3.12 True Attached File of the Sender.....	48
Figure 3.13 The Phisher's Message.....	49
Figure 3.14 The Phisher's Attached File.....	49
Figure 3.15 Processes Creating an E-mail for Phisher.....	50
Figure 3.16 The Success of the Process Creating an E-mail for Phisher.....	50
Figure 4.1 The Structure of the Proposed Design.....	54

Figure 4.2 Citizen Registration	55
Figure 4.3 Registration System	55
Figure 4.4 Addresses (A).....	57
Figure 4.5 Addresses (B).....	57
Figure 4.6 "One-To-Many" Matching	58
Figure 4.7 Citizen Sent Message from Any Website.....	58
Figure 4.8 Possible and Impossible Redundancy	59
Figure 4.9 Linking the E-mail Address.....	60
Figure 4.10 Updating the E-mail Addresses.....	60
Figure 4.11 Verification Process.....	61
Figure 4.12 Valid Users.....	62
Figure 4.13 Flowchart Diagram for the Proposed Design.....	63
Figure 4.14 Use Case Diagram for the Proposed Design	64

Abstract

The Verification from the Citizen in E-government Applications

By

Yasir Rasheed Ali Jasim

Faculty of Information Technology

Middle East University

Supervisor

Dr. Hazim Farhan

E-government is an electronic community in which the services provided by governmental organizations are provided electronically to the citizens and uses the internet as an infrastructure for its work. E-government may suffer Security problems and possible attacks such as: Hackers, phishers, malicious software, denial of services, attacks from insiders, and deceptions by the attacker. In addition to this, there are some accidental damages such as: inexpert users, insufficient administrators, hardware and software failure, and accidental disasters.

One of the most important problems facing E-government is the security of E-mail to the citizen. The security of the information is sensitive and very important to keep secret the most important things in E-government. A computer network has opened many doors for those who have bad intentions and the most prominent are the phishers, which are loaded with deceptive messages links to the sites of intended fraud on the recipient of the message in addition to viruses.

This thesis focuses on the security of E-mail. The proposed solution is trying to design a way to protect E-mail from phishers, spam and all the unwanted messages through design of verification process from the owner of the E-mail (Citizen), in case the citizen decided to gets advantages from E-government services by sending messages from the owner of E-mail addresses, without logging into E-government every time on. The reason for this proposal is that most of the operations will be implemented through the E-mail, as well as, its availability for the citizens.

ملخص

التحقق من المواطن في تطبيقات الحكومة الإلكترونية

إعداد

ياسر رشيد عالي جاسم

كلية تقنية المعلومات

جامعة الشرق الأوسط

إشراف

الدكتور حازم فرحان

الحكومة الإلكترونية هي مجتمع إلكتروني حيث يتم فيه تزويد خدمات الهيئات الحكومية إلى المواطنين إلكترونياً وهي تستعمل الإنترنت كبناء تحتي لعملها. الحكومة الإلكترونية قد تعاني من مشاكل الأمن والهجمات المحتملة مثل: لصوص الكمبيوتر، الصائدون، برامج خبيثة، نكران الخدمات، هجوم من الدخلاء، ومكر من قبل المهاجم. بالإضافة إلى هذا، هنالك بعض الأضرار العرضية مثل: المستعملون العديموا الخبرة، مدراء غير كفونين، فشل البرامج والأجهزة، وكوارث عرضية.

إحدى أهم هذه المشاكل التي تواجه الحكومة الإلكترونية هو أمن البريد الإلكتروني للمواطن. إن أمن المعلومات هو حساس وهام جداً لإبقاء سرية الأشياء الأكثر أهمية في الحكومة الإلكترونية. أن شبكة الحاسوب فتحت العديد من الأبواب لأولئك الذين لهم نوايا سيئة ومن أهمهم هم الصائدون، والتي تكون رسائلهم المخادعة محملة بروابط تؤدي الى مواقع الهدف منها الغش والاحتيال على مستلم الرسالة بالإضافة الى الفيروسات.

هذه الأطروحة تركز على أمن البريد الإلكتروني. الحل المقترح يحاول تصميم طريقة لحماية البريد الإلكتروني من الصاندين ورسالة الدعاية وكل الرسائل الغير مرغوب بها عن طريق تصميم عملية تحقق من مالك البريد الإلكتروني (المواطن) في حالة ان المواطن قرر الاستفادة من خدمات الحكومة الإلكترونية عن طريق ارسال رسالة من بريده الإلكتروني الخاص به ومن دون الحاجة للاتصال بالحكومة الإلكترونية من خلال الارتباط بها من حين الى آخر. إن السبب لهذا الاقتراح لأن أغلب العمليات ستطبق من خلال البريد الإلكتروني، بالإضافة إلى توفره للمواطنين.

Chapter 1

Introduction

CHAPTER 1

INTRODUCTION

1.1 Overview

Most states take great strides towards implementing an E-government. The purpose of developing the quality of human life has prompted states to build infrastructure for communications and electronic applications. This infrastructure would be the norm and the basis for the application of a comprehensive E-government. The role of the workmanship in the development of new computing applications is to make life easy and meaningful to the user through an access of a rapid and accurate update and retrieval of information required. The waves of an E-government are rising through public organizations and public administration across the world. More and more governments are using information and communication technology, especially the internet or web-based networks, in order to provide services between government agencies and citizens, businesses, employees and other nongovernmental agencies.

Understanding the concept of the E-government system is to provide access anywhere, any time that government services via the open communications. An E-government is composed of several components including the infrastructure for Internet communication, many of the various websites, browsers, beneficiary, products, services, databases, security and fire-walls, electronic payments and many other components.

As previously inferred from the importance of E-governments in our lives, we find that to provide the security and integrity is extremely important.

Or else, all what we have built would be blown by the wind. Today our records and our knowledge are both open to the world; therefore, the lack of conservation and without providing a good security would drag us back to earlier times and the use of traditional methods in the maintenance of our knowledge. This fact spotlights the importance of security in our lives, our business and our government. The development of electronic and new ways to make our information open is imperative. We provide honest ways to keep the development going on, but this development is not sufficient from the standpoint of security and privacy that would prove authenticity and data integrity that must be preserved. And contrary to the principles of this new trend in making systems easy to use in providing information and answering questions. The problem of security is a major problem and must be taken into consideration at a high level of politics. The security solution must be planned for this problem to be unified for all applications.

Taking into consideration the different levels of authority, this starts from the normal user's access to the user a high level of security. It is well known that any protection system is a counter to one or more of the threats. There are many threats in the application of E-government and the beginning of the intruders (Hackers, Crackers, Disguised, etc.), physical threats, threats of communications, and so on. It is impossible that there should be one system for the protection of all

previous threats, but at least we must solve one of the most important threats which is “Phishing”.

1.2 E-government definitions and the service scenario

What was indicated in the E-government initiatives are complex change efforts intended to use new and emerging technologies to support a transformation in the operation and effectiveness of government derived from government reinvention (Theresa 2002). According to a definition in this context, E-government means the realization of mutual duties and obligations and relations between the state and the individual in modern societies online and in a secure context (Arifoglu et al. 2002). In a similar fashion, the concept of "E-government" indicates a "better government structure", which is more advanced than the traditional government model and based on a stronger Information Technology (IT) background and implications (The E-government Imperative 2003). In another definition an E- government is defined as a government model which utilizes information technology in exchange of information, services and goods between citizens and commercial institutions in order to increase performance and efficiency (Turkiye 2002). In state of Texas's electronic government strategic plan (State of Texas 2001) Electronic government is defined as: government activities that take place over electronic communications among all levels of government, citizens, and the business community, including: acquiring and providing products and services; placing and receiving orders; providing and obtaining information; and completing financial transactions. Broadly defined by (Jim 2001):

"E-government is the continuous optimization of service delivery, constituency participation and governance by transforming internal and external relationships through technology, the Internet and new media.

As what Zhiyuan defined, E-government is a way for governments to prove their abilities and development by using the most innovative information and communication technologies, particularly web-based internet applications, to provide citizens and businesses with more convenient access to government information and services, to improve the quality of the services and to provide greater opportunities to participate in democratic institutions and processes; where it was included here to the transactions between government and business, government and citizen, government and employee, and among different units and levels of government. E-business and E-commerce are subsets of E-government (Zhiyuan 2002).

The scenario of service in the application of E-government is that the customer goes to a web service ministry and looks for a product / service that are the focus of attention. It is clear that after that examination of the customer service, web ministry and the identification of products or services, the necessary next step is to get the power to pass through security precautions. Figure 1.1 shows the architecture of the E-government.

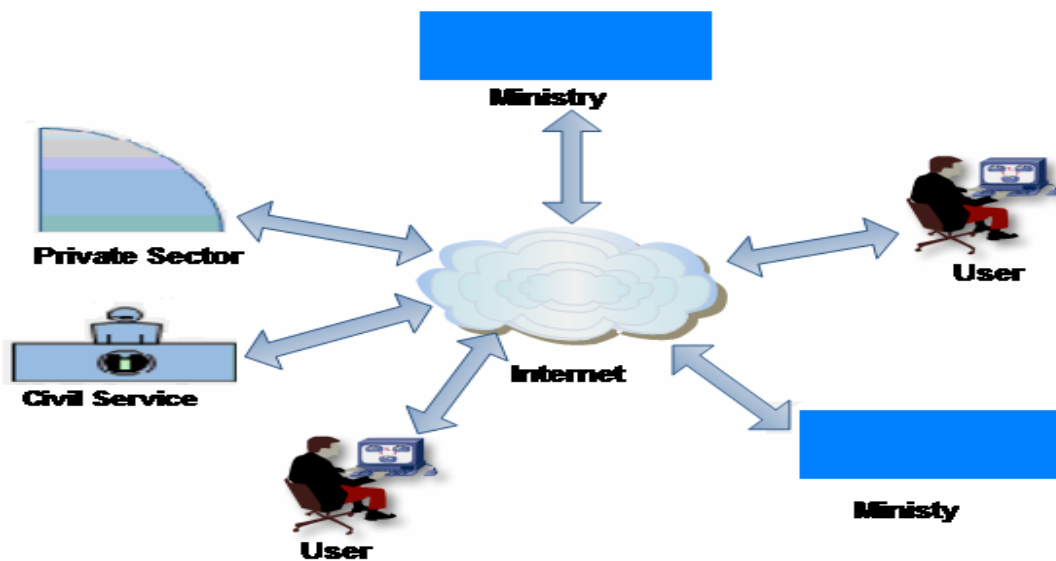


Figure 1.1 E-government Architecture

1.3 E-government and Security Importance

More and more people began looking for electronic means to transmit information. The value of electronic E-mail and messaging is more than important in our lives and many government agencies have to go for weeks without regular postal mail (Betsy 2010).

Government agencies began encouraging people to consider using electronic means to complete filings, comment on proposed rules, submit consumer complaints, ask questions, and much more. This push began over the past few years and has been magnified due to most of the operations of E-government implemented through the E-mail. E-mail has become an increasingly common tool for communication over the past decade. In the beginning, it was viewed as a very informal means of communication. Typically, individuals used it for their personal needs rather than for business use. As the Internet grew in the

1990s, so did the legitimacy of the Internet and E-mail communication. E-business, E-commerce, and E-government have emerged. E-mail has become one of the primary forms of communication for individuals everywhere.

Within this framework, we will deal with topics such as E-government, personal data processing in telecommunications and, in particular, relatively recent phenomena such as "spam".

In this context, the guarantees, inherent in the fundamental right to personal data protection in the use of the new technologies, acquire enormous relevance and make it essential that we find alternatives which prevent violations of this right, given the myriad of ways in which the public's data may now be used.

One of the most complete definitions that cover all the aspects of e-government identifies it as: "The use of information and communications technologies (ICT) by government bodies to improve the services and information provided to citizens, to upgrade the efficiency and effectiveness of public management and to substantially increase transparency in the public sector and citizen participation".

Moreover, these areas - better citizens' services, good government and the expansion of democracy - all involve regulatory, organizational and technological components. Thus, the integration of ICT's must follow a strategic plan that

envisages the legal and technological aspects from an interdisciplinary perspective and seeks to facilitate such integration and promote an environment of security.

Technological evolution has greatly expanded the possibility of sending unsolicited bulk commercial communications through automatic E-mail messages. Certain of these, such as the dispatch of unsolicited commercial E-mail messages ("spam") have reached disturbing proportions, given their massive scope. "Spam" is a problem for individuals as, in addition to violating their privacy, it may lead to error or deception, or even represent outright fraud. It also implies spending time and money in the purchase of filtering or other types of programmers.

Moreover, it also involves considerable expense for companies, both directly (lower performance and productivity of employees and the investment of time and money in solving the problems) and indirectly (false positives, spreading of viruses). For Internet service providers (ISP) and e-mail service providers (ESP), it may entail the need to acquire a broader band and greater storage capacity. At the same time, "spam" is a low-cost, highly profitable activity, particularly in cases involving fraud ("phishing" and others).

Finally, "spam" has reached global proportions and requires responses at an international level. Therefore, "spam" can seriously undermine user trust, an essential factor in the progress of e-commerce in the whole of the information society. A wide range of regulatory, technical and awareness measures, in

addition to an international cooperation, are all necessary to combat to this phenomenon.

The technical solutions addressed at putting an end to "spam" should include blocking messages from servers identified as "spam" sources, user implementation of filtering programs in their own terminals, and E-mail service providers' implementation of the same in their own servers.

In this regard, it is particularly important to pay special attention to servers that operate in open mode and open "proxy", that may be used to retransmit messages that are sent by the "spammers". These servers must be obligated to adopt the security measures necessary to prevent any such retransmission. However, filtering techniques may block important e-mails (false positives) or may not block "spam" (false negatives), causing problems that may lead to litigation. Thus, the conditions set out in customer contracts must be adapted so that the ISP/ESP's and mobile service providers can offer their customers filtering options and include clauses that prohibit sending unsolicited E-mail.

Different methods are used in designing the protection of information from one source to another, where some of the overfilling took to the complexity of the design protection systems, so that the cost and effort to access the information for authorized persons is higher than the value of the information itself.

To design a security system, we have to adopt standard specifications as proposed by (Alaa 1999) and follow the following principles:

1. A perfect security does not exist; while some people build security, other people destroy it.
2. The cost of access to information for non-authorized persons is higher than the value of the information itself.
3. The cost of the security system design and complexity must be balanced with the value of the information protected. The more the value of the information security system is, the more complex the system becomes and vice versa.
4. The security system must be able to protect itself against hackers and there should also be different levels. Even if one of these levels was not down the entire system should not be down as well, but rather only one part and the remainder of the parts work efficiently.
5. Know your enemy: Interlopers in the computer systems have developed the ability and expertise to penetrate these systems. Therefore, protection systems must be built and based on modern techniques designed to face this great challenge.

Because weakness is complex and the threats are varied and unexpected; it is not possible to protect everything from all types of threats. We must therefore develop a strategy by:-

1. Identifying what is important and its weakness: Most institutions do not specify the components of the infrastructure necessary to achieve their objectives. For the most, no one of these institutions has completed its equipment to address weaknesses, which is scientifically called Minimum Essential Infrastructure (MEI) or developed plans to address this weakness.
2. Increasing participation in the two-way information between the public and private sectors. If the government and private sectors are targets for intruders, it is very reasonable for two (private and government) to exchange and share information with each other.
3. Improving the capacity of analysis and warning: This improvement affects the ability of analyzing information and developing effective warning directly in order to defend its national infrastructure.

1.4 E-mail Systems and Threats

There are several abbreviations that were announced on the electronic mail, often abbreviated as email or E-Mail, which refer to a method of exchanging digital messages, designed primarily for human use (Tony 2000).

E-mail systems are based on a store-and-forward model in which E-mail computer server systems accept, forward, deliver and store messages on behalf of the users, who only need to connect to the E-mail infrastructure, typically an E-mail server, with a network-enabled device (e.g., a personal computer) for the duration of message submission or retrieval (DCBPA Task Force 2010). Rarely is e-mail transmitted directly from one user's device to another's. E-mail is recommended by several prominent journalistic and technical style guides (The Chicago Manual of Style Online 2008). E-mail is the form required by the Internet Engineering Task Force (IETF) working groups (Braden, Ginoza & Hagens 2007) and is also recognized in many dictionaries.

A single piece of electronic mail is called a message. An electronic mail message consists of two components, the message header, and the message body, which is the E-mail's content (Crocker 1982). The message header contains control information, including, minimally, an originator's E-mail address and one or more recipient addresses. Usually, additional information is added, such as a subject header field. Originally, a text-only communications medium, E-mail is extended to carry multi-media content attachments, which were standardized, collectively called, Multipurpose Internet Mail Extensions (MIME).

E-mail is now the cornerstone in building the applications of E-government, there are many threats which must be paid more attention too.

Email security risks include attachments; scams; viruses and worms; spyware and adware; and hidden or devious links to bad websites (Kansas State University 2009). They attack by (Symantec Corporation 2010):

- Malware is a category of malicious code that includes viruses, worms, and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms sent through E-mail and instant messages, Trojan horses dropped from websites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy. Malware works to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user.
- E-mail Spam is the electronic version of junk mail. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. Spam is a serious security concern, as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks. Messages that do not include your E-mail address in the TO: or BCC: fields are common forms of spam. Some Spam can contain offensive language or links to websites with inappropriate content.

- Phishing is the criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of fishing (PCWorld.com 2006), probably influenced by phreaking (Oxford English Dictionary Online 2006), and alludes to baits used to "catch" financial information and passwords. Phishing is typically carried out by E-mail or instant messaging (Tan & Koon 2006), and it often directs users to enter details at a fake website, whose look and feel are almost identical to the legitimate one. Phishers are nothing more than tech-savvy con artists and identified thieves. They use SPAM, malicious web sites, E-mail messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Even when using server authentication, it may require tremendous skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users (Microsoft Corporation 2007), and exploits the poor usability of current web security technologies (Josang et al. 2007).

Phishers, pretending to be legitimate companies, may use E-mail to request personal information and direct recipients to respond through malicious web sites. Phishers tend to use emotional language using scare tactics or urgent requests to entice recipients to respond. The phish sites can look remarkably like legitimate sites because they tend to use the copyrighted images from legitimate sites. Requests for confidential information via E-mail or instant message do not tend to be legitimate. Fraudulent messages are often not personalized and may share similar properties like details in the header and footer. Everyday, more and more scam E-mails are sent out. These E-mails are often very convincing or frightening to those who receive them, so replies are sent and accounts are compromised. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Figure 1.2 shows an Attack percentage around the world.



Figure 1.2 Phishers Attack Percentages around the World
(Antiphishing.org 2009)

1.5 Problem Statement

E-mail is the backbone of E-government and most of its operations are applied by sending or exchanging messages through E-mail. There is a serious problem if this backbone is not well protected.

The problem is big and really serious. In fact, it is hard to imagine that we are sending our messages by E-mail while we know that the content of the letters might be stolen or exposed, including the E-mail address of the sender and the receiver. When they encrypted and the compression of all the functions designed to protect our messages will be opened. It is possible for a phisher to disguise another person and send a message. After this frightening scenario for E-mail profile, let's imagine what will happen to the firms that depend on a secure E-mail as a means to deliver secret messages, and then, let us imagine what will happen to the E-government if this problem is left unsolved.

The aim of this thesis is to protect the E-government E-mail by proposing a design to solve the problem by ensuring that transactions between E-government and citizen are carried out with appropriate security, in an environment where E-government has no control over all websites. Mainly, the subject of this thesis is how to resolve the problem of verification of the sender (Citizen), if the sender sends a message from another website for example: WWW.YAHOO.COM

1.6 Thesis Objective

The objective of this thesis is to ensure the drive towards E-government is secure by protecting its E-mail. The problems of E-mail are many and the scope of this thesis is to solve one of the most important problems that has already happened or will happen in the future. The focus of this thesis is to prevent fraud by preventing the phishers from entering the E-government and misusing it.

Clearly, the traditional mechanisms for enforcing electronic security measures in government, embodied in the manual of protective security, cannot be applied here. Therefore, it was decided to start from first principles, and define the security requirements for E-government applications from the ground up. The result is an emerging set of documents describing the threats, security objectives and counter measures for a government to citizen (G2C) and government to business (G2B) as well as electronic interactions (Stamoulis 2001). The documents include (Standards for The Protection of Personal Information of Residents of the Commonwealth 2010):

1. Confidentiality requirements (for the protection of personal citizen information against unauthorized disclosure),
2. Authentication requirements (for the registration and identification of citizens online),
3. Network defense requirements (for the protection of government back office systems against electronic attack), and
4. Trust service requirements.

1.7 Thesis Scope

Where governments can contact among several electronic media, which may be a part of any government or among different governments or between government and society, so the E-government should use electronic information technology in three areas (Tasha 2002):

1. Internal communication (that is between its branches and its division)
2. Outreach (to contact with people and businesses).
3. Contact with other government.

From our definition of E-government and from the types of E-government and their features, we can image who we can protect the different types of the E-mails that the E-government uses. This is the general scope, but by the special scope is the address will be in the E-government itself and the type which will be used.

1.8 Thesis Motivations

The motives that have contributed to write this thesis is combat all phishers and intruders... etc; there is no place among us for a fraud or theft. Those who use E-mails are either's employees, merchants, or ordinary people. Thus, it is natural that all of them may be exposed or may cause unintended mistakes. These errors may lead to huge losses. Every day, we hear or come across the mistakes which have occurred because of staff mistakes, whether intended or unintended,

so it was our contribution to prevent workers in this area from falling into these mistakes.

1.9 Thesis Limitations

The limitation of this contribution is the lack of an integrated E-government in the country where this thesis is written. Hence, it is hard to be tested in a practical solution conjectured to preview any possible errors. It is also hard to test the possibility of finding solutions to them on the ground. Because the currently service that Jordan E-government can provide to the citizen is only information about services, in terms of forms and procedures required to obtain a certain service. This means that it is impossible for anyone to request, follow-up, and obtain a service from the relevant ministry/gov agency, but in the next phase, the E-government will evolve to offer transaction support for a wide set of E-services (The Official Site of the Jordanian E-government 2010). Some other problems are occurring in the E-mail security, such as viruses, which are out of the scope of this thesis.

1.10 Thesis Organization

In addition to this chapter, this research includes four other chapters. In this section, we will describe briefly the contents of the thesis's chapters.

Chapter 2 will give scope and functions of E-government applications and will give a brief idea about the most relevant work in the literature that is related to our study.

In chapter 3, we will discuss the methods that are used to deceive the receivers of E-mail, the way the thieves and intruders steal our messages and pretend to be people we know.

Chapter 4 will focus on designing the proposed solution as an experimental work and will refer to the rates of success or failure.

Finally, chapter 5 will discuss the conclusions of our thesis; our final results and the way we used them to contribute in the studied domain are presented among the conclusions. Future works are suggested at the end of this chapter.

Chapter 2

E-GOVERNMENT APPLICATIONS AND RELATED WORKS

CHAPTER 2

E-GOVERNMENT APPLICATIONS AND RELATED WORKS

2.1 Scope of E-government Applications

The great importance of the E-governments use of information technology is to break the administrative border that has been developed by the administrative management of any government.

From the definition of E-government, we can realize the importance of building and using E-government applications in our lives, to facilitate the process of getting specific services for citizens. So, the tendency of building and implementing applications for an E-government is increased everyday, and the governments adopt this approach of computerizing their services incrementally. Governments worldwide are faced with the challenge of transformation and the need to reinvent government systems in order to deliver efficient and cost effective services, information and knowledge through information and communication technologies. The development of information and communication technologies catalyzed and led up to E-governments, also E-governments present a tremendous impetus to move forward in the 21st century with a higher quality, cost-effective, government services and a better relationship between the citizens and government. One of the most important aspects of the E-government is the way brings citizens and businesses closer to their governments (Zhiyuan 2002).

We can outline eight different potential types or models in an E-government system that is useful to define the scope of E-government studies (Zhiyuan 2002):

- Government-to-Citizen (G2C);
- Citizen-to-Government (C2G);
- Government-to- Business (G2B);
- Business-to-Government (B2G);
- Government-to-Government (G2G);
- Government-to-Nonprofit (G2N);
- Nonprofit-to-Government (N2G); and
- Government-to-Employee (G2E).

We can also examine some examples in E-government practices and presents a generally-applicable framework for analysis of challenges and problems in the E-governments development.

More and more attractions appeal to researchers and practitioners come to search for a consensus regarding E-government diagrams and initiatives. E-government may be defined as a continuum from information provision when organizations and public agencies publish static information to the Internet to web interactive communication and E-transactions, and to one-stop integrated virtual governmental services (Zhiyuan 2002). In the broadest sense, E- government project aims at establishing a better government structure, meaning that E-government focuses on "government" more rather than "e" (Erdem 2010).

According to Fountain who uses the term "virtual state", the digitalization of data and communication makes fundamental changes in the nature of government and its organization (Fountain 2005). Main components of E-government are E- firm, E- institution and E- citizen (Erdem 2010). Each of these will work to realize the "E" within them and they will develop in interaction, so E-government will develop eventually. The directions of E-government services can be grouped into three categories (Erdem 2010): {(G2G), (G2C), and (G2B)}, there are four kinds of activities of E-government (Jeffrey 2000; Mary 2003):

- Pushing information over the Internet, e.g.: regulatory services, general holidays, public hearing schedules, issue briefs, and notifications, etc.
- Two-way communications between the agency and the citizen, a business, or another government agency. In this model, users can engage in dialogue with agencies and post problems, comments, or requests to the agency.
- Conducting transactions, e.g.: lodging tax returns, applying for services and grants.
- Governance, e.g.: online polling, voting, and campaigning.

2.2 Functions of E-government Applications

Theresa outlined its functions as follows: Citizen accessed to government information, providing access to governmental information is the most common

digital government initiative (Theresa 2000). Facilitating general compliance's, E-government can also mean providing electronic access to services that facilitate compliance with a set of rules or regulations. Citizens access to personal benefits, electronic benefits transfer and online application for public assistance and worker's compensation are examples of services that provide the citizen with electronic access to personal benefits.

Procurement including bidding, purchasing, and payment, procurement applications allow government agencies to reap the benefits being realized in the private sector through electronic commerce applications. Electronic vendor cataloging, bid submissions and tabulations, electronic purchasing, and payment are government-to-government and government-to-business transactions that serve both the needs of government agencies as well as their private trading partners. Government-to-government information and service integration, integrating service delivery programs across government agencies and, between levels of government, requires electronic information sharing and integration. Citizens participation and online democracy both include access to elected officials, discussion forums, "town meetings," voter registration, and ultimately online voting. These services are intended to serve the community at large (Theresa 2000). Viewed from technical terms; E-government is an integrated tool comprising three enabling sets of new technology (Zhiyuan 2002):

1. Infrastructure,

2. Solutions and
3. The exploitation of public portals.

An E-government infrastructure enables the implementation of specific applications to address specific problems and issues of governmental management, so it is as a way for governments to use the most innovative information and communication technologies, particularly web-based Internet applications, so as to provide citizens and businesses with more convenient access to governmental information and services, to improve the quality of the services and to provide greater opportunities to participate in democratic institutions and processes (Zhiyuan 2002).

2.3 Related Work

This section gives a brief discussion about the most relevant works in the literatures that are related to this study to fight the phishers. We can note from all the following that there are systems which appear to protect the E-mail from phisher. So, we can't say that we do not have strong systems to fight the phishings but, we can say that it is not strict, and because of this lack of rigor will produce serious errors compromise the security of E-government in terms of E-mail.

1. “Spam Arrest, Brian Cartmell, 2001” (Spam Arrest 2001).

Launched in late 2001 in Seattle Washington, Spam Arrest's patent-protected and affordable system efficiently stops spam while offering extensive user flexibility. Spam Arrest blocks spam based on the Sender Address (the E-

mail address of the person sending the E-mail). There are three (3) types of sender addresses: Authorized, Unauthorized and Blocked.

When an E-mail arrives from an unauthorized (unknown) sender, an automated verification E-mail is sent from Spam Arrest asking the sender to verify him or herself by clicking on an included link. This link will direct the sender to a webpage which states that Spam Arrest is being used to block unwanted E-mails, and instructs the sender to type in a short verification word clearly displayed on the page. Once a sender successfully completes this quick and easy process, all future E-mails from that sending address are authorized and will be met with no further verification requests from Spam Arrest.

In just a few short years, Spam Arrest has seen explosive growth in its user base, while steadily expanding services and increasing functionality. Considered by many to be the top spam blocking service around, Spam Arrest prides itself on its continued efforts at monitoring automated junk E-mail techniques, upgrading automatically as necessary to protect its users from viruses, phishing and unwanted E-mail.

Limitations:

- Spam Arrest depends on real people sending you real E-mail receiving the Spam Arrest verification request. Spammers use fake or invalid return E-mail addresses and automated systems, which means that they never receive the

Verification Request and so cannot verify themselves. But the new fact of phishers can receive the Spam Arrest verification request and can reply it.

- Some jurisdictions do not allow the limitation or exclusion.
- The amount of E-mail address that Spam Arrest can treat is not enough.
- Spam Arrest verification request can't apply only by the sender's action.

2. **“Sender Address Verification, Tal Golan, 2004”** (Circle ID 2004)

This approach, known as Sender Address Verification or SAV, is poised to cripple the spammer's ability to deliver machine-generated E-mail. SAV employs a patented methodology that asks first-time senders to verify their E-mail address before a message is forwarded to an individual recipient's inbox. SAV is easy to set up and provides tremendous value to both IT and business users.

SAV makes it impossible for the purveyors of spam to realize the financial gains that have been enjoyed in the past. SAV eliminates the unfettered access to email inboxes that was available to crafty spammers (phishers), enabling companies to regain productivity and IT resources once lost to fight spam. As this simple and elegant approach gains widespread acceptance, spam, as we know it, may be entirely eradicated.

Limitations:

- We can't ask all citizens to set up.
- The new fishers cannot answer to questions.

3. **“Bluebottle, Bluebottle Solutions Pty Ltd, 2006”** (Bluebottle Solutions 2006)

It is anti-spam and anti-phishing E-mail technologies helps keep E-mail's inbox free of spam and phishing.

When Bluebottle receives a message from an E-mail address or domain not on your "Allowed" list, it E-mails the sender a "verification request". This asks the senders to verify themselves by clicking on a link. Once verified, the system automatically adds the sender's E-mail address to your "Allowed" list and the message is sent through. Future messages are automatically let through until removing the sender's E-mail address from the “Allowed" list.

To avoid identification, spammers or phishers commonly use fake E-mail addresses. Consequently, the verification request is never seen or responded to, so spammers don't get added to allow list and don't receive spam or phishing E-mail. If sending an E-mail, Bluebottle automatically adds the recipient's E-mail address to the allowed list. This means that they don't spend time managing E-mail or configuring spam settings. It's all automatic - and best of all, the senders don't get a verification request when they reply to E-mail.

Limitations:

- Many users worry and feel afraid from clicking on a link.
- With huge amount of messages, there is a delay that will happen.
- The new fishers can click on a link.

4. **“Australian Government E-mail Address Naming Standards and Implementation Guidance, Australian Government Staff Group, 2008”**(Michelle 2008)

These standards have been produced by Australian Government Information Management Office (AGIMO) within the Department of Finance and Deregulation at the request of the Australian Government’s Business Process Transformation Committee (BPTC). The standards have been endorsed by and are issued under the authority of the Australian Government's Chief Information Officer Committee (CIOC). The BPTC requirement was for Email Address Naming Standards that defined a format for E-mail address creation that:

- Presents a consistent image of government accessibility;
- Is intuitive to use; and
- Provides a simple way to find or determine email addresses of Australian Government employees.

The Standards comprise three elements:

- Published personal email addresses,
- Managing Duplicates, and
- Functional Addresses.

Standards Limitations:

- The workspace on the Australian Government Department of Finance and Deregulation (GovDex) website can only be accessed by nominated contacts in relevant agencies. This can be accessed at www.govdex.gov.au.
- The E-mail address must have the person's names in all lowercase only.
- The email address should as much as possible reflect the way an individual spells their name.
- The amount of any additional spam generated by application of these standards is unclear at present, and will need to be monitored as the standards are applied.

5. “Comprehensive Email Filtering, Barracuda Networks Inc., 2008” (Barracuda Networks Inc. 2008)

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against E-mails phishing, spam, web

and threats as well as products that improve application delivery and network access, message archiving, backup and data protection. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and the European organization are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif.

Filtering E-mails in two advanced processes. Barracuda Networks designed the affordable Barracuda Spam & Virus Firewall as an easy-to-use, enterprise-class hardware and software solution for businesses of all sizes that comprehensively evaluates each E-mail, using two main classes of sophisticated algorithms and techniques:

- Connection management and
- Mail scanning.

During the connection management process, E-mails are filtered through five defense layers to verify authenticity of enveloped information, and any inappropriate incoming mail connections are dropped even before receiving the message. Any E-mails that survive the connection verification process must then undergo a thorough mail scanning process that involves an additional seven defense layers of message analysis.

Limitations:

- Citizens that relay E-mail through known servers or communicate frequently with known partners should add the IP addresses of those trusted relays and good E-mail servers to the Rate Control exemption list.
- Can treat many types of phishing and spam but not all.

6. “Thunderbird Sender Verification Extension, Joshua Tauberer, 2009” (Tauberer 2009)

This is an extension for the Mozilla Thunderbird E-mail program that reports, when possible, for protecting E-mails from phishing ,whether the sender shown in the From: The header was actually the sender of the E-mail. In fact, forging the From: header is possible. This is an anti-phishing used to protect from fraudulent E-mails asking for sensitive information, and zombie-spread viruses claiming to be from someone they are not.

The extension uses Sender Policy Framework (SPF) (in a nonstandard way) to verify the sender's domain, and SURBL, Spamhaus, DNSWL, and Sender Score Certified for reputation information.

The extension checks the domain name (e.g. aol.com) in the From: header, but not the user name's part (e.g. the "my.name" part in my.name@aol.com).The

extension sits at the top of every E-mail message and reports the verification status of the sender as shown into figures 2.1 and 2.2.

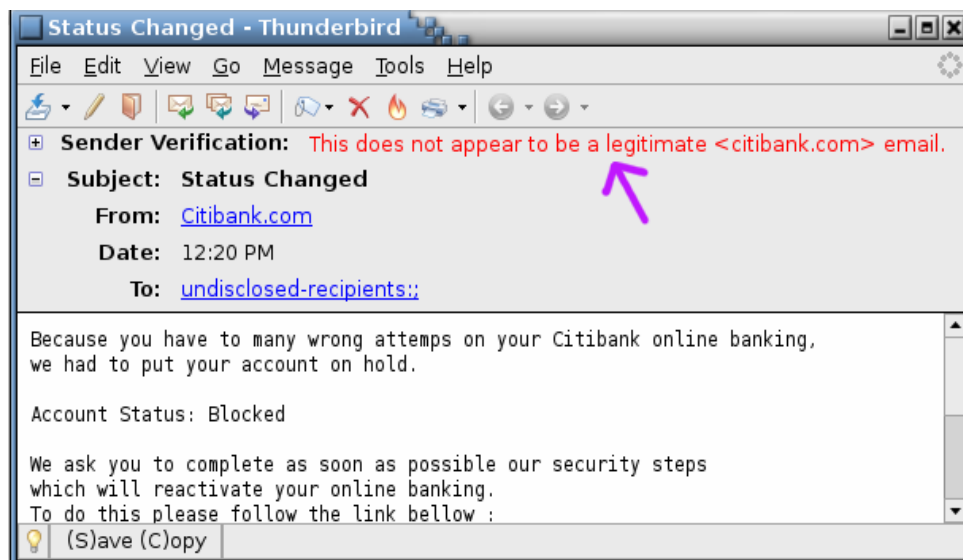


Figure 2.1 "Sender Verification" Lines Show the Results of Verification Checks Performed by the Extension (Tauberer 2009).

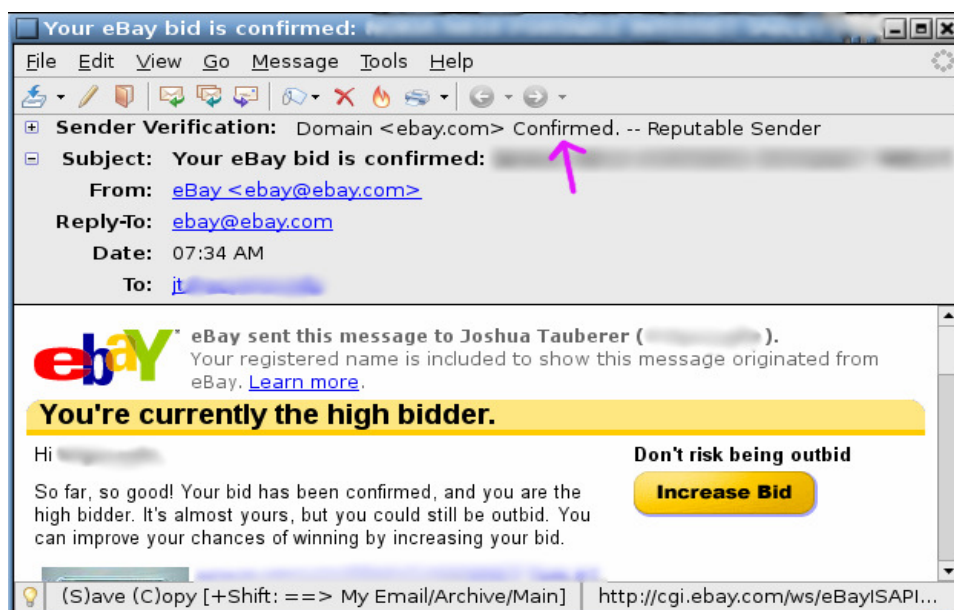


Figure 2.2 "Sender Verification" lines show the Results of Verification Checks Performed by the Extension (Tauberer 2009).

Limitations:

- Since many domains don't support SPF, E-mails claimed to be from these domains can't be verified with the methods used by the extension.
- These new E-mail protocols aren't perfect, and neither is the extension, so positive verification results should be interpreted with a common sense.
- This method can't treat all kinds of phishers.

7. “Interoperability Program, State of Tasmania, 2010” (Tasmanian Government Email Address and Username Standards 2010).

The Tasmanian Government E-mail Address and Username Standards version 1.1 were approved for use in Tasmanian Government Agencies on 8 September, 2008 by the Tasmanian Government's Inter Agency Steering Committee (IASC).

There are two main purposes of these Standards (Tasmanian Government Email Address and Username Standards 2010):

- To provide for a consistent whole of government approach for the format of E-mail addresses, usernames and display names.
- To fight the phishers.

These standards also include guidance on:

- Selecting appropriate terms for E-mail domain names and role-based or functional email addresses;
- Policy for the management of redundant email addresses and domains;
- A recommended approach for managing duplicate names.

These standards are based upon and supersede the Tasmanian Government Email Address Naming Standard May 2000 and have been developed to encourage consistency of user attributes across the government. Adoption of these standards will assist agencies to participate in the implementation of multi-agency and whole-of-government IT applications and services.

Standard Limitations:

- All organizations using the <.tas.gov.au> E-mail domain should comply with these standards.
- This standard applies to user accounts. It does not apply to administrative and service accounts for an agency's internal use only (Tasmanian Government Standard format for usernames 2010).

Chapter 3

SYSTEM ANALYSIS

CHAPTER THREE SYSTEM ANALYSIS

3.1 Overview

This chapter will analyze the current system that has a problem and explains the way it will be solved using a proposed solution. In fact, this solution attempts to prevent the E-mails from malicious acts that hack and steal user's messages and falsify E-mail addresses to trace confidential information. They try to hack personal E-mails, and try to find a trove of information (E-government). The phishres mode's will be studied and analyzed in order to reach new ways to fool us. We have always observed in our E-mail that there were attempts which really came from the actual studies and real analyses. But there is no problem in this World that cannot be solved. Hence, this chapter will focus on gathering information and analyzing how the phishers reached a new ways to cheat the confidential information. In order to develop the current system, we need to analyze the current system. Analysis involves a detailed study of the current system as shown in figure 3.1, leading to specifications of a new system.

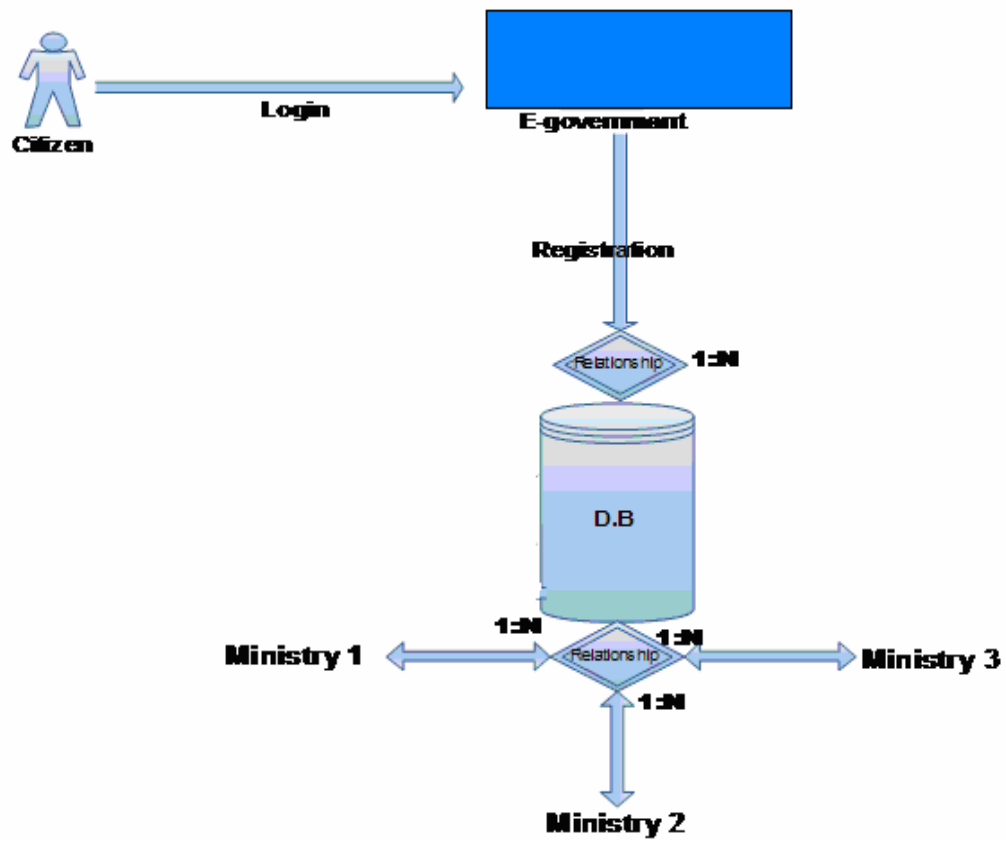


Figure 3.1 The Structure of the Current System

3.2 Current System Scenarios

There are only two scenarios of the current system, when the citizen wants to take advantage of E-government services. Citizen will login E-government site, as shown in figure 3.2.

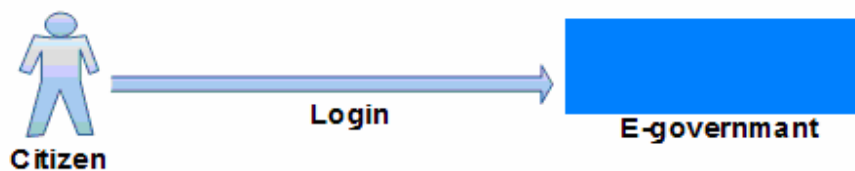


Figure 3.2 Citizen Login E-government Site

The registration system of the E-government will ask the citizen about recording information related to the citizens, such as the first name, last name, E-mail, address, date of birth and national number in the verification process, as shown in figure 3.3, and then the citizen can do all transactions inside the E-government website or the citizen can send messages through “submit messages” that is found inside the E-government website as shown in figures 3.4, 3.5, 3.6..

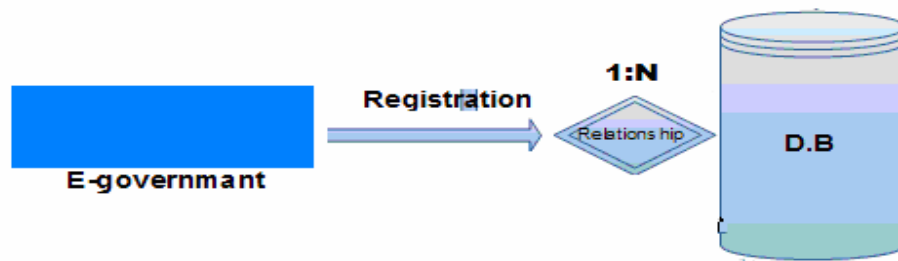


Figure 3.3 A Citizen’s Registration into the E-Government Database

CHIP/Children's Medicaid
We've got your kids covered.

Application Request
Enter your name and address. We will send you a blank application for Children's Health Insurance Program (CHIP), Children's Medicaid, and CHIP perinatal.

* First Name Middle Name or Initial * Last Name

* Street Address Apt/Lot#

* City * State * ZIP Code County

[Close This Page](#) [Submit](#)

Figure 3.4 Application Request (USA E-government 2010)

Citizen Registration

Field	Value
Citizen Number*	<input type="text"/>
First Name*	<input type="text"/>
Middle Name*	<input type="text"/>
Last Name*	<input type="text"/>
Address*	<input type="text"/>
<input type="button" value="update"/>	

* = Mandatory form fields

[Back to list Citizens](#)

Figure 3.5 Citizen's Registration Form
(Tanzania E-government 2005)

Send E-Mail

Field	Value
From (Email Address)*	<input type="text"/>
Subject*	<input type="text"/>
Message*	<input type="text"/>
<input type="button" value="send"/>	

* = Mandatory form fields

Figure 3.6 Send E-mail Form
(Tanzania E-government 2005)

3.3 Security Importance

In the past, the organizations and individuals saved their confidential information in certain files behind the walls. These practices lasted for a long time; documents were stored in the rooms with no fear from thief or intruders coming from overseas to look for these businessmen and reveal their secrets. In other words, fear was external, so we can say that there is an inverse relationship;

as time progresses less security is provided. This is reason behind the fact that everyone has been looking for a way to save his/her privacy. Unfortunately, these traditional ways no longer meet the requirements of security. Instead, it is time we need to publish and store our confidential information through the Internet, of this point comes the importance of security in our lives but we can't say that we do not have strong security for the systems, but we can say that it is necessary to protect the E-mail which is one of the most important gates in our lives and not just for E-government.

3.4 Phishing Scenarios

Common phishing techniques include sending a false URL via a fraudulent E-mail to the victim, using instant-messaging application and planting false links in web pages. In any case, once the unsuspecting user opens the URL, he is connected to the attacker's web server which appears to be the legitimate server, where he is prompted to enter his personal details.

There are three possible phishing scenarios (Anti-phishing.org 2009):

1. Wrong-domain server: The most common scenario. The attacker solicits the user to connect to a false URL, which includes a domain-name different from the real server's domain name.
2. DNS-poisoning: the attacker somehow manages to divert traffic designated to the real server's URL to his own machine. This case is similar to the previous one, except that the domain name appears to be

valid to the user. In this case no, solicitation is required, as the user connects to the attacker's machine whenever he attempts to connect to the real server.

3. Real Man-in-the-Middle: the attacker is in full control of one of the hops in the path between the user and the real server. In this case, no solicitation is required, as the attacker's machine fully controls any traffic that passes through it.

3.5 Phishers Events

The problem, which results from phishers events, appears through our daily lives in the personal and business areas and cannot be overcome. There are deals and money wasted in the wrong area caused by phisher's attacks by entering a fabrication message in the network or adding a constraint in the file where this attack is into authentication, as shown in figure 3.7.

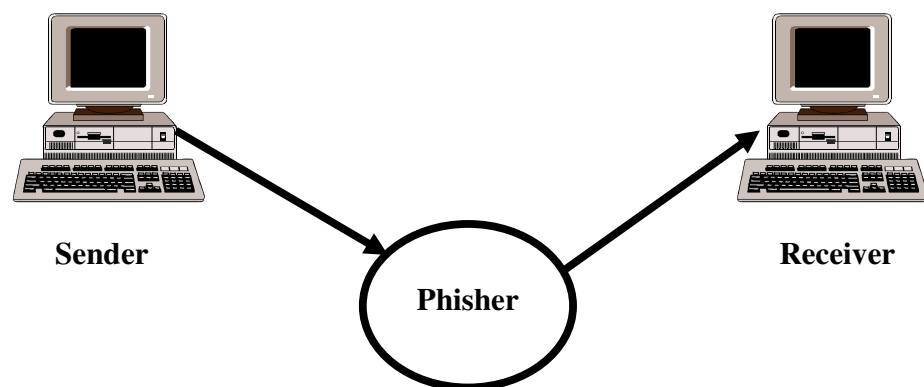


Figure 3.7 Fabrication

Because of these mistakes, intended or unintended from professionals and non-professional people, correct E-mail addresses are important in protecting the

privacy and secrecy of information. This privacy can be secured by ensuring that the information contained goes to the right recipients.

Phisher starts to create more information on purpose. At this point, the attacker wants to be more hidden whenever possible. Some of these methods make a full search and transfer (DNS Zone), as well as website browsers for compilation of E-mail addresses and important information, especially collected for the same purpose. Is an attempt to collect more information by the attacker, will usually be completed inspection Ping and check the web server. Phisher will verify the current generations of applications and services on the server, and he uses the techniques of Banner Grabbing.

3.6 The Problem Analysis

In this section, we describe the phase of problem analysis for the current system, present a summary of how the phishers work, and then analyze these works to get the best solution to avoid them.

E-governments are responsible for any transaction from inside its website and are not responsible for any transactions or information provided from other websites, as shown in figure 3.8. This note gives an indication; there is a fear of any scam message that can be sent from an E-mail. In this case, there is a fear from the sent message that it can be from a phisher (the sender is not the real E-mail owner).

► **Services by the Government of Jordan**

You are about to leave the Jordan e-Government Portal. Please revert to the privacy policy of the website you are about to view. Jordan e-Government Portal is not responsible for any transactions and/or services and/or information provided by other websites.



Figure 3.8 E-government Is Not Responsible for Other Websites (Services by the Government of Jordan 2010)

The current system will face a big problem which is that SMTP has no generally-required mechanisms for authentication. Sometimes, when a user sends messages to his friends, they see these messages in their spams rather than their inboxes. Mainly, any E-mail address has two parts; the part before the @ symbol is the local-part of the address, which is often the username of the recipient, and the part after @ is the domain, which refers to the domain's name to which the E-mail message will be sent. Addresses found in the header fields of E-mail (Display Name) should not be considered authoritative, because as we mentioned above, the SMTP has no generally-required mechanisms for authentication. Forged E-mail addresses are often seen in spam, phishing, and many other internet-based scams.

Hence, even through an E-mail address apparently consist of two parts, it actually contains three parts as shown below:

- Display name
- User name
- Domain

“Display name” < User name @ Domain >

Figure 3.9 E-mail address

The fact we recognize is that the message sent from the sender to the receiver is able to reach safely and the phisher cannot stop this reach. The real problem occurs when the phisher seize the opportunity when we do not check the addresses of E-mail we receive to achieve his purpose. We can observe that through two messages received from one sender as shown in figure 3.10.

	From	Subject	Date	Size
	Ali Hassan	SC	9:21 PM	960KB
	Ali Hassan	SC	9:02 PM	839KB

Same Sender

Same Subject

Different Date

Figure 3.10 Shown Same Senders, Same Subject and Different Date

(Y Rasheed 2010, pers. comm., 15 March)

It is normal that we would receive two messages from the same sender and it is also normal that they would contain the same subject. In this case, there are two probabilities:

The first is that the same sender has decided to send the same message twice to ensure that his message has been received.

The second probability is that the sender may have possibly sent the second message because he wants to make some modifications on his information and decided to send it again. In both cases, the latest message will be used, relied on and we will not pay attention to the old message, and this is the fact that the problem emerges from. Figure 3.11 shows the true message of the sender and figure 3.12 shows the attached file to the real sender.

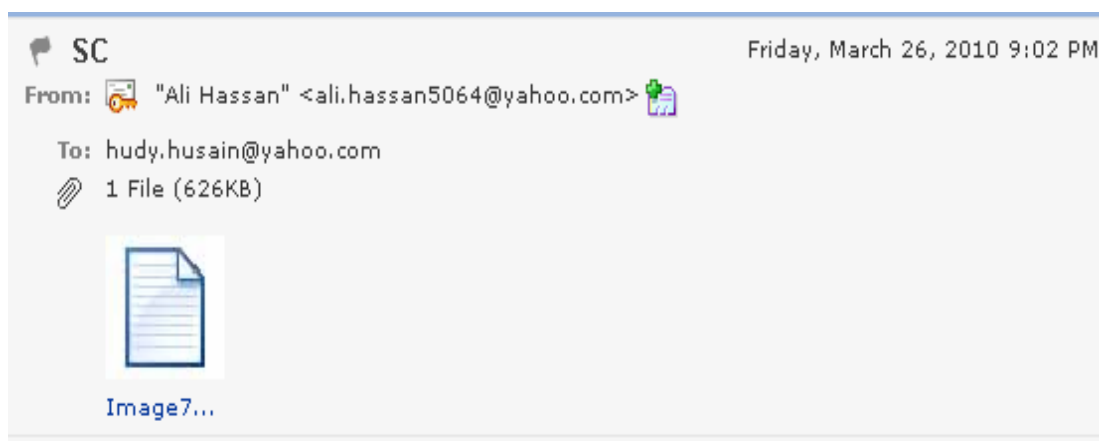


Figure 3.11 True Message of the Sender
(Y Rasheed 2010, pers. comm., 15 March)

SALES CONFIRMATION

买 方: **KHDAYR ABBAS TURKI CO. AND PARTENERS**
 The Buyer: P.O.BOX: 928130 AMMAN 11190, JORDAN

No.: **CT-2010-007**
 Date: **27-JAN., 2010**

兹确认售予你方下列货品，其成交条件如下：

We hereby confirm having sold to you the following goods terms and conditions as specified below:

(1) 货物名称、规格 Name of commodity, specifications	(2) 数量 Quantity		(3) 单价 Unit Price	(4) 金额 Amount
BURMA TEAK FACED PLYWOOD HARDWOOD CORE, 4.8MMX3'X7' AA GRADE, C/C 4.8MMX3'X7' A GRADE, Q/C 3.6MMX3'X7' AA GRADE, C/C 4.8MMX4'X8' AA GRADE, C/C 3.6MMX4'X8' AA GRADE, C/C	SHEETS	M3	CFR (Per Sheet)	AQABA
	20000	187.5384	USD 6.90	USD 138,000.00
	20000	187.5384	USD 5.90	USD 118,000.00
	18900	132.9178	USD 5.53	USD 104,517.00
	2700	38.5793	USD 9.43	USD 25,461.00
	4160	44.5806	USD 7.50	USD 31,200.00
TOTAL:	65760 SHEETS	591.1545 M3	***	USD 417,178.00

5 数量及总值均得有的增减，由卖方决定。

With 5% more or less both in amount and quantity allowed at the seller's option.

6 包装

Packing : EACH SET IN A CRATE

7 装运期限

Time of shipment: BY CONTAINER. SHIPMENT IN THE END OF FEB., 2010.

8 装运口岸和目的地

Loading port & Destination: FROM SHANGHAI, CHINA TO AQABA PORT, JORDAN.

9 保险由卖方按发票金额的110% 投保至

为止的 险。

Insurance: BY BUYER

10 付款条件

Term of Payment: 30% ADVANCE PAYMENT (USD: 125,153.40) BY T/T BEFORE SHIPMENT, REST PAYMENT BY D/P.

Please Remit Proceeds to the Following:

SHANGHAI PUDONG DEVELOPMENT BANK JIAXING BRANCH. (SWIFT BIC: SPDRCN336)

For Credit To:

TONGXIANG SHENGFEI DECORATE MATERIAL CO., LTD.

A/C NO. (USD) : 860 414 547 100 000 12

桐乡市晟丰装饰材料有限公司
 TONGXIANG SHENGFEI DECORATE MATERIAL CO., LTD.

THE BUYERS

Figure 3.12 True Attached File of the Sender

(Y Rasheed 2010, pers. comm., 15 March)

Figure 3.13 shows the phisher's message and figure 3.14 shows the phisher attached file.

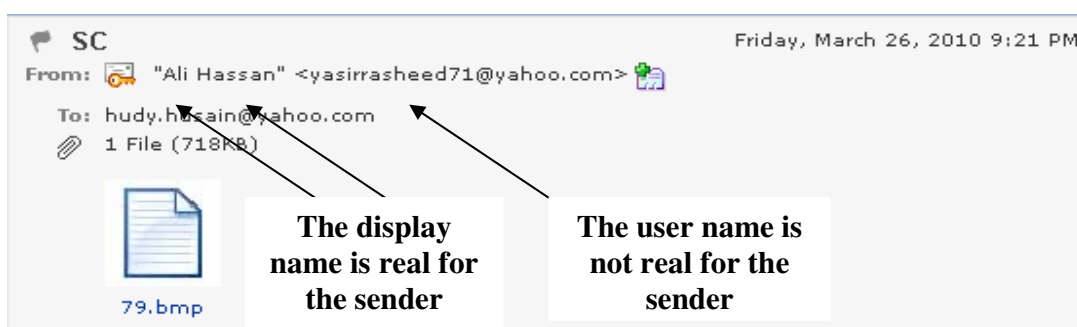


Figure 3.13 The Phisher's Message
(Y Rasheed 2010, pers. comm., 15 March)

SALES CONFIRMATION

买方: **KHDAYR ABBAS TURKI CO. AND PARTENERS** No.: **CT-2010-007**
 The Buyer: **P.O.BOX: 928130 AMMAN 11190, JORDAN** Date: **27-JAN.,2010**

兹确认售予你方下列货品, 其成交条件如下:
 We hereby confirm having sold to you the following goods terms and conditions as specified below:

(1) 货物名称、规格 Name of commodity, specifications	(2) 数量 Quantity		(3) 单价 Unit Price	(4) 金额 Amount
	SHEETS	M3	CFR(Por/Sheet)	AQABA
BURMA TEAK FACED PLYWOOD				
HARDWOOD CORE,				
4.8MMX3'X7' AA GRADE,C/C	20000	187.5384	USD 6.90	USD 138,000.00
4.8MMX3'X7' A GRADE,C/C	20000	187.5384	USD 5.90	USD 118,000.00
3.6MMX3'X7' AA GRADE,C/C	18900	132.9178	USD 5.53	USD 104,517.00
4.8MMX4'X8' AA GRADE,C/C	2700	38.5793	USD 9.43	USD 25,461.00
3.6MMX4'X8' AA GRADE,C/C	4160	44.5806	USD 7.50	USD 31,200.00
TOTAL:	65760	591.1545	***	USD 417,178.00
	SHEETS	M3		

5 数量及总值均得有增减, 由卖方决定。
 With 5% more or less both in amount and quantity allowed at the seller's option.

6 包装
 Packing: EACH SET IN A CRATE

7 装运期限
 Time of shipment: BY CONTAINER, SHIPMENT IN THE END OF FEB., 2010.

8 装运口岸和目的地
 Loading port & Destination: FROM SHANGHAI, CHINA TO AQABA PORT, JORDAN.

9 保险 由卖方按发票金额的110% 按保至 为止的 险。
 Insurance: BY BUYER

10 付款条件
 Term of Payment: 30% ADVANCE PAYMENT (USD: 125,153.40) BY T/T BEFORE SHIPMENT, REST PAYMENT BY D/P.

Beneficiary Bank
 AGRICULTURAL BANK OF CHINA, JIAXING BRANCH, No.383 Xidex Street,
 Jiaxing City, 314000, Zhejiang Province, China, TELEX: 351186 ABCIX CN
 SWIFT CODE: ABOCCNBJ10

Beneficiary:
 JIASHAN HAOSHENG TIMBER CO., LTD. Jiashan Economic Development Zone,
 J County, 314100, Zhejiang, China, A/C NO: 1933 1414 0400 0296 9

桐乡市晟丰装饰材料有限公司
 TONGXIANG SHENG FENG DECORATE MATERIAL CO., LTD.

THE BUYERS

The phisher purpose

Figure 3.14 The Phisher's Attached File
(Y Rasheed 2010, pers. comm., 15 March)

The possibility that this problem occurs is shown in figure 3.15 and figure 3.16.

The screenshot shows a Yahoo! account creation form. The 'Name' field is split into two boxes: 'Ali' and 'Hassan'. A label 'Different' with an arrow points to the 'Ali' box. Other fields include Gender (Male), Birthday (January 10, 1970), Country (Jordan), and Postal Code (00962). Below the form, there is a section titled 'Select an ID and password' with a 'Yahoo! ID and Email' field containing 'yasirrasheed71@yahoo.com' and a 'Change' link. The 'Password' field is empty, and the 'Re-type Password' field is also empty. A 'Password Strength' indicator shows four empty boxes. A note below the password fields states: 'Capitalization matters. Use 6 to 32 characters, and don't use your name or Yahoo! ID.'

Figure 3.15 Processes Creating an E-mail for Phisher
(Y Rasheed 2010, pers. comm., 15 March)

The screenshot shows a Yahoo! account confirmation page. At the top, the Yahoo! logo is on the left and 'Yahoo! | Help' is on the right. The main heading is 'Congratulations, Ali!' with a sub-message: 'A confirmation message was sent to you via email.' Below this, a box titled 'Below are your account details' contains the following information: 'You will need this information to sign in to Yahoo! and to reset your password in case you forget it. Please print and keep this information in a safe place for future reference.' followed by 'Yahoo! ID & Email yasirrasheed71@yahoo.com address:', 'Alternate Email yasirexp@hotmail.com', and 'Birthday 10 January 1970'. A 'Print Account Details' link is also present. To the right of the account details box, there is a checkbox for 'Install the new Yahoo! Toolbar and make Yahoo! Mail faster.' with the instruction '(please follow the next few steps to get your new toolbar)'.

Figure 3.16 The Success of the Process Creating an E-mail for Phisher
(Y Rasheed 2010, pers. comm., 15 March)

At this point the disaster will happen. The users of E-mail rely on the reliability of an E-mail. Even if we audit and focus on the sender of the messages, we can't observe that the E-mail addresses are various. Different, one is true and the second is false, which causes this problem. The lack of scrutiny is due to two reasons: the first is the enormous amount of work and the second is the different level of professionalism of the computer users.

Mainly, the subject of this thesis is how to resolve the problem of verification of the sender, if the sender sends a message from another website. For example: WWW.YAHOO.COM.

Now, let's imagine our example and reverse this example on our E-government and what will happen if others have our information, and how to miss-chance to happen such as problems. Chapter four will explain in detail the design of the proposed solution to protect the E-mail of the E-government.

Chapter 4

DESIGNING THE PROPOSED SOLUTION

CHAPTER FOUR

DESIGNING THE PROPOSED SOLUTION

4.1 Overview

This chapter will focus on designing the proposed solution as an experimental work. Input, output and processing specifications are all drawn up in detail. In E-government applications, E-mails will be considered among the important constitutions of these applications. Some of the E-mails are highly secured and others are just secured.

There are different methods used in the design of the protection of information, where some of these methods have complexity of the design protection systems. So while working to solve this problem (phisher) at the beginning, we have to pay attention to the value of the information. As mentioned, we can get a complete system to protect the E-mail in E-government applications, such as: Citizen to E-government (as a low level of security)

The proposed solution tries to prevent any phishers, access to our confidential information that was stored in E-government databases. The proposed solution will save precious time and effort that phishers try to make us lose.

4.2 Designing the Proposed Solution

In this section, the researcher will address the low level of security (Citizen to E-government); there is no chance to use cryptographic algorithms for many reasons:

1. There is no way to determine the value of information.
2. We should not impose restrictions on the citizens, because we must encourage them to contact the E-government, rather than making them feel bored.

The proposed solution is a verification process from the owner of the E-mail as shown in figure 4.1

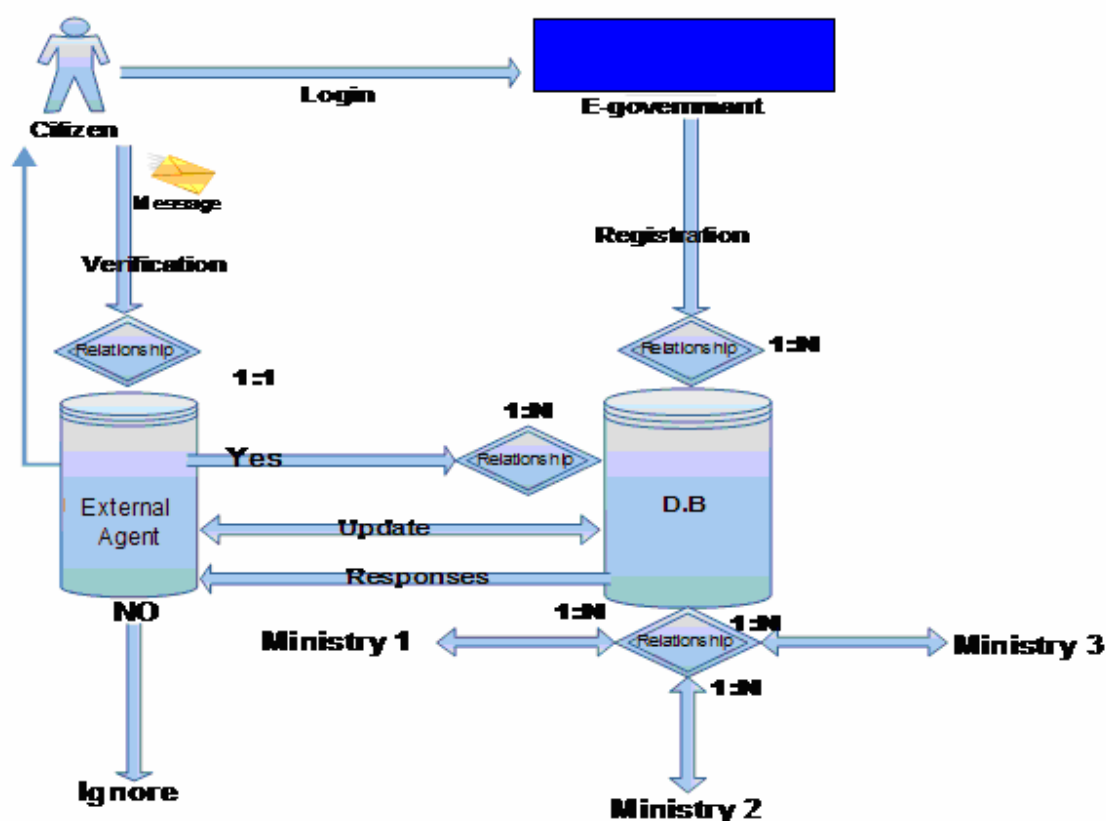


Figure 4.1 The Structure of the Proposed Design

The proposed solution proposes to link all ministries to only one registration system, which records information on the citizens. Some of this information is compulsory, such as the first name, last name and also the E-mail, while others are optional, such as the address, date of birth and the national number in the verification process, as shown in figures 4.2, 4.3.

Citizen Registration

Field	Value
Citizen Number*	<input type="text"/>
First Name*	<input type="text"/>
Middle Name*	<input type="text"/>
Last Name*	<input type="text"/>
Address*	<input type="text"/>
(Email Address)*	<input type="text"/>

Figure 4.2 Citizen Registration

First name	<input type="text" value="Ali"/>	
Second name	<input type="text" value="Majed"/>	
Last name	<input type="text" value="Ali"/>	
Date of Birth	<input type="text" value="3/20/1950"/>	<input type="button" value="Find Record"/>
ZIP	<input type="text" value="962"/>	
National number	<input type="text" value="654784"/>	
Address	<input type="text" value="Jordan-Arbid"/>	
E-mail	<input type="text" value="ali.majed@hotmail.com"/>	
<input type="button" value="Add Record"/> <input type="button" value="Save Record"/> <input type="button" value="Delete Record"/> <input type="button" value="Close Form"/>		

Figure 4.3 Registration System

The proposed solution suggests providing the citizens by special E-mails, which can be used from any website, to do any transaction required. There are several goals of providing citizens with special E-mail addresses, these objectives are:

- Citizen should not feel bored, because of using the special E-mail address that is provided by the E-government website without going back and searching for an E-government site.
- Citizens can distinguish the special E-mail address which is provided by the E-government and use it anytime easily. It is impossible for any citizen to remember all E-mail addresses and for which activities they were used. We can see that in figures 4.4 and figure 4.5 which show that every ministry has their E-mail addresses and websites. This means that are dozens of E-mail addresses we must remember if we think using them for our website.
- The special E-mail address that the E-government provides has a significant role in the verification process.

Income and Sales Tax Department Contact Information

Address:	Jabal Amman -3rd circle -Tower Building
P.O.Box:	840818
Zip code:	11184
City:	Amman
Telephone:	(962) 6 4604444
Fax:	(962) 6 4624599
e-mail:	istd@istd.gov.jo
Website address:	www.incometax.gov.jo

Figure 4.4 Address (A) (Income and Sales Tax Department 2010)

Department of Land and Survey Contact Information

Address:	Jebal al Weibdeh – near Lozmila Hospital – Land and Survey Street
P.O.Box:	70
Zip code:	11193
City:	Amman
Telephone:	(962) 6 463 2601
Fax:	(962) 6 4614 567
e-mail:	dls@dls.gov.jo
Website address:	www.dls.gov.jo

Figure 4.5Addresses (B) (Land and Survey 2010)

From all of the mentioned above, we can summarize the following three points:

1. E-governments fear from other websites.
2. There are dozens of E-mail addresses.
3. The inability to use encryption algorithms.

Moreover, we can search the entire database to verify that the citizen has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching, as shown in figure 4.6. The new approach verifies any citizen's claim of identity from the message that sent from many websites. This is also called "one-to-one" matching, as shown in figure 4.7.

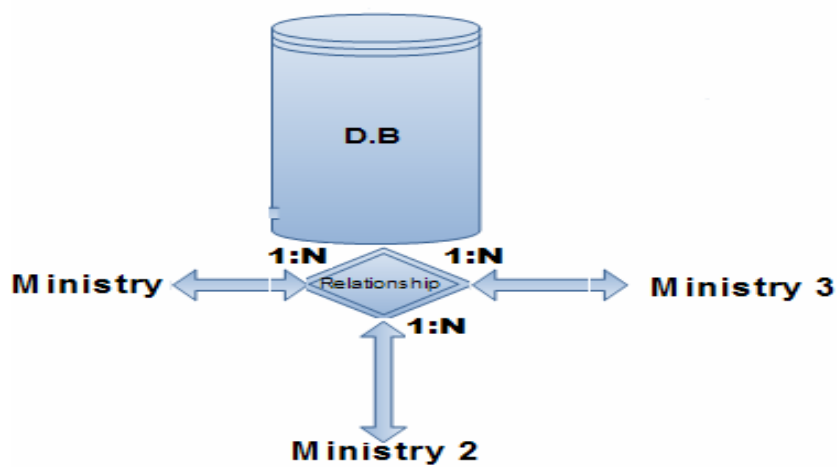


Figure 4.6 "One-To-Many" Matching

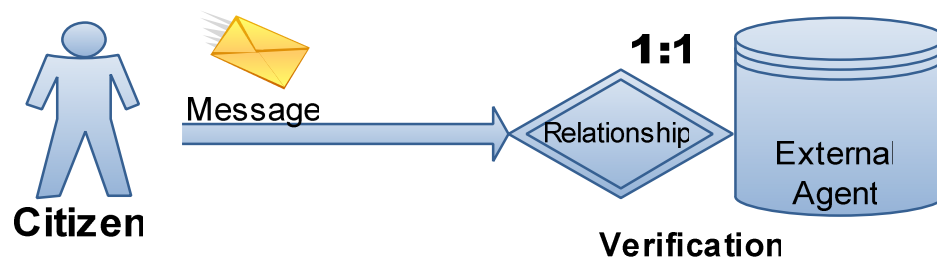


Figure 4.7 Citizen Sent Message from Any Website

The main idea of the proposed solution is that it adopts the redundancy.

We can actually note in addition to many other benefits of E-mail that there is no chance for redundancy as long as the mail server does not accept the redundancy.

In fact, there are two cases in which the redundancy may occur. This can be clearly seen in figure 4.8. Phisher fakes sender of an E-mail address that does not exist to recipients that are no longer or never been valid.

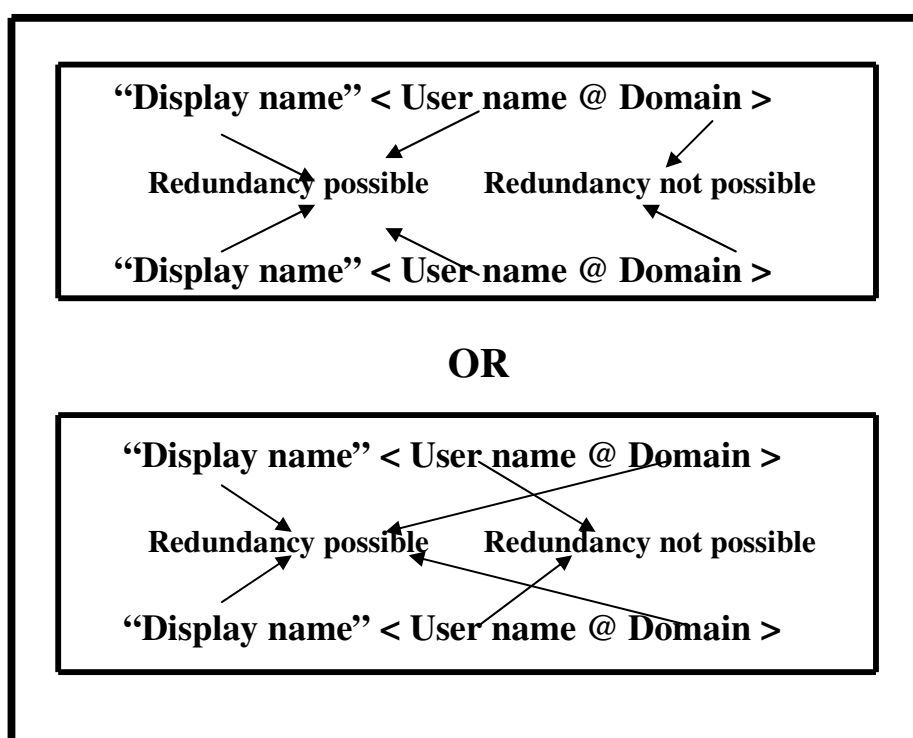


Figure 4.8 Possible and Impossible Redundancy

The proposed solution suggests linking the database of the E-government registration system to an external agent, as shown in figure 4.9.

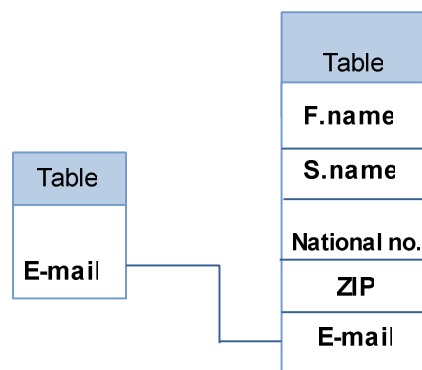


Figure 4.9 Linking the E-mail Address

In the following, we can discuss linking and using the external agent, which has two basic roles:

1. Continuous updates of the E-mail addresses which are obtained from E-government registration system databases, as shown in figure 4.10.

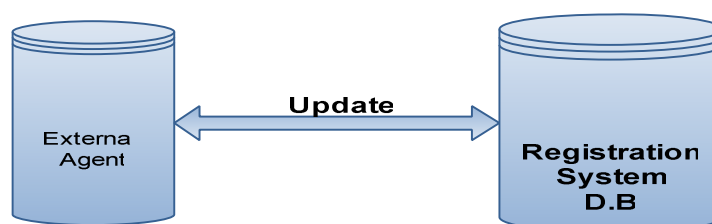


Figure 4.10 Updating the E-mail Addresses

2. Verification process from the sender identity, through comparing the E-mail address that registered in the E-government registration system database with an E-mail address in the sender's message. If

the citizen was registered in the E-government registration system database, the message be accepted (the reason for this is that redundancy will occur) and the rest of the procedures will be done, but if it is not registered, the message will be ignored, as shown in figure 4.11.

Therefore, the main role of the external agent is validating recipients and accepting valid citizen's E-mails in particular. They already have records in the E-government registration system.

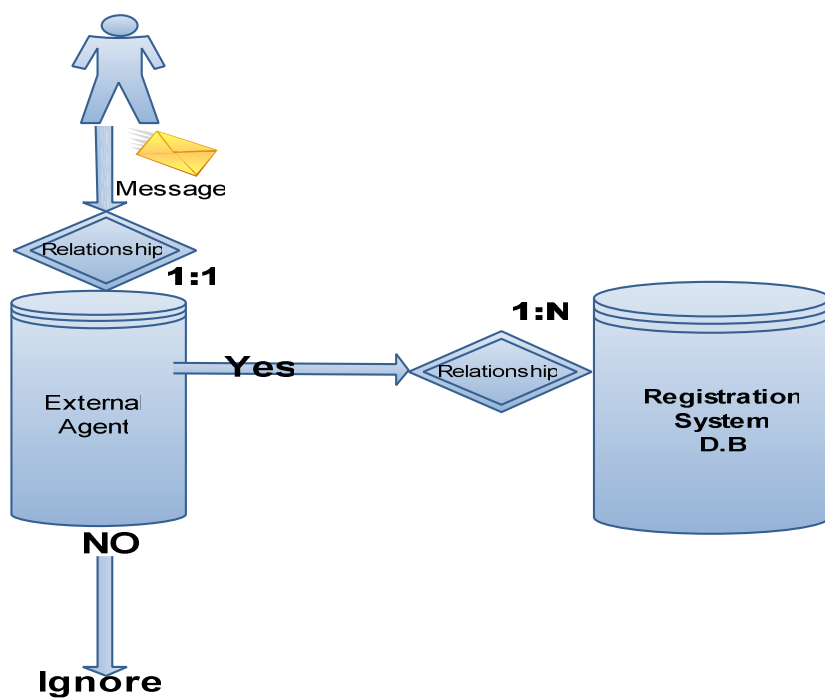


Figure 4.11 Verification Process

The verification process can be conducted on the basis of the active directory, using the databases or text address lists. The external agent uses a

filtering point to filter SMTP traffic and not to filter POP3 traffic. This is due to the fact that there is a tradeoff. In other words, we would lose the ability to use it before the arrival of the filtering point. This feature can be used to validate recipients and accept E-mails only for valid users as shown in figure 4.12. The external agent can treat a million messages per day.

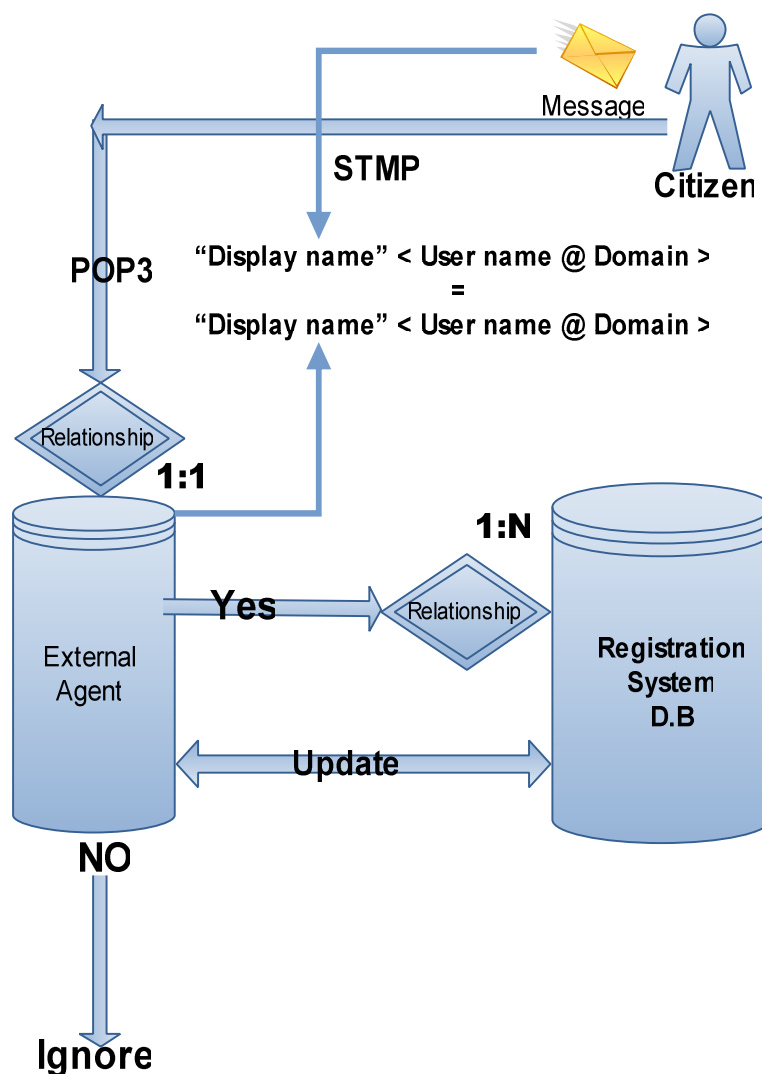


Figure 4.12 Valid Users

4.2.1 The Flowchart of the Proposed Design

In order to understand the way proposed design will precisely work, we need to go through the following diagram and track it from two starting points that lead to the success or failure of the process using the proposed design.

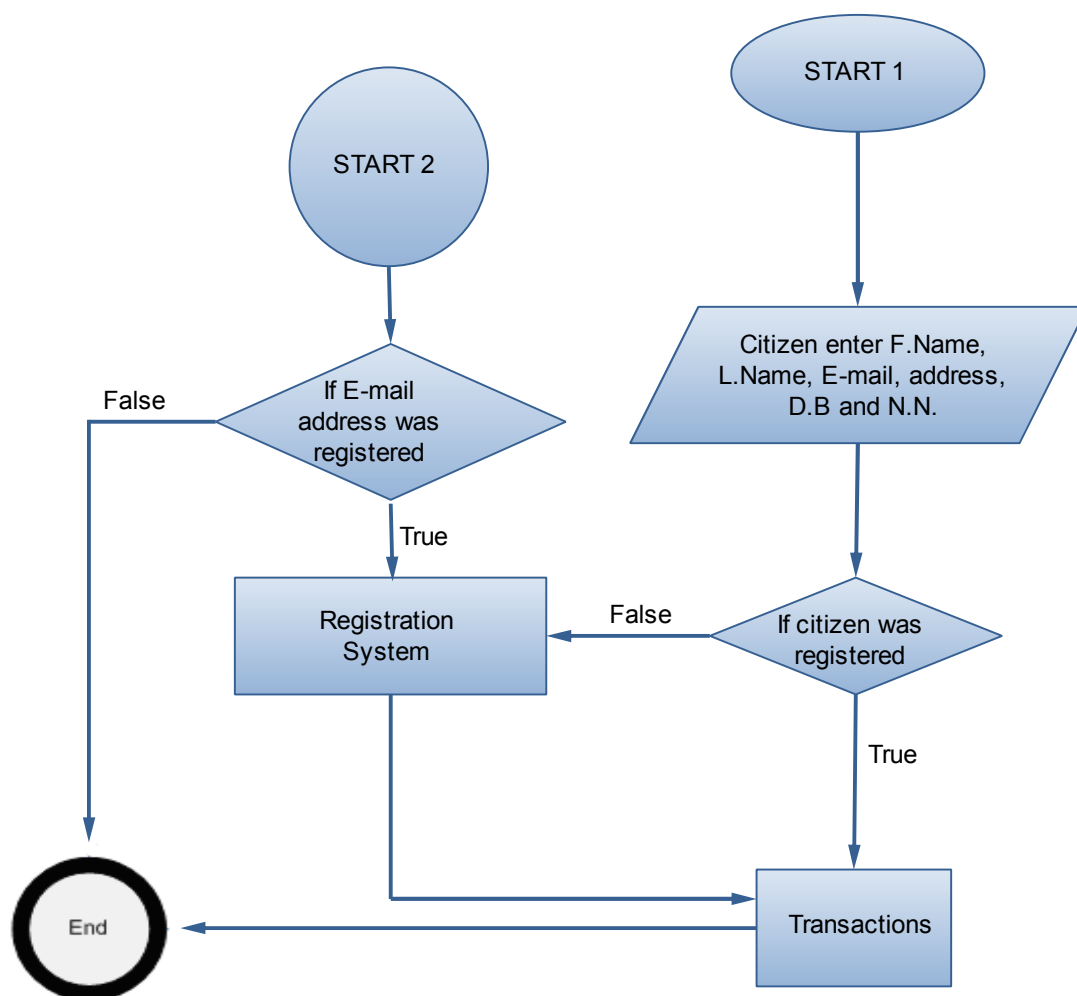


Figure 4.13 Flowchart Diagram for the Proposed Design

4.2.2 Use Case Diagram of the Proposed System

The use case diagram of the proposed system shows the system's use cases and the actor. The following figure 4.14 shows the various user roles and how these roles are uses into system.

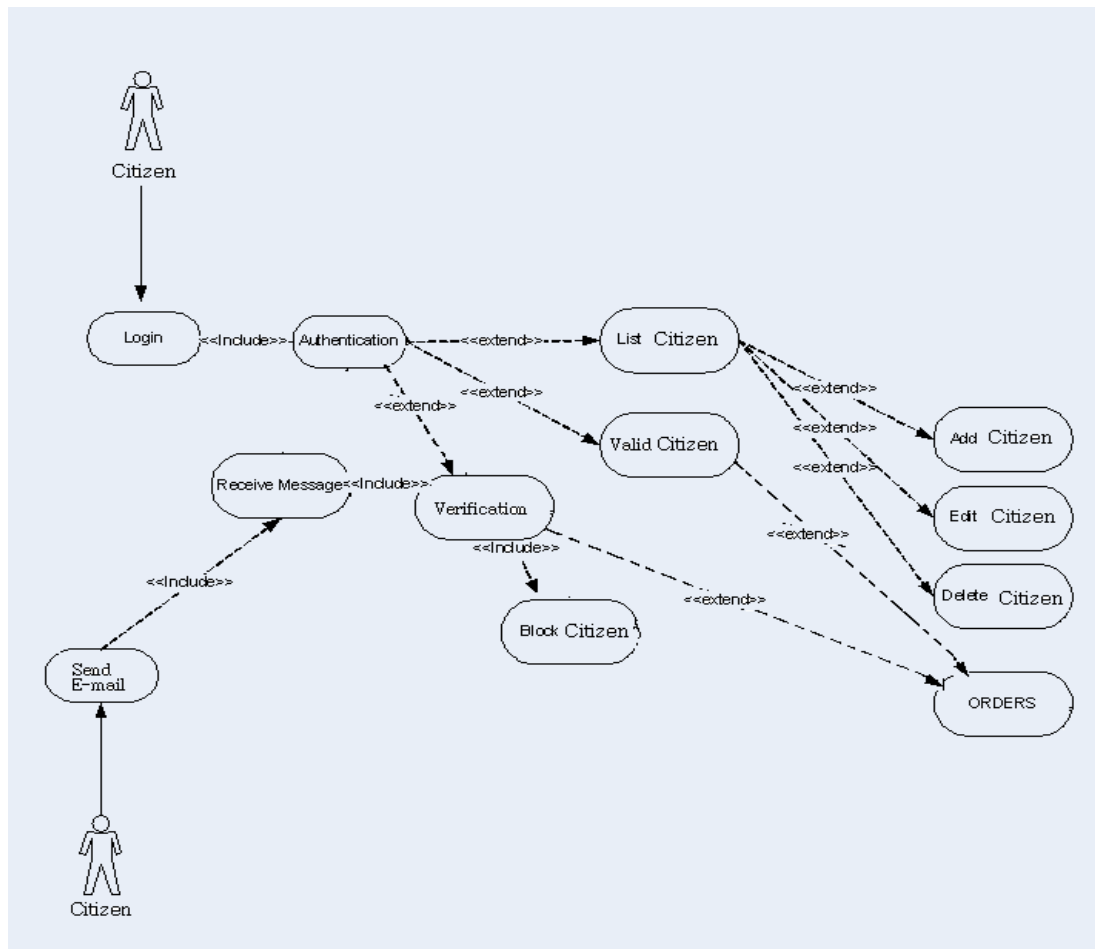


Figure 4.14 Use Case Diagram for the Proposed Design

As a case study, we can verify the proposed design through an example into appendix A.

4.3 New System Analysis

The most common method today is a deceptive E-mail message. The messages that arrive are about the need to collect account information or anything else in order to win the funds by direct or indirect ways, may be is a collection of information about a specific person to strike deals. After applying the proposed solution, the external agent of the system that works to ensure the identity of the sender (Citizen) is shown in figure 4.12, the sender (Citizen) was registered in the registration system or not, if the sender (Citizen) was registered, the message will be inserted into the E-government web without any problem and all transactions will be normal. However, if the sender (Citizen) was not registered, the system will consider this message as phishing, spam or unwanted message ... etc.

The system will reject this message and prevent it from entering. As a result, whole content of the message will be neglected and the system will not allow it to enter. The system also will not allow any deceptive phishing. Moreover, many other scams will be broadcasted to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing into a bogus site, where their confidential information can be collected, and will not enter into an E-government web.

The system will not be allowed to enter malware-based phishing, malware can be introduced as an E-mail attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities, and also the Keyloggers and Screenloggers are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet.

The system will not allow session hijacking describes an attack where users' activities are monitored until they sign into a target account or transaction and establish their bona fide credentials. At that point, the malicious software takes over and can undertake unauthorized actions, such as transferring funds without the user's knowledge. Also, Web Trojans pop up invisibly when users are attempting to log in.

The system will not allow any system's reconfiguration attacks to modify settings on a user's PC for malicious purposes. For example: URLs in a favorite file might be modified to direct users to look alike websites.

The system will not allow any data thefts. Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly, PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, and employee related records,

etc., thieves profit from selling to those who may want to embarrass or cause economic damage to competitors.

Thus, we can say that we could achieve the aim of protecting the E-government E-mail by proposing a design to solve the problem of ensuring the transactions between E-government and citizen are carried out with appropriate security, in an environment where E-government has no control over all websites. Mainly, we can say the problem of verification of the sender (Citizen) was solved, if the sender sends a message from another website.

Chapter 5

Conclusions and Future Work

CHAPTER FIVE

CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

In this section, the researcher presents the conclusions of this research, in addition to the way he has used these final results to contribute in the studied domain.

We focused on studying and analyzing the phishing problem to obtain three main objectives:

1. Preventing phishers, spam and unwanted messages.
2. Encourage citizens by not imposing restrictions on the citizens through facilitating communication in the E-government applications.
3. Citizens can send any messages from their E-mail addresses to do a transaction.

The final results that we found from our research are that the proposed design can be used for Citizen-to-Government (C2G) potential to solve phishing problems.

5.2 Future Work

By working on our thesis step by step, many ideas and issues were appeared but not accomplished yet because of the lack of time, resources, and other constraints. Hence, we would like to suggest the following for future work:

- Applying this design into Jordan E-government in the next phase.
- Using the same design to verify messages that sent to E-government by SMS.
- By creating only one E-mail address under "Supplier" name, all the businessmen and citizens can find the goods that they want to buy without searching for websites.

APPENDIX

APPENDICX

APPENDICX A: An Example of System Proposed



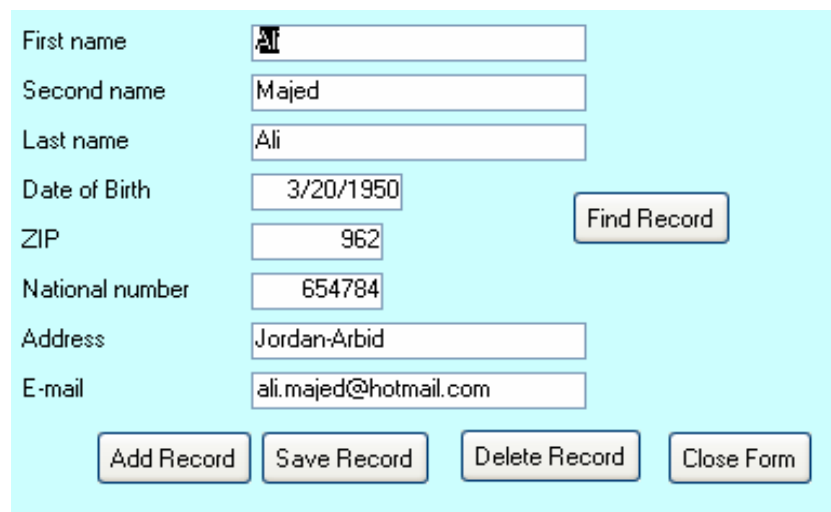
Welcome to E-Government Citizens Registration Process

To Start Registration Process Please [Click Here](#)

To Add New E-mail Please [Click Here](#)

To Close This Form Please [Click Here](#)

Figure 1: Registration System



First name	<input type="text" value="Ali"/>
Second name	<input type="text" value="Majed"/>
Last name	<input type="text" value="Ali"/>
Date of Birth	<input type="text" value="3/20/1950"/>
ZIP	<input type="text" value="962"/>
National number	<input type="text" value="654784"/>
Address	<input type="text" value="Jordan-Arbid"/>
E-mail	<input type="text" value="ali.majed@hotmail.com"/>

[Find Record](#)

[Add Record](#) [Save Record](#) [Delete Record](#) [Close Form](#)

Figure 2: Registration Process

Registration Table : Table								
	First name	Second name	Last name	Date of Birth	ZIP	National numbe	Address	E-ma
▶ +	Ali	Majed	Ali	3/20/1950	962	654784	Jordan-Arbid	ali.majed@hotmail.com
+	Luay	Muhsin	Alzubaidy	5/5/1968	962	764356	Jordan-Amman	luay1970@gmail.com
+	Muhammed	Jafar	Alkaraki	9/20/1982	962	6578342	Jordan-Alkarak	Muhammed82@hotmail.com
+	Yasir	Jassim	Alkarkhi	6/20/1972	962	3452369	Jordan-Madaba	yasir_rasheed72@yahoo.com
+	Yasir	Rasheed	Alkarkhi	6/18/1972	962	1234567	Jordan-Amman	yasirexp@yahoo.com
*					0	0		

Figure 3: Registration Table

E-mail Table : Table	
	E-mail
▶ +	ali.majed@hotmail.com
+	luay1970@gmail.com
+	luay19701@gmail.com
+	Muhammed82@hotmail.com
+	yasir_rasheed72@yahoo.com
+	yasirexp@yahoo.com
+	yasirexp1@yahoo.com
+	yasirexp2@yahoo.com
*	

Figure 4: Email Table

Query1 : Select Query						
E-mail Table		Registratio...				
* E-mail		Date of Birth ZIP National numt Address E-mail				
Field:	E-mail	First name	Second name	Last name	Date of Birth	ZIP
Table:	E-mail Table	Registration Table	Registration Table	Registration Table	Registration Table	Registration Table
Sort:						
Show:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Criteria:						
or:						

Figure 5: Linking E-mail Table with Registration Table

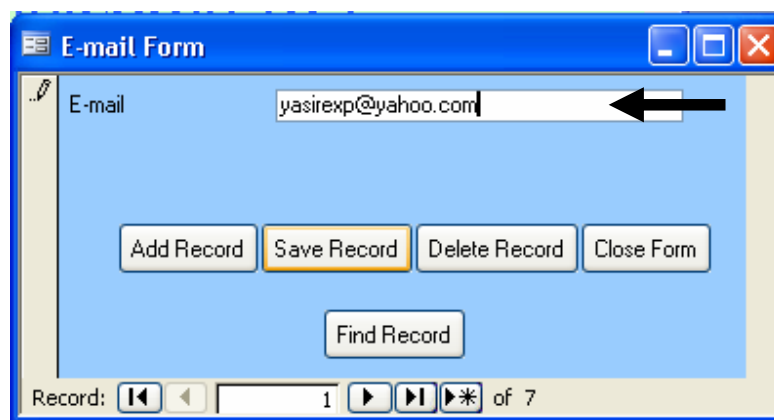


Figure 6: Enter E-mail that already registered

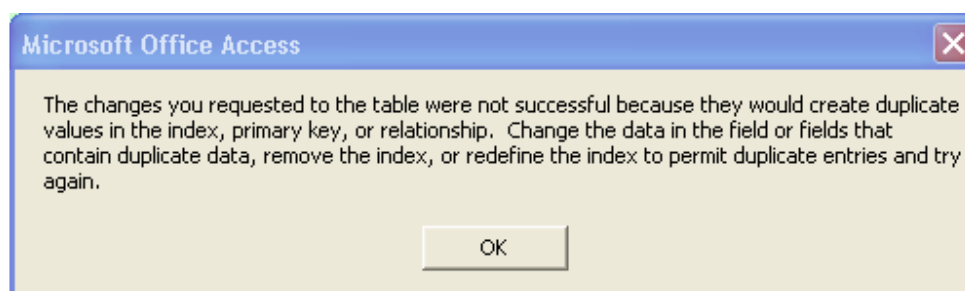


Figure 7: Duplicate

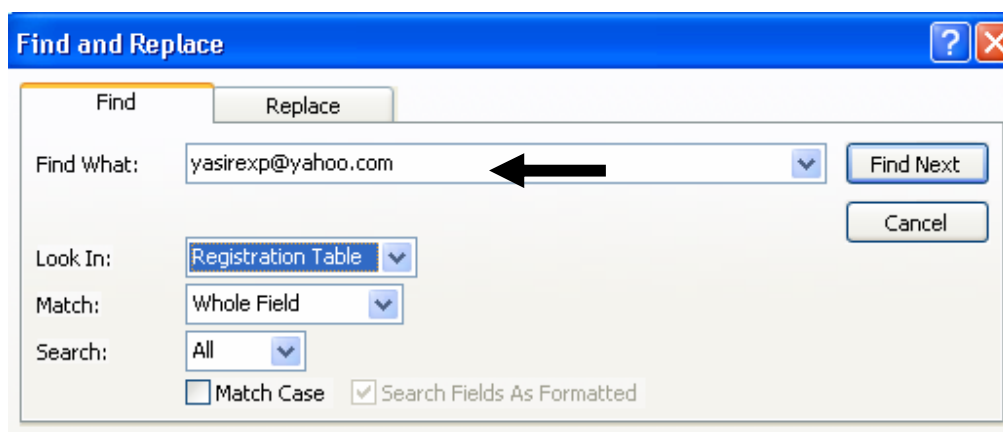


Figure 8: Find E-mail Address

First name	<input type="text" value="Yasir"/>
Second name	<input type="text" value="Rasheed"/>
Last name	<input type="text" value="Alkarkhi"/>
Date of Birth	<input type="text" value="6/18/1972"/>
ZIP	<input type="text" value="962"/>
National number	<input type="text" value="1234567"/>
Address	<input type="text" value="Jordan-Amman"/>
E-mail	<input type="text" value="yasirexp@yahoo.com"/>

Figure 9: Find All Information

APPENDICX B: Comparison of the Proposed Approach with the related works

The table 2.1 present the comparison between the proposed approach and with the most related works that appear how the proposed approach are best to protect E-government E-mail from phishers attacks.

R \C	Operations	Handles
Spam Arrest	Operations on the E-mail	Handles some types of phishers
Sender Address Verification	Operations on the E-mail	Handles some types of phishers
Bluebottle	Operations on the E-mail	Handles some types of phishers
Australian Government E-mail Address Naming Standards and Implementation Guidance	Operations on the E-mail	Handles some types of phishers
Comprehensive Email Filtering	Operations on the E-mail	Handles some types of phishers
Thunderbird Sender Verification Extension	Operations on the E-mail	Handles some types of phishers
Interoperability Program	Operations on the E-mail	Handles some types of phishers
Proposed design	Operations on the E-mail	Handles all types of phishers

Table: Comparison

REFERENCES

REFERENCES

1. Alaa Hussein Al- Hammami, "Standard Specification for the design of a security system to protect the information", Journal of Rafidain University College of Science, second edition, 1999, Baghdad - Iraq.
2. Antiphishing.org, "Crimeware and Phishing" viewed 20 December 2009, <http://www.antiphishing.org/crimeware.html>
3. Arifoglu, A., A. Körnes, A. Yazıcı, M.K. Akgül ve A. Ayvalı (2002), E-Devlet Yolunda Türkiye, Türkiye Bilişim Derneği: Ankara. p.12.
4. Barracuda Networks Inc. (2008). Second release. United States: Barracuda Networks is privately held with its International headquarters in Campbell, Calif. Viewed into 22 March 2010, www.barracudanetworks.com
5. Betsy Joyce "The importance of electronic communication: Where we've been, where we are now, and what's coming - Internet Watch - Brief Article". Public Roads. FindArticles.com. 30 May, 2010. Viewed 2 June 2010, <http://findarticles.com/p/articles>
6. Bluebottle Solutions Pty Ltd, 2006." Bluebottle E-mail". Viewed 20 March 2010, <http://www.bluebottle.com>, 45 Scott St, Beaumaris, Vic 3193
7. Braden; Ginoza; Hagens (2007-11-30). "RFC Document Style". Style Guide. RFC Editor. <http://www.rfc-editor.org/rfc-style-guide/rfc-style-manual-08.txt>. Retrieved 2008-11-24. That refers to terms-online that explicitly requires email spelling.

8. Circle ID, 2004. Sender Address Verification:" Solving the Spam Crisis". Viewed into 22 May 2010, <http://www.circleid.com>.
9. Crocker, D., "Standard for the Format of ARPA Internet Text Messages", STD 11, RFC 822, UDEL, August 1982.
- 10.DCBPA Task Force "Data Center Best Practices and Architecture for the California State University", Oct 7, 2009, DRAFT, Version: 0.4.1. Viewed 12 March 2010 , <http://webcache.googleusercontent.com>
- 11.Erdem R. ERKUL, 2008, "What is e- government, Digital Government (Digital state)?". Viewed in 3 Jan 2010, <http://www.digital-government.net/e-government.html>
- 12.Fountain, J.E. (2005). Central Issues in the Political Development of the Virtual State. The Network Society and the Knowledge Economy; Portugal in the Global Context. Lisbon, March 4-5, 2005 p.2-3.
- 13.Income and Sales Tax Department, The Official Site of the Jordanian E-government, 2010. Viewed 12 January 2010,<http://www.jordan.gov.jo>
- 14.Jim Melitski, The World of E-government and E-governance, 2001. <http://www.aspanet.org/solutions/The World of E-government and E-governance.htm>.
- 15.Josang, Audun et al. . "Security Usability Principles for Vulnerability Analysis and Risk Assessment." (PDF). Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC'07). Viewed 10 February 2009, <http://www.unik.no/people/josang/papers/JAGAM2007-ACSAC.pdf>. Retrieved 2007.

16. Kansas State University, Manhattan, KS, 66506, 785-532-6011, ©2006 Kansas State University, November 5, 2009.

17. Land and Survey, The Official Site of the Jordanian E-government, 2010. Viewed 12 January, <http://www.jordan.gov.jo>

18. Michelle Cristallo, "Australian Government Email Address Naming Standards and Implementation Guidance", February 2008. Viewed 11 October 2009, www.govdex.gov.au.

19. Microsoft Corporation. "What is social engineering?". "Spam Slayer: Do You SpeakSpam? Viewed 21 October 2009, <http://www.microsoft.com/protect/yourself/phishing/engineering.msp> x. Retrieved August 22, 2007.

20. Oxford English Dictionary Online. "'phishing, n." OED Online, March 2006, Oxford University Press.". Viewed 25 June 2009, <http://dictionary.oed.com/cgi/entry/30004304/>. Retrieved August 9, 2006.

21. PCWorld.com "Spam Slayer: Do You SpeakSpam? Viewed 22 May 2009 ". <http://www.pcworld.com/article/id,113431-page,1/article.html>. Retrieved August 16, 2006.

22. PCWorld.com, 2009. Viewed 22 January 2009, <http://www.pcworld.com/article/id,13...y/article.html&>

- Antiphishing.org, 2009. Viewed 22 January 2009, <http://www.antiphishing.org/resources.html>
- 23.Services by the Government of Jordan, The Official Site of the Jordanian E-government, 2010. Viewed 12 January, <http://www.jordan.gov.jo>
- 24.Spam Arrest, 2001,"Protecting mailboxes". Viewed into 24 May 2010, <https://www.spamarrest.com>
- 25.Stamoulis D., Gouscos D., Georgiadis P., Martakos D.,"Revisiting public information management for effective e-government services", Information Management & Computer Security, 2001,Vol. 9 ,Iss. 4, Pag.146 - 153, ISSN: 0968-5227, DOI: 10.1108/09685220110400327, MCB UP Ltd.
- 26.Standards for the Protection of Personal Information of Residents of the Commonwealth, 2010. Viewed in Jan 2010 <http://webcache.googleusercontent.com>
- 27.State of Texas, Department of Information Resources Electronic Government Strategic Plan, January 2001.
- 28.Symantec.com, (©1995 - 2010 Symantec Corporation). Viewed 6 Jan 2010, <http://www.symantec.com>
- 29.Tan, Koon. "Phishing and Spamming via IM (SPIM)". Internet Storm Center. Viewed 25 July 2009, <http://isc.sans.org/diary.php?storyid=1905>. Retrieved December 5, 2006.

30. Tanzania E-government, 2005," Citizen Registration Form" &" Send E-mail Form". viewed 25 October 2009, <http://www.tanzaniagateway.org>
31. Tasha H., "Service Delivery Challenges E-Government Can Tackle ", Dec 2002. Vol. 6, No. 8. Viewed in Oct 2009, <http://webcache.googleusercontent.com>
32. Tasmanian Government Email Address and Username Standards Version 1.1, 7 January 2010. viewed 12 March 2010, http://www.egovernment.tas.gov.au/themes/interoperability/standards_and_guidelines
33. Tauberer J., 2009, Thunderbird Sender Verification Extension," Protect Yourself From Phishing". Viewed into 25 June 2010, <http://razor.occams.info/code/spf/>
34. The Chicago Manual of Style Online "Hyphens, En Dashes, Em Dashes - Q&A".viewed 6 February 2009, http://www.chicagomanualofstyle.org/CMS_FAQ/HyphensEnDashesEmDashes/HyphensEnDashesEmDashes05.html. Retrieved 2008-05-18.
35. The e-Government Imperative: Main Findings, Policy Brief, OECD (2003a), OECD Observer, March 2003.
36. The Official Site of the Jordanian E-government, 2010. viewed 10 January 2010, <http://www.jordan.gov.jo>
37. Theresa A. Pardo "Realizing the Promise of Digital Government: It's More than Building a Web Site", Information Impact, October, 2000.
38. Theresa Pardo, 2002 "Realizing the Promise of Digital Government: It's more than Building a Web Site", Information Impacts Magazine, Vol 17, Issue 2.

39. Tony Long "A Matter of (Wired News) Style", , Wired magazine, 23 October 2000
40. Türkiye Bilişim Derneği (2002), a.g.e, p.22
41. USA E-government, 2010. Viewed 12 March 2010, <http://www.usa.gov/Citizen/Topics/Health/HealthInsurance.shtml>
42. Zhiyuan Fang., E-Government in Digital Era: Concept, Practice, and Development, International Journal of the Computer, the Internet and Management, Vol. 10, No.2, 2002, p 1-22, ISBN: 960-8457-11-4.