

**E-GOVERNMENT SERVICE SECURITY MODEL FOR NUSAJAYA ICT
CENTRE**

Jama Mohamed Jama

UNIVERSITI TEKNOLOGI MALAYSIA

**E-GOVERNMENT SERVICE SECURITY MODEL FOR NUSAJAYA ICT
CENTRE**

JAMA MOHAMED JAMA

A dissertation report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Information Technology – Management)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JUNE 2011

I dedicated this dissertation to my beloved family and my supervisor Assoc. Prof. Dr Othman Bin Ibrahim for their life-time sacrifice, love, encouragement and blessing and special thank goes to my beloved uncles and cousin, Omar Abdi Ali, Abdulrahman Mohamoud Ali and Degan Abdulrahman for their valuable support and assistance.

ACKNOWLEDGEMENT

First and foremost I thank Allah that I am able to complete my Master's research Secondly; I wish to express my sincere appreciation to my supervisor, Assoc. Prof. Dr Othman Bin Ibrahim for his encouragement, Advice and guidance. He inspired me greatly to complete my dissertations and his willing to motivate me contributed tremendously to my research. Thank you for giving me the opportunity to experience this challenging field.

I also would like to thank my respectful examiners for the initial and vive assessments and comments of this research that will keep me encouraged. I would also thankful to technical staffs of ICT Nusajaya for their collaboration. I would also like to express my appreciation to all the lecturers and my colleagues of MSc IT Management programs in UTM Campus Johor Bahru specially FSKSM post Graduate Studies' Lecturers, staff for their support and encouragement. I would also like to express my appreciation to Kak Lijah with her support views and tips.

ABSTRACT

E-government security is considered one of the crucial factors for achieving an advanced stage of government. As the number of e-government services introduced increases, higher level of e-government security is therefore required. In order to provide a highly secured yet responsive and economical access of government service for the citizens, security is seen as the primary goal for businesses and as their trusted partners. Over the past years, security has evolved from technology issues in the government institutions as it also affects the daily security related incidents such as network intrusion, hacking, viruses or denial of services attacks. The participants of this research are ICT technical staff of Nusajaya ICT department in Johor Bahru. Survey questionnaires instrument were chosen as the data collection method to study the risk and threats associated with e-government service and its security measures. The focus of the research relies on how e-government service security will help citizens and analysis the current existing e-government security. Via the initial planning using the suitable methodology for the analysis and design phase guided the research towards the development of proposed model which will help the existing e-government security.

ABSTRAK

Keselamatan E-Kerajaan merupakan salah satu faktor penting bagi mencapai kemajuan pelaksanaan E-Kerajaan. Oleh kerana jumlah perkhidmatan E-Kerajaan yang diperkenalkan kepada pengguna meningkat, maka tahap keselamatan E-Kerajaan yang lebih tinggi amat diperlukan. Bagi menyediakan keselamatan yang tinggi, responsif dan capaian yang menjimatkan terhadap perkhidmatan kerajaan kepada masyarakat, maka keselamatan ini juga menjadi perkara utama terhadap perniagaan dan rakan kongsi lain yang dipercayai. Oleh itu, peserta yang terlibat di dalam kajian ini adalah terdiri daripada kakitangan teknikal di Jabatan ICT Nusajaya Johor Bahru, dan penyelidikan ini adalah untuk mengkaji risiko yang berhubungkait dengan keselamatan perkhidmatan E-Kerajaan. Sepanjang tahun lalu, keselamatan telah berkembang dari isu-isu teknologi dalam kerajaan elektronik, malah agensi kerajaan juga dipengaruhi setiap hari oleh isu keselamatan berkaitan seperti gangguan rangkaian, pencerobohan, virus atau serangan terhadap penolakan perkhidmatan, dan beberapa kejadian telah dilaporkan tetapi kebanyakan daripada masalah tersebut tidak dilaporkan. Semasa kajian ini dijalankan, persoalan penting telah ditumpukan terhadap; bagaimana keselamatan perkhidmatan E-Kerajaan dapat membantu masyarakat, di samping menjalankan analisis terhadap keselamatan E-Kerajaan secara terkini dengan melakukan beberapa tinjauan. Metodologi kajian ini adalah merangkumi aspek perancangan awal, analisis dan rekabentuk pengembangan cadangan model yang dapat membantu keselamatan E-Kerajaan.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xii
	LIST OF APPENDIX	xiii
1	RESEARCH OVERVIEW	1
	1.1. Introduction	1
	1.2. Background of Study	2
	1.3. Problem Statement	4
	1.4. Objectives of the Study	5
	1.5. Research Questions	5
	1.6. Importance of the Study	6
	1.7. Scope of the Study	6
	1.8. Chapter Summary	7
2	LITERATURE REVIEW	8
	2.1. Introduction	8
	2.2. E-government Implementations	9
	2.3. Value of E-governments initiative	11

2.4 Benefits of E-government Initiative	12
2.5 Challenges of E-government	14
2.5.1 Access Issues	15
2.5.2 Technical Issues	15
2.5.3 Human Factors	15
2.5.4 Service Delivery Issues	16
2.5.5 Delivery Integrated Services	16
2.5.6 Resource Issues	17
2.5.7 Other Issues	17
2.6 Security of E-government Service	18
2.6.1 E-Government Security: a Citizen's Perspective	19
2.6.2 The Government's Perspective	19
2.6.3 Constituents of Trust in E-government	20
2.6.4 Domain of Trust in E-government	20
2.7 Importance of Security in E-government	21
2.7.1 Information Intercepting	21
2.7.2 Information Tampering	22
2.7.3 Services Denying	22
2.7.4 Information Faking	22
2.8 Common Security Principals in E-government	23
2.9 Procedure of Risk Analysis in E-government	25
2.9.1 Risk Identifying	25
2.9.2 Risk Analysis	26
2.9.3 Risk Controlling	29
2.10 Model of E-government Service Security	30
2.10.1 User Environment of E-government	32
2.10.1.1 Identity Management System	33
2.10.1.2 Access Management Systems	33
2.10.1.3 Interaction Management System	34
2.10.2 Transport Environment of E-government	37
2.10.3 ICT Assets Environments	38
2.11 E-government Security Management Framework	40

2.12	Threats to E-government Services and Clients	42
2.12.1	E-government Service Assets	43
2.12.2	Internal Sources of Threat	44
2.12.3	External Sources of Threat	45
2.13	Service Security Environment of E-government	46
2.13.1	Environment Assumptions	46
2.13.2	Domain Model	46
2.13.3	External Security Policy Framework	47
2.14	Tools of Maintaining Information Security in E-government	47
2.14.1	Steganography	49
2.14.2	Steganalysis	51
2.15	Risk Factors of E-government	51
2.15.1	External & Internal barrier of E-government Implementation	52
2.15.2	Budget Barrier	53
2.15.3	Common Technical Frameworks and Infrastructure	54
2.15.4	Digital Divided	54
2.15.5	Privacy and Security Concerns	55
2.15.6	Rapid Technology Change	55
2.15.7	Citizen Expectation and Seamless Services	55
2.16	Discussions	56
2.16.1	Implementations of E-government	56
2.17	Chapter Summary	57
3	RESEARCH METHODOLOGY	58
3.1	Introduction	58
3.2	Research Strategy	59
3.2.1	Qualitative Research	59
3.3	Operational Framework	60
3.4	Data Collection	65
3.4.1	Primary Data	65
3.4.2	Secondary Data	66
3.5	Sampling and Respondents	66

	3.6 Data Analysis	67
	3.7 Project Validity and Reliability	67
	3.7.1 Reliability	68
	3.8 Project Schedule	68
	3.9 Chapter Summary	69
4	DATA COLLECTION DATA ANALYSIS	70
	4.1. Introduction	70
	4.2. Survey Analysis	71
	4.2.1. Survey Findings	72
	4.3. Respondent's Profile	73
	4.4. Identifying Risk and Importance in E-government Security	75
	4.5. Recommendation on E-government Service Security	83
	4.6 Chapter Summary	85
5	E-GOVERNMENT SERVICE SECURITY MODEL FOR NUSAJAYA ICT CENTRE	86
	5.1 Introduction	86
	5.2 Analysis of Existing Model and Framework of E-government Security	87
	5.3. Derivation of Proposed Model	90
	5.4. The Proposed Model	91
	5.4.1 E-government Users	92
	5.4.2 Process	93
	5.4.3 Technology	94
	5.4.4 Security Components	94
	5.4.5 E-government Application Services	97
	5.5. User Acceptance Test of the Proposed Model	99
	5.6. Chapter Summary	103
6	DISCUSSION AND CONCLUSION	104
	6.1 Introduction	104
	6.2 Achievements	105
	6.3 Recommendation of How to Use the Proposed Model	106

6.4 Constraints and Challenges	106
6.5 Aspirations	107
6.6 Chapter Summary	108
REFERENCES	109
APPENDIX A	112
APPENDIX B	113
APPENDIX C	121

LIST OF TABLES

TABLE	TITLE	PAGE
Table 2.1:	Possible Threat Sources	27
Table 2.2:	Definition of Risk Probability	29
Table 2.3:	Description of the Model	32
Table 2.4:	User Management Components	35
Table 2.5:	Secure Communication System	38
Table 2.6:	ICT Component Management	39
Table 2.7:	Security Management Framework	41
Table 3.1:	Details of Operational Framework	62
Table 4.1:	Gender Profile	72
Table 4.2:	Risk on E-government Services Delivery	76
Table 4.3:	Cyber Crimes Against Assets	77
Table 4.4:	Cyber crimes against government assets and states	78
Table 4.5:	Security Components Appropriate of E-government Service	79
Table 4.6:	Security Technology in E-government	80
Table 4.7:	Security Components and Activities	81
Table 4.8:	Methods of Securing E-government website	82
Table 5.1:	Analysis of Existing Model in E-government Service Security	88
Table 5.2:	Users Required Process	93
Table 5.3:	Security Components	94
Table 5.4:	ICT Security Components	96
Table 5.5:	Current E-government Applications	98
Table 5.6:	Verifying the Completeness of the Model	100
Table 5.7:	Verifying the Consistency of the Proposed Model	101
Table 5.8:	Benefits of the Proposed Model for Nusajaya ICT Centre	102

LISTE OF FIGURES

FIGURE NO	LIST OF FIGURES	PAGE
Figure 2.1:	E-government Implementations	10
Figure 2.2:	E-government Security Model	31
Figure 2.3:	Framework of Security Management	40
Figure 3.1:	Project Operational Framework	61
Figure 4.1:	Gender Profile	73
Figure 4.2:	Respondents Age	73
Figure 4.3:	Respondent's Usage of e-Government Service	75
Figure 4.4:	Utilization of E-government Security Technology	83
Figure 4.5:	Any Related Security Technology E-government Service	84
Figure 5.1:	Proposed Model of e-Government Service Security	92
Figure 5.2:	Verifying the Completeness of the Model	100
Figure 5.3:	Verifying the Consistency of the Proposed Model for Nusajaya centre	101
Figure 5.4:	The benefits of the Proposed Model Nusajaya ICT Centre	102

APPENDIX	TITLE	PAGE
Appendix A	Gantt chart	112
Appendix B	Sample of Survey	113
Appendix C	Sample of Questionnaires for User Acceptance Test	121

CHAPTER 1

RESEARCH OVERVIEW

1.1 Introduction

The implementation of e-government service security framework is considered as one of the most important elements of government policy. It is designed with an aim of protection mechanisms for the government transactions over the Information Communication Technology (ICT). For several decades, governments have increased their level of protection for enhancement of efficiency and effectiveness on the functions. Therefore, security is still the key demand with high expectations of government to promote their defense systems to both internal and external threats in near future.

The major goal of security in e-government is to minimize the risks associated with the government transactions that based on electronically networking.

The measurement for security risk management in e-government includes: risk highlighting, risk analyzing and risk controlling that included in the popularity of computer network technology.

Eventually, there are no specific rules for e-government risk management, but it's required an initial scan and detect on both internal and external environment of e-government systems that include a further checking on the weakness of the system. Apparently, that follows a complete analysis of e-government security risk and then relevant security plan and measurements. Following that, tracking and monitor those predefined plan for the initial implementation stage will be added as in important task and finally adjustment on the risk management that involved any time based on environment changes and draw advance disaster recovery plan. Considering the essence of e-government security, it is therefore urgent to dispose on whole effective and purpose countermeasures which is to minimize the potential risk and security bugs.

1.2 Background of the Study

E-government security provides benefits to the citizens and to public administrators at a number of levels. At its most basic level, e-government can connect modern technologies to enable the departments achieve efficiency. One of the most important issues that need to be addressed in e-government technology is to apply security measures which are mainly to increase the government productivity, accuracy, privacy and efficiency in business administrative operations. To achieve the overall mission, set security measure and defense to protect the e-government activities is crucially needed. It is mainly because, government's assets are easy transferred by hackers, networking intrusions and viruses and also any possible threats that may have likely to happen. So, security measures are aimed to deliver

government services in electronic version safely. To support the purpose of the research, numerous studies on the effects of risk in e-government have been published. Studies showed that the number of risks associates the e-government are highly increasing every year, due to the inadequate security measures.

There are scopes for even greater efficiencies in the future through greater sharing of processes within and between departments. Of all the security methods and issue that are common in e-commerce is understood can also be used to e-government risk management subject, but e-government is different because it has direct network access to each other that is much better than business networks because most of them are linked for passing, transferring and sharing information. Moreover, business network accesses are competitors where they don't allow their sensitive information to be shared publicity. The importance of e-government is to use electronic information technology to break boundary of government administrative organization to have virtual electronic government security (Kaur, 2003).

Accesses have been government's main target for the people towards information and service communication and delivery to each other through different kind of electronic media of both internal and external government organizations. However, there are still many problems in e-government services exposed to the spread of computer network technology and information sharing. Due to that problem, security became an important factor as result of fast development and e-government systems.

1.3 Problem Statement

In the e-government security development, which is mainly based on internet faces constant security problem due the complicated and vulnerability of the network. It is the complete invalidation of the network and server systems of increasing or growing risk. Its often comes from attacks of the hackers, viruses, stealing and manmade destruction of the device.

Nusajaya ICT department has experienced a dramatic risk growth in e-government fields which became the key issues of the government security committees. E-government related risks are happening all the time and some cases are receiving significant publicity. The range of incidents varies in greatly and can include events such as network intrusion, viruses, and denial of services or identity thefts.

Given the situations, it's the suitable period that the associated with governments, to take serious efforts in studying the possible dangers of risks in e-governments that may arises in the form of this useful technology. Many developed nations have not only invested into research programs to study the effects of risk in e-governments but also shared with public on the research findings on how the risks can affect the electronic governments operations in general.

E-government services face a lot of security problem such as: identity theft, hacking and denial of service. These aspects are related with e-government users, or invader who steals the information from the government or other users. So, protecting the citizen's privacy, security and giving them assurance that their information will be violated or changed became the important aspect of service success. It is to avoid the mass retention of e-service user of e-government.

Apart from the studies conducted on the short term effects of the e-government risk security, there is a growing need to determine direct security association of government operations. Recently, investigation done showed that the issues on security risk is increasing more and more, where unauthorized user are keen to steal the properties of the government. Hence, e-government security became a strategic approach to protect both internal and external threats.

1.4 Objectives of the Study

In order to achieve the objectives of the research, researcher has listed here below:

- i. To study the e-Government risks and threats.
- ii. To identify e-government security dimensions and methods that can be managed in e-government services.
- iii. To propose an effective e-Government service security model in order to improve security measures.

1.5 Research Questions

The research questions are:

- i. What is the security issue in e-government service elements?
- ii. What are the elements of risk analysis?
- iii. How risk and threats can be minimized in e-government services?

1.6 Importance of the Study

Due to the problems that dwell with the increases for e-government service both internal and external activities in Nusajaya ICT, this study expresses risk of e-government services and security methods that is used today. The e-government security service is a process of measuring security to e-government service and keeps track on user's demand and government online performance.

Findings of this study will help both authority and customers to identify e-government risk and source of threats and notices e-government security risk so that user and authority may have experience to investigate publicly and raise public level awareness and more extensive studies have be planned in the near future.

1.7 Scope of the Study

In order to achieve the scope of the study, researcher has selected sample of respondents. The respondent of this research study will be the technical staffs in Nusajaya, in ICT department in Johor Bahru who has basic and wide knowledge and background of e-government service will be respectively selected. This study is believed will improve the existing securities of e-government accessibility including delivery of e-government services to its end users.

1.8 Chapter Summary

This chapter provides a brief description about e-government security and risk associated with e-government systems. The researcher has strived hard to understand the problems and risks on security measurements in the e-governments service systems. The problem statement gives clear guidelines for identifying the research questions and research objectives, altogether drawn the scope of the research and finally the importance of the study was briefly discussed.