Sudan University of Science & Technology

College of Postgraduate Studies

College of Computer Science & Information Technology

Developing an Approach for Securing E-government Accessibility

تطوير إسلوب للنفاذ الآمن للحكومة الإلكترونية

A dissertation submitted in the fulfillment of the requirements for the award of the degree of

Doctor of Philosophy (Computer Science)

By:

Rasha GalalEldin Hassan Mohamed

Supervisor:

Prof. Dr. Othman O. Khalifa

Dec., 2017

DEDICATION

To my parents who are continuously support me.
To Bayan College of science and Technology, the body who really helped me and encouraged me to go further.
To Prof. Izzeldin Mohammed Osman, the founder of Computer Science PhD program by Taught Courses and research in Sudan University of Science and Technology.

AKNOWLEDGMENT

I thank God and my friends for their help and support. I am thankful to my supervisor Prof. Dr. Othman O. Khalifa for his tremendous help, support, guide, feedback and encouragement throughout the research and during my PhD study.
I would like to express my deep gratitude to Prof. Dr. Aisha Hassan Abdallah; she has been a great source of assistance. Deepest thanks are extended to all Bayan College staff.
Also I can never forget my parents and all my family for their helpful and patient for my faults throughout my life.

Abstract

E-government applications are developed under ICT to serve citizens and other stakeholders with all governmental services electronically. All nations strive to deploy E-government in an effective and efficient way. E-government security is considered one of the crucial factors for achieving an advanced stage of e-government. As the number of e-government services introduced to the user increases, a higher level of e-government security is required. However, threats and risks are increased as will. Attackers explore and exploit the vulnerabilities found in Internet platform application, then seek holes for falsification, forged and spoofed identity, hence most of security issues to gain access of protected systems.

The research conducted a mix-method systematic qualitative and quantitative research, A case study strategy is conducted to find facts that can assist Sudan e-government initiatives for best citizen's adoption, case study findings assist in developing the proposed solution.

This work proposed a framework to develop a secure communication in E-government for authentication on the application layer. The solution will serve to provide trusteeship through insure and verify the identity of stakeholders who use governmental electronic services, this research propose an authentication framework in an appropriate approach to secure e-government, where this approach might need to encompasses multi-model of security to work in efficient security environment, that compromises both of technical and non-technical issues and to be applied.

This research contribute to empirical and theoretical knowledge, where the research study the weakness in e-government environment, and implement a model to secure login for the most sensitive Internet-based e-government services, this is done using a hybrid biometric fingerprint and digital signature, to tight accessibility to e-government and provide security in depth strategy. The model is testing using penetration testing which yield a positive results against the major types of web application attacks.

تمهيد:

تطور تطبيقات الحكومة الإلكترونية تحت تكنولوجيا المعلومات والاتصالات لخدمة المواطنين وأصحاب المصلحة الآخرين مع جميع الخدمات الحكومية إلكترونيا. وتسعى جميع الدول إلى نشر الحكومة الإلكترونية بطريقة مؤثرة وفعالة. ويعتبر أمن الحكومة الإلكترونية أحد العوامل الحاسمة لتحقيق مرحلة متقدمة من الحكومة الإلكترونية. ومع ازدياد عدد خدمات الحكومة الالكترونية المقدمة للمستخدم، يلزم وجود مستوى أعلى من الأمن الحكومي الالكتروني. ومع ذلك، تزداد التهديدات والمخاطر كثيرا. يقوم المهاجمين باستكشاف واستغلال نقاط الضعف الموجودة في تطبيقات الإنترنت، ثم يسعى لتزوير الهوية والانتحال، وبالتالي ينتهك معظم القضايا الأمنية للوصول إلى النظم المحمية. وقد أجري البحث منهجا بحثيا وكميا و منهجا مختلطا، وقد تم إجراء إستراتيجية دراسة حالة لإيجاد الحقائق التي يمكن أن تساعد مبادرات الحكومة الإلكترونية في السودان من أجل تبني مستوى أفضل للمواطن، وتساعد نتائج دراسة الحالة في تطوير الحل المقترح.

واقترح هذا العمل إطارا لتطوير اتصال آمن في الحكومة الإلكترونية من أجل المصادقة على طبقة التطبيق. وسيعمل هذا الحل على توفير الوصاية من خلال التأكد من هوية أصحاب المصلحة الذين يستخدمون الخدمات الإلكترونية الحكومية والتحقق من هويتهم، ويقترح هذا البحث إطارا للتوثيق في نهج مناسب لتأمين الحكومة الإلكترونية، حيث قد يحتاج هذا النهج إلى أن يشمل نموذجا متعدد الأمن للعمل في بيئة أمنية فعالة، مما ينفع المسائل التقنية وغير التقنية.

ويسهم هذا البحث في المعرفة التجريبية والنظرية، حيث تقدم الدراسة البحثية نقاط الضعف في بيئة الحكومة الإلكترونية، وتم تنفيذ نموذج تسجيل دخول آمن لخدمات الحكومة الإلكترونية على شبكة الإنترنت الأكثر حساسية، ويتم ذلك باستخدام بصمات الاصابع الهجينة والتوقيع الرقمي ، و ذلك لتمكين الوصول اللى الحكومة الإلكترونية وتوفير الأمن في استراتيجية اعمق. تم اختبار النموذج باستخدام اختبار الاختراق التي نتج عنه نتائج إيجابية ضد أنواع رئيسية من الهجمات في تطبيقات الويب.

Table of Contents

List of Tables:

List of Figures:

List of Abbreviations:

AED	Advanced Encryption Standard
ATM	Automated Teller Machines
BCEA	Barriers Challenges E-Gov Adoption
BLP	Bell-LaPadula
BYOD	Bring Your Own Device
CA	Certification Authority
CER	Crossover Error Rate
CERT	Computer Event Response Team
CP	Cultures and Privacy
CPU	Central Processing Unit
DI	Demographic Information
DNA	Deoxyribonucleic Acid
DOI	Diffusion of Innovation
DSA	Digital Signature Algorithm
DSC	Digital Signature Certificates
ECDSA	Elliptic Curve Digital Signature Algorithm
ED	E-gov Development
E-Democracy	Electronic Democracy
eGMMs	e-Government Maturity Models
e-Gov	Electronic Government
e-GUSM	e-Government Unified Security Model
E-Management	Electronic Management
E-Management	Electronic Management
E-Policy	Electronic Policy
E-Services	Electronic Services
FAR	False Acceptance Rate
FRR	False Rejection Rate
G&B	Government and Business/commerce
G&C	Government and Citizens
G&G	Government agencies
G&H	Government and Households
HTML	Hyper Text Markup Language
IaaS	Infrastructure as a Service
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IP	Internet Protocol
MCDM	Multi-criteria Decision Making
MD	Message-Digest

M-Government	Mobile-Government
MM	Motivational Model
MPCU	Model of PC Utilization
NGOs	Non-Government Organization
NIC	National Information Center
OWASP	Open Web Application Security
PaaS	Platform as a Service
PKI	Public Key Infrastructure
PKI	Public Key Infrastructure
RAM	Random Access Memory
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest-Shamir Adleman
SaaS	Software as a Service
SCT	Social Cognitive Theory
SEE	Security Experience in E-government
SHA	Secure Hash Algorithm
SOC	Security Operation Centre
SPSS	Statistical Package for Social Sciences
SQL	Structured Query Language
TAM	Technology Acceptance Model
TCP	Transmission Control Protocol
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
UAPA	Users Awareness Perceptions and Attitudes
UTAUT	Unified Theory of Acceptance and Use of Technology
XSS	Cross-Site Scripting

List of Appendices:

CHAPTER I

Introduction

1.1. Introduction:

Today almost all organizations have improved their performance through allowing more information exchange within their organization as well as between their distributers, suppliers, and customers using web support.

E-government is the application of Information and Communication Technology (ICT) - which is a study of developing and using technology to process information and aid communication - by government agencies and citizens.

Securing e-government contribute directly in the trust formation between citizens and government, online communications differ than face-to-face communication this may lead to impersonate someone identity and gain unauthorized access of information, while information might be sensitive and the resulted attack compromise the country reputation.

This dissertation is encompasses all security issues that compromise E-government accessibility and walks through technical issues and non-technical issues which was done using Case Study in Sudan E-government, in addition to survey on the existing non-technical and technical models to produce a general authentication framework.

This chapter aims to provide the reader a background about E-government and Network Security fields, it is also addresses the research challenge being conducted in the real world that form the problem statement which yield from these fields, moreover stating dissertation objectives, research scope and the structure of dissertation outlines.

The research of this dissertation Reviews E-government Services benefits (Jensen , Sherry , 2010) and threats that may e-governments face and the need for secure transaction services for applications (Alexander , 2003), where some of the security issues in e-Government are discussed. Moreover creation framework for establishing digital identities – A key component for establishing security and trust for ICT applications in public networks such as the Internet (Henriksson, 2006).

The research also addresses the requirements of secure access of e-government through authenticity of communication partner (Malik, 2011) and Confidentiality which refer to ensuring that no unauthorised third parties can gain knowledge of the transferred data, and much more issues. In addition to these issues ensuring security of e-government applications and infrastructures is crucial to maintain trust among e-government users (Sofia, 2009).

The research spotted light on existing applications of e-government and provided security Electronic voting (Dominique et al, 2007), e-government transaction such as retrieving driving citations (Amina, Omaima ,2009), e-passport (Luca , Dario ,2014) and security issues that may these application compromise. Evaluate the degree of security of e-Gov we need to examine regulations or/and sometimes security policy and a model as a security measure (Mohammad, Hamdan, 2012)(Irfan, Junseok, 2010)(Geoffrey, 2012)(Geoffrey et al,).

The research argued about the use of Biometrics and Security in E-government ensure identity and authentication of citizen (Piyush et al.,2012), Identification is a prerequisite, with each user required to proffer an identifier (ID) that is included in the authorization lists of the system to be accessed. Moreover the use of digital signature in E-government it is very important to confirm identity of both sides of communication and prevent unauthorized users from destructing documents (Sharifi et al, 2004)

Dealing with digital era is evolving with risks, and the need for security will arise due to the increased amount of risks, these risks are threatened the valuable information, once these information will belonging to government, and information available on digital environment, hence the governmental information are always compromise.

The research concerns about secure access to e-government, which is considered as the fundamental issue in security. Secure access provide better communication access, hence all parties in the communication need to authenticate each other and because there are no a physical identities this will increase the space of spoofing, impersonate, and fraud of identities.

1.2. Background:

Electronic government (e-government) or e-Gov is the use ICT tools and applications, wither it was internet-based or non-internet based to make better interaction through different delivery models and activities between government and citizens (G2C), government and business/commerce (G2B), between government agencies (G2G), or government and Households (G2H) (Valentina ,2004), but it may face a number of limitations that affect the way of interaction.

Figure1.1 illustrates agencies as a service provider and how information flow citizens. (United Nations, 2012)

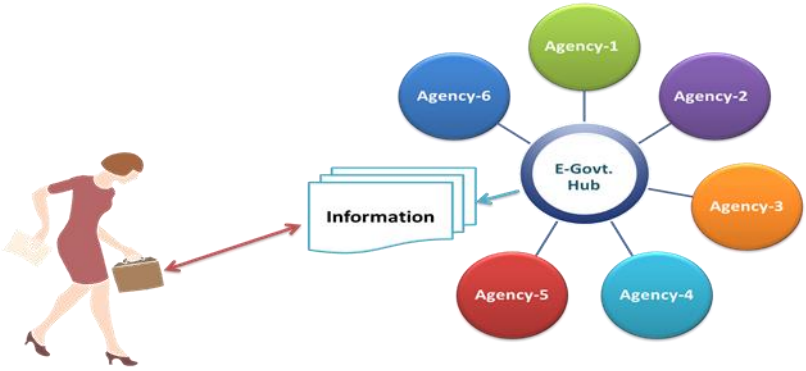

Figure 1. 1:Typical E-Government Architecture Model

Electronic Government applications range from electronic portals developed to provide basic information or services to citizens, to applications to electronic voting, and citizen participation in the rule-making process. A recent review to the emerging literature in electronic government suggests that the diversity of E-Government applications can be grouped in 4 main categories:

- Electronic Services (E-Services),
- Electronic Management (E-Management),
- Electronic Democracy (E-Democracy),
- and Electronic Policy (E-Policy).

E-Services applications are those relating to the delivery of information or services to the citizen. Desirable features of these applications are the organization of the information according to the "customer profile", the capability to allow a "customizable" experience, and the ability to "make transparent" to the user the agency or level of government. The main issues from the security point of view are the verification of the identity of the server computer (Authentication), the integrity of the message, confidentiality, and the privacy associated with the transmission of the information. Although the authentication of the user is also desirable, simple user authentication mechanisms such as passwords are cost-effective for most of these applications, however nowadays it will easy attack.

E-Management applications include those related to the improvement of government internal operations inside a single instance of government or across agencies. Many of these applications require a significant change in government

processes, including a more intense interaction among government agencies through database integration or intercommunication. Protecting the integrity of data, guaranteeing the privacy of the citizens, and controlling the access to data only to the authorized agents are undoubtedly the most relevant security issues in this kind of applications. The integration of databases calls for a clear definition of information ownership and access. Finally, for transactions and services among government agencies and private corporations such as procurement, authentication and non-repudiation becomes important issues (Gil-Garcia et al, 2007).

E-Democracy is mostly associated with electronic voting, but it is also associated with citizen participation in the processes of policy making, promoting and preserving the democratic values. These applications pose the most complex set of security concerns for their successful implementation. E-Democracy applications must include the same elements of security associated with E-services in terms of authentication, integrity, confidentiality, and privacy of the communications. However, some applications call for better approaches to user authentication while assuring their anonymity.

Finally, E-Policy is related to the design of public policies that facilitate and promote the development of the information society. Technology is changing the structure of social organizations and their interaction. This new structures require an adjusted policy framework to facilitate the interaction and promote democracy and equal opportunities to the different constituencies. Here we can think that policy about privacy and access to the information, and the tension associated with these two important issues are the key elements for E-Policy. Monitoring of Internet transactions by some government agencies provides a good example of the tension between these values. On one hand, privacy concerns of Internet users create pressures to reduce monitoring to a minimal level. On the other hand, threats to security breaches promote a closer monitoring of the activity.

All these issues associated with providing security, because the growth of using Internet through information revolution, risks are increased and the need for security is become the most important thing to protect our valuable assets and to build trusteeship, therefore “Information security” the field arises to concern about providing security for the technical risks – including host security, network security

and Internet security - and non-technical risks – including human attitudes, ethical issues, physical assets and also natural disasters – this field is always seek to provide *confidentiality, authentication, availability and integrity* of information.

Privacy and security of information is a priority issue in dealing with E-government:

1.1.1. most of e-government applications depend on Internet to deliver a widen service for citizen, the increased transparency and easier access will considered as an advantage, on the other hand it will raise a significant issue risks will increased because there are vulnerabilities (RabahAlshboul,2012), however if the vulnerability been known there will be a mechanism to recover it otherwise it will exploited by attackers.

1.1.2. E-government needs to store detailed information about all citizens' profiles; this sensitive information might be used by attackers which yield a potential exposure to *confidentiality*, or even information being modified in an unexpected way to produce lack of *integrity* (Shailendra ,2011).

1.1.3. A problem arises when someone wants to verify and *authenticate* the owner of – information/object - and sometimes vice versa in order to access some information in e- government application (ZHOU,2012) such as e-voting (DimitriosZissis, DimitriosLekkas, 2011), e-passports (Luca , Dario ,2014) or e-transactions (Amina, Omaima ,2009) through the e-government portal.

1.1.4. A breach of security may be compromised to yield lack of *availability* of information to citizen, where majority of e-government projects in developing countries fail (Danish ,2006).

The importance of providing security in e-government, comes after those security holes found on TCP/IP network layers and other vulnerable resources wither it was technical or non-technical, or even deployment of inadequate security standards and cyber regulations, moreover there is no standard mechanism to detect vulnerabilities, where vulnerability might be known or the worst case unknown.

Security is a process; no one static standard can assure adequate security because the threats to the security of a site are constantly evolving. Still, government policy makers need to take measures to protect data from destruction, loss, misuse, or alteration. These measures involve both managerial and technical measures. In addition, the measures should be appropriate to the circumstances (e.g. health records of individuals must be afforded greater security than the typical information submitted). An electronic government web site need not have to fully describe the security measures taken to protect consumer's information. Detailed disclosures could confuse citizen/consumers and invite security breaches. Yet, some disclosures of security measures are necessary to enhance consumer's trust in the privacy of their information. Specifically, Web sites should post disclosures about security that specifically address the fact that measures are taken after receipt of consumer's personal data (Aly, 2003). In particular, Web sites should disclose basic data security systems, and retention processes. This could include an explanation of how third parties must safeguard the information and an assurance about the integrity of security measures.

Access critical information:

The ability to restrict access of certain users will mitigate risks indeed, grant access rights to those only how authorised to get information with read/write permission policy, hence sensitive information should kept in highly secure way.

Authentication is one way to verify ones identity and to insure that this user has the right to access of information, Figure 1.2 shows that the need for secure relation between citizens and agencies through e-government.

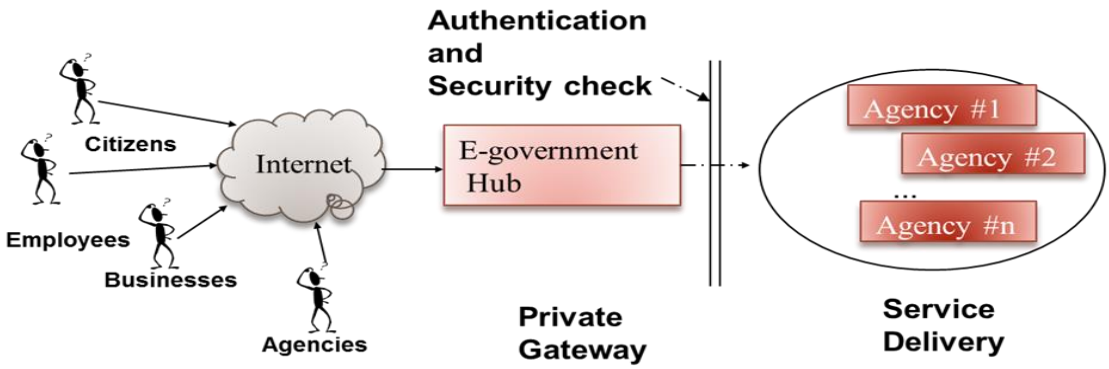

Figure 1. 3: securing service delivery

Attackers always targeting information as the most important component of information systems through what is called “cybercrime”, a number of threats been found in the emerging technologies, such as social media, cloud computing, smart phone technology(J. Jang-Jaccard, S.Nepal, 2014), etc., and understanding all vulnerabilities in exiting technologies in order to be covered will become a great challenge.

The need for e-government in Sudan adoptions reshape the public sector activities and processes, building relation between citizens and the government, enhancing transparency and increasing government capacity. Sudan E-Government still need more work to adopt and implement E-Government project. (Quanxi, Elhadi , 2014) Meanwhile readiness and e-government adoption processes should encompasses security issues as will.

1.3. Research Problem & its significant:

E-Government services face a lot of security problem such as: identity theft, hacking, denial of service and even more attacks. 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 not be violated or changed became the important aspect of service success, hence it’s often comes from attacks of the hackers, viruses, stealing and manmade destruction of the device.

Attackers explore and exploit the vulnerabilities found in Internet platform application, while e-government is Internet-based application hence vulnerabilities are always there, moreover Absence of laid down security policy and lack of risk assessment encourages attackers to seek backdoors even the systems protected. Falsification, forged and spoofed identity, hence most of security issues.

E-government in Sudan are taken a great steps to be adopted and security has an important role in trust formation of citizens and their adoption of e-government, so designing and implementing more effective approaches for securing access of E-government is an important issue, because, the governmental information is usually so sensitive. Even lack of citizen awareness and participation in E-Government

Implementation particularly to trust and deal with ICT technology to send and receive information or in other words to use it for fulfilling their governmental services. The main reason behind E-Government project failure in developing countries is gap experienced between the design and reality implementation of information system. If e-government systems design and implementation take these issues in consideration, we can build a useful e-government systems and gain citizens trust.

1.4. The motivation around this research:

E-government reediness and adoption are facing a lot of challenges these challenges are the motivation around this research and this is to gain the following:

- Be part of the emerging global knowledge based economy and society.
- Interaction with the developing e-governments worldwide.
- Accelerate social and Economic development through globalization

While the need of e-government will become a prerequisite in each country in the world and a measure in developing nations, supporting e-government services with a security will be the first requirement to maintain adoption and sustainably of e-government services.

The United Nations classify countries as either developed or developing based upon the GDP per capita, human assets, and degree of economic vulnerability (Sara, 2012) , In developed countries e-government has become an evolving and important issue to provide governmental services and providing security to e-government are considered and take place. Sudan is considered developing country, the infrastructure of ICT in Sudan is growing up in this stage Sudan is preparing a portal for e-government and providing Security is an open issue to be implemented.

1.5. Research Objectives:

The main objective of this research is to develop an authentication framework and the requirements for the e-government security. The use of such services, the level of security can be significantly increased. On this basis, the national security risks incurred can be greatly reduced.

The sub- Objectives are:

1. To investigate the existing methods and techniques to secure E-government
2. To propose a novel Framework of authentication for e-government security.
3. To Test, evaluate and benchmark of the proposed solution
4. To contribute to the development of a favorable environment for sound economic growth

1.6. Research philosophy:

1. Strengthen the interaction between citizens and the country to enhance participation of civil society in public affairs and promote social inclusion
2. Disseminate and promote the new e-Governance services, so that all citizens have access to them on an equal opportunity standing.

The research concerns about make a rise in service delivery from government to citizens moreover facilitate governmental operations which come with citizens benefits to give them a space for creativity to country advancement. This will encourage good relationship between citizens and country.

Moreover living level will get better and as a result, various e-government initiatives have been conducted across the country to decrease telecommunications costs, increase the rate of development in the field of information technology and narrow the digital divide between the rural and urban areas.

1.7. Research Questions

Research questions concentrate on implementing the proposed solution and examine the approach and authentication framework to answer the following:

First: Do citizens Trust e-government applications?

Second: Are accessing information systems and e-government applications reliable?

Third: Do Governments/citizens verify and Ensure identities?

Security of information is essential to the building confidence and trust in e-government, to do so we can achieve healthy relationship between government and citizens and vice versa, this lead directly to reliability. According to the Dictionary As an adjective, Reliable means consistently good in quality or performance, able to be trusted.

To ensure identities in e-government we need to examines identification and verification methods of biometrics, the most reliable identification method in addition to most effective cryptographic techniques to secure the process of identification and verification methods of biometrics

1.8. Research Scope

This research concerns of providing security thorough application layer on e-government application, where citizens seeking the right access to governmental services electronically, to do so and governments need to insure identity of citizens authenticating the communication parties, where this build trust of C2G and G2C services. From these aspects accessibility means that the rights of both sides to access to the information required. The research will not cover the integrity or availability of information, but seeks authentication and authenticity of information.

1.9. Dissertation outlines:

Chapter 1: Introduction

The dissertation starts in this chapter with introduction and background to E-government and E-government security, the chapter addresses the area of the research and its significance, objectives and the motivation around this research, moreover the research scope and research questions and philosophy.

Chapter 2: Literature Review

In this chapter provide a holistic view and theoretical background about E-government security and applications of e-government moreover survey on the on the use of technologies in e-government such as Biometrics, cloud computing and mobile E-government. The chapter also examines the related works of existing models for e-

government assessment and security standards and how to gain trust, finally the chapter ends with a summery.

Chapter 3: Research Methodology

Start this chapter with an introduction to the methodology being used in the research, the chapter also describe the proposed solution by conducting a case study about Sudan E-government and produce case study findings and results, the chapter also address the research tools and evaluation techniques through simulation of a secure login for e-government and describe which tools to use to do a penetration test to evaluate the simulated model, finally the chapter ends with a summery.

Chapter 4: Design of the Proposed Fingerprint Digital Signature Model

Start this chapter with an introduction to the proposed authentication framework and describe the proposed model for e-government authentication that uses fingerprint as identification process and digital signature for verification, the chapter present how this model tackle e-government secure access, finally the chapter ends with a summery.

Chapter 5: Testing of the Proposed

Start this chapter with an introduction to chapter contents where the chapter presented the resulted simulation analysis and resulted analysis of testing to draw a discussion and, finally the chapter ends with a summery.

Chapter 6 Conclusion and Recommendations

This chapter presents a summary of the results and the achievement of the research study, after revisiting the research objectives. As a conclusion, the chapter indicates how the presented research study can evolve and contribute to a further research. Finally concludes with addressing the limitation of the research study conducted in this dissertation and future recommendations is discussed.

CHAPTER II

Literature Review

2. Literature Review:

2.1. Introduction:

This chapter is to give a spot light about a research area, provided an overview of secure e-government accessibility and a comprehensive related works. The chapter provide a holistic information and up-to-date literature review on e-government applications, services and provided security that challenge e-government adopting.

2.2. An overview of secure e-government accessibly:

2.2.1. E-government Services benefits

Majority of the state e-government sites offered a series of e-services such as government to business; government to education; government to employment and training; government to travel, recreation, and transportation; government to citizens including news, visitor's guide, family, health, safety, license application, law, justice, and legislature.

Providing governmental electronic services will impact on time, effort and cost of administrative process, this yield a good community competitive across the world, moreover improving the quality of provided service, and the operational level (Jensen , Sherry , 2010), unfortunately the growth of using these e-services on the Internet may be threatened and main target of attackers.

2.2.2. E-government threats:

In the designing of an efficient e-Government system, security becomes the main issues to be considered. E-Government system is type of on-line system that require a ICT based network to execute properly but e-Government system is different from other on-line system particularly with reference to security as an e-Government system handles a lot of secure and legal information that must be protected from unauthorized users. The Canadian Government is using an advanced Web portal called BusinessGateway.ca not only making available information and communication similar to the Austrian Help.gov but also

secure transaction services for businesses (Alexander , 2003). Security is critical for their successful implementation for e-Government and transaction based services. Some of the security issues in e-Government are discussed below:

- Confidentiality/Privacy/Accessibility: ensuring that systems and information are accessible to those authorised to access it.
- Integrity: ensuring systems and data have not been tampered with (either accidentally or maliciously) and are in their original and intended state.
- Accountability/Non-repudiation: ensuring that when data is delivered to a recipient neither recipient nor sender can deny having received or sent the data.
- Authentication: ensuring that entities (whether individuals, hardware or software) can be authenticated as being the original and genuine entity.
- Trust: that there is an infrastructure both technical and non-technical which engenders trust and that this is made visible to the community of users.

Table 2. 1: Security Threats and their solution in an on-line system/project (Alexander , 2003)

Threat	Security	Function	Technology
Data intercepted or modified illicitly/ Data integrity	Encryption Algorithm/ Hash Function	Encode data to prevent tampering	Cryptography Algorithms, MD5/ SHA etc.
Unauthorized user on one network gains access to another	Firewall	Firewall prevents certain traffic from entering the network or server	VPN / Firewall
False Identity with an intention of fraud	Authentication	Identity verification of both sender and receiver	Password/Digital Signature
Copyright protection of data	Digital watermarking	This type of data is copyrighted but not secret.	Digital Signal/Image Processing, watermarking

2.2.3. Technology Framework for Online Trust

- Digital Envelope

It combines the high speed of symmetric encryption (e.g., AES Rijndael) and the key management convenience of public key encryption. Includes PSE (Smartcards, Mega-brid, USB tokens), biometrics, Hardware Security Modules etc..

- Digital Signature

It combines Hash Algorithms (FIPS-180), Key Exchange, Public Key Encryption to provide Data integrity, Non-repudiation and Certificate-based Authentication. Digital credentials are established using ITU-T X.509 Digital Certificate Standard

- Digital Certificate

ITU-T X.509 creates the framework for establishing digital identities – A key component for establishing security and trust for ICT applications in public networks such as the Internet (Henriksson, 2006)

2.2.4. Industry Solutions for Online Trust and Security

Table 2. 2: Industry Solutions for Online Trust and Security

Common e-Security technologies				
	Authentication	Confidentiality	Integrity	Non-repudiation
Anti-virus			√	
Firewalls	√	√		
Access Control	√	√		
Encryption		√		
Public Key Infrastructure	√	√	√	√

2.2.5. Secure access of e-government:

There are a number of security objectives relating to communication between customer and agency that must be met by conventional communication procedures and by communication procedures in e-government. Some of the security objectives and requirements are also sub-aspects of higher-level security objectives.

- Binding force

The generic term "binding force" refers to the aim of ensuring that the data transferred is seen to be "valid". Particularly important aspects that need to be ensured here are the legally binding nature (in the sense of entering into a contract), fulfilment of the requirement for the written form (as required by law) and non-repudiation (protection against subsequent denial of authorship). Also of importance are the requirements for identifiability of originator (ability to attribute the identification data unambiguously to the originator), unequivocal mapping of the authentication data to master data and data integrity (protection against modification of data during transfer). For many transactions the time of verification of identity is significant and there may be a need for ex-ante authentication (i.e. authentication before providing the service).

Note: The requirements "identifiability of originator" and "addressability of recipient" are often grouped together under the security objective "authenticity of communication partner" (Malik , 2011).

- Confidentiality

Confidentiality is understood to refer to the aim of ensuring that no unauthorised third parties can gain knowledge of the transferred data. In particular, the aspects of security of data transfer (protection against others reading the data during transfer) and addressability of recipient (protection against the transmission of data to an unauthorised third party) must be ensured. Further security objectives depending on the particular transaction,

further security objectives, e.g. availability (of communication pathways etc.) may need to be investigated.

Communication in e-government; when considering communication in e-government, it is (only) necessary to look at the particular sub-process in an e-government service in which data is exchanged between customer and agency, i.e. only data input and output are considered. When looking at communication between customer and agency, a distinction needs to be made between data transfer from customer to agency (customer as "originator") and data transfer from agency to customer (customer as "recipient")(Malik , 2011).

2.2.6. Building trust through authentication:

While we talk about security we need to shed light on preserving trust. Ensuring security of e-government applications and infrastructures is crucial to maintain trust among stakeholders to store, process and exchange information over the e-government systems.

As Baier states "*Trust involves the belief that others will, so far as they can, look after our interests, that they will not take advantage or harm us. Therefore, trust involves personal vulnerability caused by uncertainty about the future behavior of others, we cannot be sure, but we believe that they will be benign, or at least not malign, and act accordingly in a way which may possibly put us at risk.*" (Sofia, 2009).

We need to study citizen's characteristics and needs to be properly understood, these can be found through two dimensions: (trust on government and trust on Internet), the study(Sofia, 2009) specify twelve determinants of e-government trust which include :(age, perceived usefulness, perceived quality, risk perception, Privacy concerns, perceived organizational trustworthiness, trust in technology, Propensity to trust, years of Internet experience, Income, education and Gender), however training may be another determinant of trust.

To be successful, e-government projects must build trust within agencies, between agencies, across governments, and with businesses, Non-Government Organization (NGOs) and citizens.

When conceptualizing e-government, developers often do not realize the many boundaries, both physical and administrative, that the proposed project will cross. Yet, the success of e-government often comes down to building trust and common understanding with the variety of players early in the process. The biggest concern for most parties is that change brought about by a new system will negatively impact them. Almost every successful e-government project is a case example in building trust.

The issue of trust also involves two issues of special concern to any online service:

- Privacy: protecting personal information the government collects about individuals.
- Security: protecting e-government sites from attack and misuse.

Developing a unified identity authentication in e-government (ZHOU,2012) using digital signature through centralized authentication and a unified certification services may serve not forget account credentials among different e-government services instead of remembering several accounts, however this solution may attract attacker to account spoofing.

2.3. Related Works:

E-government applications and assessments, new trends and e-government

2.3.1. Applications of e-government and provided security:

2.3.1.1. Electronic voting machines and applications are become important to be adopted by many countries, however any failure in electing the correct candidate may result in untruthfulness (Dominique et al, 2007), these failures may be due to the interfaces that are not well designed or software bugs or even hardware malfunctioning, ensuring validation in software may be a good solution (Dominique et al, 2007), however it’s not provide a total security.

2.3.1.2. Some countries adopt e-transaction through e-government portal, such as retrieving driving citations and other services, these services require confidential information and authentication, where data may be exposed to modifications, the study by (Amina, Omaima ,2009) suggested a good solution that preserve Authentication, Confidentiality, Integrity and Non-repudiation of data through different levels as the most critical characteristics of secured data, however the study concentrate a specific application underplaying the risks comes from other e-government applications and underlying infrastructures.

2.3.1.3. Another threat may appear from the use of e-government application is cloning and tampering passports electronically (Luca , Dario ,2014) the e-passport contains the information on chip and according to International Civil Aviation Organization (ICAO), The chip stores owner's personal data and biometric features, and other information, in (Luca , Dario ,2014) provide a comprehensive study which views that the inspection process of e-passport doesn't reject a document in many cases such as old version chips or using different security protocols while passport is valid hence it durable from 5 to10 years, this may be vulnerable and attacker may exploit it and ignore a security measure to accept reading chip information and clone it into a new blank chip and tampering information, additional check is provided as an enhancement security to control inspection process so, it cannot be sidestepped by the attacker(Luca , Dario ,2014), however it's not official implemented yet.

2.3.2. Assessment of e-government:

2.3.2.1. United Nation e-government assessment:

According to the 2012 United Nations E-government Survey rankings, the Republic of Korea is the world leader (0.9283) in the use of e-government followed by the Netherlands (0.9125), the United Kingdom(0.8960) and Denmark (0.8889), with the United States, France, Sweden, Norway, Finland

and Singapore close behind, these information according to the UN's 2012 e-Government Readiness Index. The survey focuses on to what degree countries involved the use of ICT in different areas such as entrepreneurship, innovation, research and development, promoting distance learning, e-health, the use of cellular technology, Bridging the digital divide, therefore the United Nations e-government assessment concentrate on the concept of integrated services that exploit inter-linkages (may be interoperability) among different public services(United Nations,2012), however they didn't assess any security aspects in e-government.

2.3.2.2. Assessment of e-government security:

Cyber security has to deal with cyber regulations on different fields such as e-Commerce, e-Banking, e-Government and e-Healthcare, and all these depend on the governance of cyberspace to facilitate the use of web as a medium to promote global interchange without risk.

To evaluate the degree of security of e-Gov we need to examine regulations or/and sometimes security policy and a model as a security measure. In (Mohammad , Hamdan,2012) is pointing out the most important threats that may e-government face, they classify them into 3 classes (client end threats, communication channel threats or server end threats) and what are security requirements for information systems and privacy, however the study concentrate on the performance measure and ignoring the fact that prevention is better than cure, although it might be good to build security metrics.

Most of studies adopted e-Government maturity models (eGMMs) where it is dedicated to evaluate the e-Gov and (eGMMs) refers to the maturity stages of a common frame of reference for e-government, the maturity stages are: web-presence, interactional, transactional, transformational, and continuous improvement (Geoffrey, 2012) However, the models lack built-in security services.

Developing information security matrices to measure and evaluate security of e-government is a critical issue therefore there are a number of models that dedicated to evaluate Information security in e-Gov, by reviewing all models and standards of information security maturity models (ISMM), ISMM model seeks the full compliance having full control on an information systems through these steps (prevent-detect-correct) (Geoffrey, 2011) (Malik, 2011), another solution made using fuzzy logic Multi-criteria Decision Making (MCDM) framework to assess e-Gov security strategy (Irfan, Junseok, 2010). Moreover security models are analysed (N. Alharbi,2013) according to the security issues wither it was technical or non-technical, the technical issues may concerns about problems related to availability, confidentiality or integrity, and the non-technical issues are related to trust, lack of awareness, digital divide and ethical issues, the existing security models and theories, where they are classified into:

- **Technical models:** such as Bell-LaPadula (BLP) Model(focus in confidentiality), Biba Model (focus on integrity), Clark-Wilson Model(focus on integrity), The Chinese Wall (focus on Privacy and integrity), Lambrinoudak is Security Framework (availability and authentication), Infosec Model (focus on availability, integrity and confidentiality)
- **Non-Technical Models and Theories:** such as Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Technology Acceptance Model (TAM), Diffusion of Innovation (DOI), Motivational Model (MM), Social Cognitive Theory (SCT), Model of PC Utilization (MPCU), Unified Theory of Acceptance and Use of Technology (UTAUT), the last model encompasses all above non-technical theories, where Figure 2.1 state a relation between the eight factors of accepting new technologies.

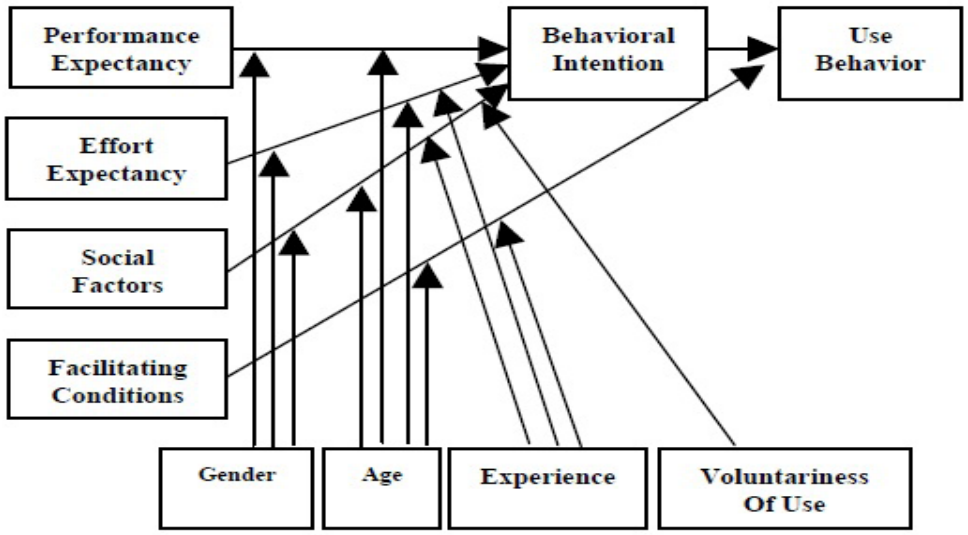

Figure 2. 2: the eight factors of UTAUT (N. Alharbi,2013)

The study tackles "There is no model covers both of technical and non-technical issues in the same time" (N. Alharbi,2013).

Technical models:

The most critical information characteristics are: authentication of users, availability, integrity and confidentiality of information, these characteristics can be implemented through the following models:

Lambrinoudakis security framework:

The framework was developed to identify and organize the security requirements for the information systems supporting the e-services offered by the e-government (Sabri , 2008), this framework developed to avoid denial of service attack that compromising availably of information, it is used to ensure authentication also, this can be done through It contains five steps (setting up the supporting system, authentication, setting up the service, offering the service, and after service task) (N. Alharbi,2013).

InfoSec model:

This model can minimize the vulnerabilities and security holes of completed attacks and selecting the best action to protect the system from electronic eavesdropping (N. Alharbi,2013), it covers availability, integrity and confidentiality of information, Figure 2.3represent the InfoSec model which considered as amulti-layered model (Sabri , 2008)

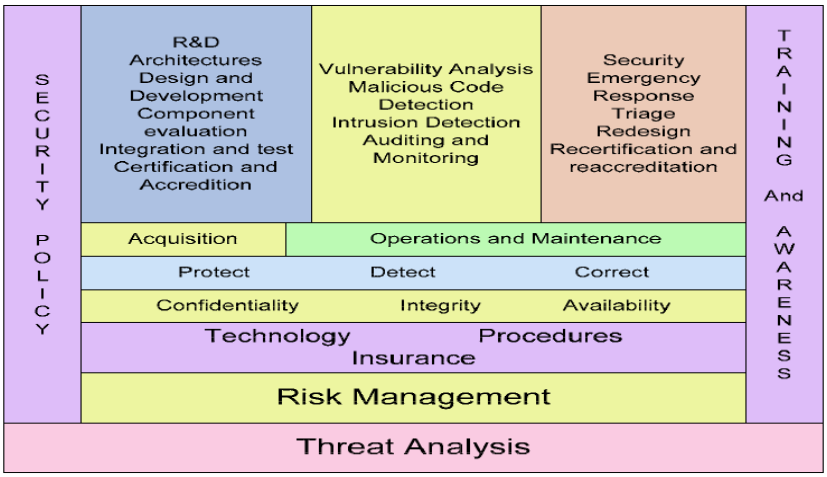

Figure 2. 4: the InfoSec Model

It considered an excellent model to be implemented in securing e-government services.

Non- Technical model to gain Trust

The use and adoption of e-government depends mainly on human factors. Through literature review, we choose the UTAUT (Unified Theory of Acceptance and Use of Technology) this model measure the user acceptance of any technology and it might be useful to build user confidence and trust, however the effect of the use in terms of security reasons will extent the user acceptability of e-government services where social engineering attacks may take a place as a new factor that compromise security of e-services, hence increasing user awareness of social engineering and phishing attacks will become an important practice.

2.3.3. E-government Security and New trends:

2.3.3.1. Cloud computing and security in E-government:

Cloud computing is a technology to provide a service to clients through Internet in different models, a) Infrastructure as a Service (IaaS), b) Software as a Service (SaaS) and c) Platform as a Service (PaaS) [(Charalampos, Marinos , 2011), (Bernd et al , 2013), Although cloud computing has a number of benefits such as cost reduction, massive storage space, scalability and elasticity, but it faced by a great challenge in providing data protection and compliance , building a so-called G-cloud or (government cloud) usually require more secure and reliable authentication and identification mechanisms (Bernd et al , 2013).

The study (Smitha , Chitharanjan , 2012) proposed a new mechanism for database encryption with flexible performance and database access, where it ensuring confidentiality of government sensitive data. The mechanism rely on an encrypt/decrypt AED (advanced encryption standard) symmetric key algorithm, which encrypt all data before storing into the cloud, it uses coarse index to improve the query performance which avoid the full table scan, once the scheme uses secret keys the proposed solution is to embed the key in a finger print image that uses DCT based image (Smitha , Chitharanjan , 2012).

2.3.3.2. Secure M-Government (Mobile-Government):

The new trend BYOD (bring your own device) become popular in most companies and associations(Ali ,2013), where employees use their own smart phones to access information systems, however this indeed increase security risks. The general fear is that the user mobile phone numbers will be traced, when they send their opinions and inquiries to the government (Ibrahim , 2004) this may compromise user's privacy.

The research (Shadi et al, 2007) study the transition from E-government to M-government and stating the success factors as it is shown in Table 2.3, the factors are ordered according to the importance percentages, where the privacy

and security considered as the most important factor that affects on the use of M-government.

Table 2. 3: M-Gov success factors and importance percentages (Shadi et al, 2007)

65%	**- Privacy and Security**
55%	**- Infrastructure**
52%	**- User needs and preferences**
48%	**- Quality and user friendly applications**
48%	**- E-government**
48%	**- Acceptance**
48%	**- Cost**
45%	- Standards and data exchange protocols
42%	- Coherent m-government framework
42%	- High mobile penetration
39%	- Infrastructure management
35%	- M-government awareness
32%	- Access
29%	- Strategy
26%	- IT literacy
26%	- M-government portal and exclusive gateway
13%	- Partnership with private sector
10%	- Legal issues: liberalisation of telecommunication sector

Vulnerabilities can be found extensively in wireless communication, in (Thamer, Steve) proposed an advanced authentication method for m-Government, however the study depends only on questioners not an experimental model, although it might be useful result that users are willing to use M-government without fear of risk!.

2.3.3.3. Digital signature in e-government

In the process of government documents flow, it is very important to confirm identity of both sides of communication and prevent unauthorized users from destructing documents. When people or businesses deal with government, they need to prove who they are to access some government services, for example when registering a company or looking at a person's medical records. Therefore, authentication is the process of confirming the identity of the person, to the required level of confidence.With the Internet becoming a mainstream channel for interacting, transacting and participating, online authentication has become a prerequisite for effective and efficient government worldwide. Digital signature is one of these tools. It is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a

document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signature is a major technological to guarantee non-repudiation and the integrity of government documents on the Internet. The basic purpose of digital signature is not different from our conventional signature. The purpose therefore is to authenticate the document, to identify the person and to make the contents of the document binding on person putting digital signature. The purpose of digital signature is the same as the handwritten signature. Instead of using pen and paper, a digital signature uses digital keys (public-key cryptology). Like the pen and paper method. A digital signature attaches the identity of the signer to the document and records a binding commitment to the document. The real value is in avoiding the paper and keeping your data electronic. There are many algorithms of digital signature. The preferred way is digital signature based on Public Key Infrastructure (PKI) and certification Authority (CA). In addition to typical RSA-based digital signature, people have been increasingly attached to ECDSA (elliptic curve digital signature algorithm), group signature scheme, and multi-signature scheme and so on. In his paper, RSA-based digital signature is bound up with user role. Figure 2.3describes the process of digital signature.

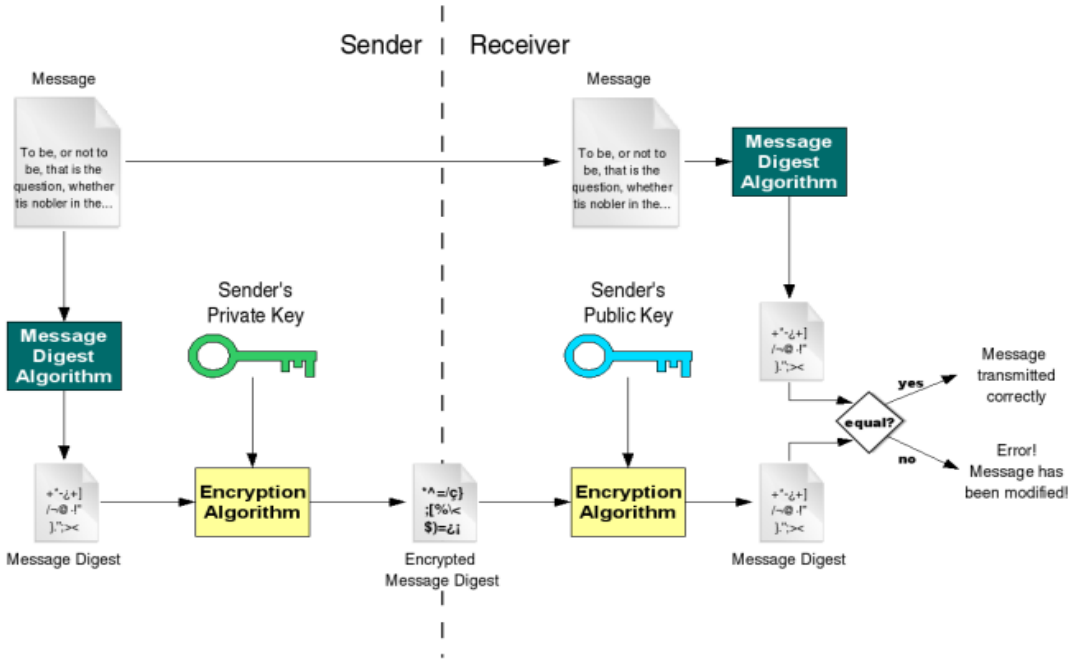

Figure 2. 5: Digital Signature Generation and Verification

Handwritten Signatures v/s Digital Signatures

A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature. A Digital Signature is a combination of 0 & 1s created using crypto algorithms.

An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Further, paper contracts often have the ink signature block on the last page, allowing previous pages to be replaced after the contract has been signed. Digital signatures on the other hand compute the hash or digest of the complete document and a change of even one bit in the previous pages of the document will make the digital signature verification fail. As can be seen in the underlying figure, a Digital Signature is a string of bits appended to a document. The size of a digital signature depends on the Hash function like SHA 1 / SHA2 etc. used to create the message digest and the signing key. Itis usually a few bytes.

Table 2. 4: Handwritten Versus Digital Signatures

Parameter	Paper	Electronic
Authenticity	May be forged	Cannot be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	c. Any computer user d. Error free

Comparison and Analysis among Three Digital Signature Algorithms

It has become clear over the past several decades that public-key (asymmetric) cryptography is an indispensable tool for simplifying key management and enabling secure communication. And digital signature algorithms exactly build on it. It is one of the major developments in network security. The need for Digital Signature has arisen with the rapid growth of digital communications. A Digital Signature algorithm authenticates the integrity of the signed data and identity of the signatory. Authentication in a Digital Signature is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message. There are three main contenders: RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm). Each has a variable key size that can be increased to achieve higher security at the cost of slower cryptographic operations. The best attack known on each public-key cryptosystem requires an amount of computation determined by a security parameter which is related to the key size (RabahAlshboul,2012)(Henriksson, 2006).

A. RSA

The RSA public-key cryptosystem involves exponentiation modulo a number n that is the product of two large prime numbers. Plaintext is encrypted in blocks, with each block having a binary value less than the number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is i bits, where $2i<n\leq 2i+1$.Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$$C = M^e \bmod n$$

$$M = C\ d \bmod n = (M^e)\ d \bmod n = M\ ed \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e,n} and a private key of PR ={d,n}.When referring to the key size for RSA, what is meant is the length of the modulus n in bits. A typical key size for RSA is 1024 bits. RSA can be used for encryption and also be used for digital signature. RSA encryption is quite slow because of large key size and

modular exponentiation operations that have to be used to ensure security. For the same reason, RSA's Digital Signature is slow as well (Sharifi et al, 2004). The length of transmitted Signature equals the length of transmitted message. In other words longer the message, the longer the Digital Signature

B. DSA

The DSA is based on the difficulty of computing discrete logarithms and is based on schemes originally presented by ElGamal and Schnorr. Specifically, the DSA is public-key techniques based on exponentiation modulo a large prime number p. For this scheme, the key size is the length of the prime p in bits, and a typical value is 1024 bits. When exploiting the size of it, the best attack known is the General Number Field Sieve. However, another important security parameter is the size of exponents used for exponentiation. For DSA, the exponent size is fixed at 160 bits.

C. ECDSA

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Typically, elliptic curves are defined over either the integers modulo a prime number (GF(p)) or over binary polynomials (GF(2m)). When referring to the key size, what is meant is the size of the prime number or binary polynomials in bits. Typical key sizes are in the range 160 to200 bits. The security parameter is the size of multipliers which is limited to the order of the generator used and slightly smaller than the key size(Abhishek , Sunil, 2014).

1. Digital Signature Certificates

Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet. A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to the individual. Digital certificates are the digital equivalent (i.e.

electronic format) of physical or paper certificates. Examples of physical certificates are driver's licenses, passports or membership cards.

Digital Signature Certificates are endorsed by a trusted authority empowered by law to issue them, known as the Certifying Authority or CA. The CA is responsible for vetting all applications for Digital Signature Certificates, and once satisfied, generates a Digital Certificate by digitally signing the Public key of the individual along with other information using its own Private key.

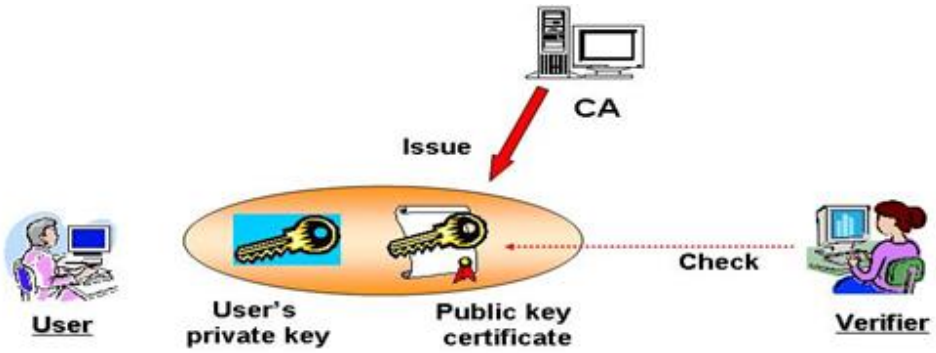

Figure 2. 6: Digital Signature Generation and Verification

Figure 2.4illustrate the role of CA in PKI where the preferred way is digital signature based on Public Key Infrastructure (PKI) and certification Authority (CA).

2.3.3.4. Biometrics and Security in E-government:

Government systems wither it was electronic or non-electronic need to ensure identity and authentication of citizen, bioinformatics as a science uses computers to better understand biology, with the aid of biometric as a tool can asset in the field of computer forensics that search the evidence about cyber-crime, the biometric systems may function either in verification mode or identification mode; where systems need to perform a number of comparing and recognizing processes to deal with authorized user, biometrics data may be characterized through *face recognition, fingerprint, Iris, voice, hand &*

finger geometry, whoever there are possible attacks on biometric systems as shown in Figure 2.5 (Piyush et al.,2012).

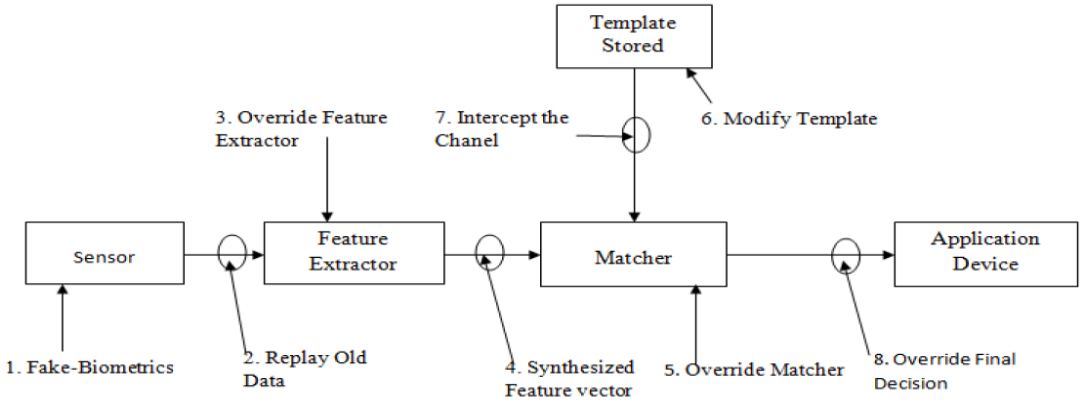

Figure 2. 7: shows possible attacks on biometric systems (Piyush et al.,2012)

As in (Piyush et al.,2012) there is a proposed system to recover vulnerabilities rely on applying two security strategies (diversity of defence and defence in depth strategies) which consider an advantage. The solution shown in Figure 2.8 depends on four mechanisms

a. Multi-biometrics: do not depend on a single biometric data i.e. use fingerprint, iris, face, hand geometry or voice all together.
b. Use sequence number: protection from replay old data.
c. Access control: use of multilevel security
d. Cryptographic techniques: use of encryption algorithms or digital signature

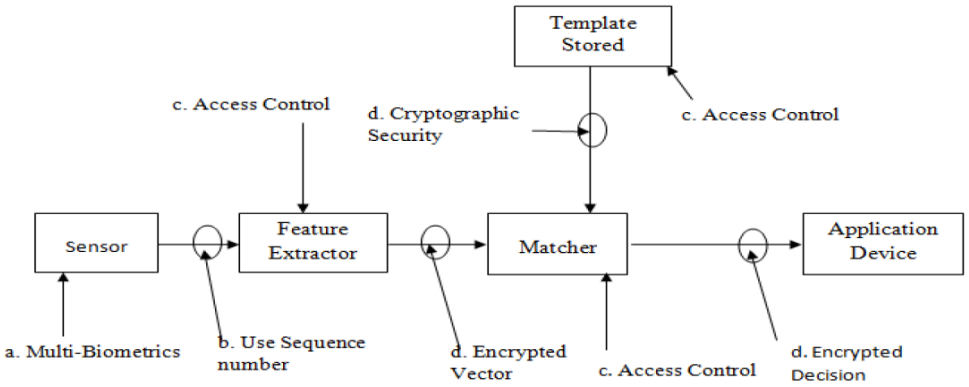

Figure 2. 9: Solution to remove vulnerabilities in system (Piyush et al.,2012)

Biometric Fingerprint in e-government

Biometrics can be used for identification and verification of different things about human beings, where Biometrics are the use of a person's unique physiological, behavioural, and morphological characteristic to provide positive personal identification(Rodger , 2004), whoever Biometric identification technologies have been associated generally with expensive and secure applications.

Biometric systems are considered the most important systems for identification process in most of controlled access systems such as ATM, cellular phones, smart cards, desktop PCs, workstations and computer networks (Tripathi, 2011). all biometric systems use the four-stage procedures: Capture, Extraction, Comparison, and Matching (Piyush et al.,2012),(2012 , صفاء واخرون .د).Biometric fingerprint capture step to capture human fingerprint sample during Enrollment, identification, or verification processes using fingerprint scanner, the extraction process is done to take a unique data extracted from a sample and a template is created and stored, the third stage is to compare the template with the new sample and finally a matching process is done to decide if the features extracted from the new sample are match or none-match(2012 , صفاء واخرون .د).

Biometric fingerprint is the best known biometric technology, Fingerprint identification process is used the impressions on human fingers made by the minute ridge formations or patterns found on the human fingertips (Rodger , 2004),(Anil et al,

1997). Human use fingerprint for identification for long time, no two persons have exactly the same arrangement of ridge patterns (even identical twins), and the patterns of any one individual remain unchanged throughout life (Rodger , 2004). Table 2.5present a comparison between different biometric technologies, and here the identification process on the different biometric technologies must satisfy the following requirements (Tripathi, 2011),(Anil et al, 1997):

- Universality: every person should have the characteristic;
- Uniqueness: no two persons should be the same in terms of the characteristic;
- Permanence: the characteristic should be constant with time;
- Collectability: the characteristic can be measured quantitatively.
  And other requirements:
- Performance: is the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy;
- Acceptability: to what extent people are willing to accept the biometric system;
- Circumvention: how easy it is to fool the system by fraudulent techniques.

Table 2. 5: Comparison between biometric technologies (Tripathi, 2011),(Anil et al, 1997)

Biometrics	Univer-sality	Unique-ness	Permanen-ce	Collecta-bility	Performa-nce	Acceptabil-ity	Circumvention
Retina	High	High	Medium	Low	High	Low	High
Face	High	Low	Medium	High	Low	High	Low
Finger print	Medium	High	High	Medium	High	Medium	High
Hand geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
DNA	High	High	High	Low	High	Low	Low

Biometric has been widely used in forensics, such criminal identification and jail security and has the possibility to be widely adopted in a very broad range of government services (Piyush et al.,2012)

- Banking security, such as electronic fund transfers, ATM security, check cashing and credit card transactions;
- Physical access control, such as airport access control;
- Information system security, such as access to database via login privileges;
- Government benefits distribution, such as welfare disbursement programs;
- National-id systems, which provide a unique id to the citizens and integrate different government services;
- Voter and driver registration, providing registration facilities for voters and drivers
- Customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated (Piyush et al.,2012)

Biometric fingerprint is considered as the most suitable biometric technology for e-government services for Uniqueness, Circumvention and Permanence reasons, however it is still vulnerable to clone fingerprint (Luca , Dario ,2014) over Internet based application, this research proposed a solution to combine biometric fingerprint and digital signature as a two way verification model that narrow the chance of attack and provide an effective authentication method for access e-government services.

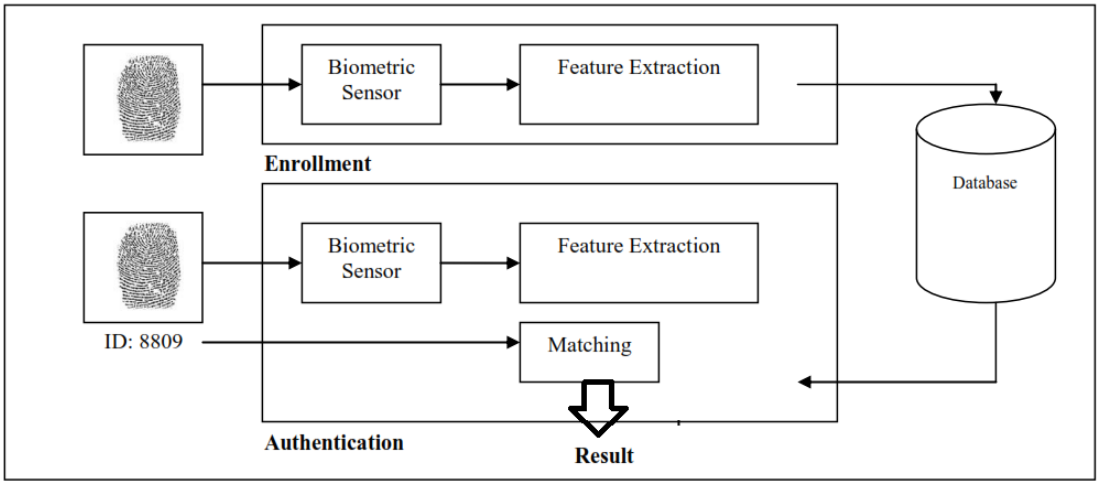

Figure 2. 10: Generic Biometric System (Tripathi, 2011)

Figure 2.7 illustrate how the process of Enrolment and authentication in a Generic Biometric system (Tripathi, 2011), for fingerprint system, Enrollment process start by acquiring the fingerprint image from fingerprint scanner (biometric sensor), then the feature extraction process will start to find the minutia(the unique data) according the feature extraction methods and level of extracted features, features encoding process might be minutia-based, image-based or texture-based where these processes produce a template which finally will store in a database to terminate the Enrollment process. The authentication process will start by acquiring the fingerprint image and then the verification process will start by compare the features extracted from the new fingerprint image and with a template from database, here 1:1 process is done, if its matched then the new fingerprint will verified and authenticated(Tripathi, 2011),(د. صفاء واخرون , 2012), it's worth to mention that it is impossible to reconstruct a fingerprint from the biometric template file, although, it's possible to have the same global features, but the local features remain unique.

The identifying power of a particular biometric encompasses has two terms:

- False Rejection Rate (FRR), or a Type I Error
- False Acceptance Rate (FAR) or a Type II Error, and
- Crossover Error Rate (CER).

For example, if the false acceptance rate threshold is increased to make it more difficult for impostors to gain access, it also will become harder for authorized people to gain access. As FAR goes down, FRR rises.

On the other hand, if the false acceptance threshold is lowered as to make it very easy for authorized users to gain access, then it will be more likely that an imposter will slip through. Hence, as FRR goes down, FAR rises. The CER is a percentage rating of Type I versus Type II errors. A lower CER rate means better accuracy (Rodger , 2004).

FRR and FAR is used for measuring the effectiveness of biometrics matching technology. For biometric fingerprint Typical False Rejection Rates range between 0.03%-1.4%, Typical False Acceptance Rates are around 0.01%-0.001%, and these rates depend on the manufacturer and the algorithm used.

Features of interest in fingerprint are known patterns all patterns constructed from the core point as it is seen in Figure 2.8, where a Core Point - is the approximate centre of

the fingerprint, and is used as the reference point for reading/classifying the print (Rahul et al ,2013).

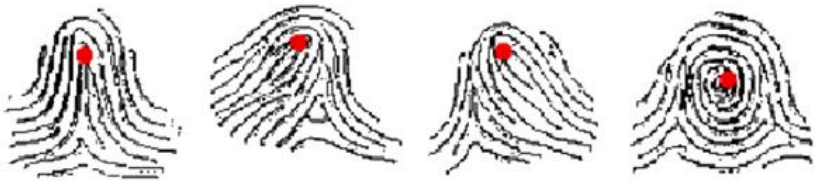

Figure 2.8: shows the types of fingerprint features which can be

Figure 2. 8, Figure 2.9, Figure 2.10and Figure 2.11shows the types of fingerprint features which can be:

- Global Features - are the characteristics that any human can see with the naked eye (Rahul et al ,2013), (2012 , د. صفاء واخرون)
    1. Basic Ridge Patterns: Loop - is the most common (~65% of all prints), Arch - more open curve than a loop, Whorl - ridge that makes a complete circle (~30% of all prints)
    2. Pattern Area: is the part of the fingerprint that contains all the global features. However, some local features may be found outside the pattern area.
    3. Delta: is the point on the first bifurcation, abrupt ending ridge, meeting of two ridges, dot, fragmentary ridge, or any point on a ridge at or nearest the centre of divergence of two type lines, located at or directly in front of their point of divergence.
    4. Type Lines: are the two innermost ridges that start parallel, diverge, and tend to surround the pattern area.
    5. Ridge Count: is the number of ridges between the delta and the core.

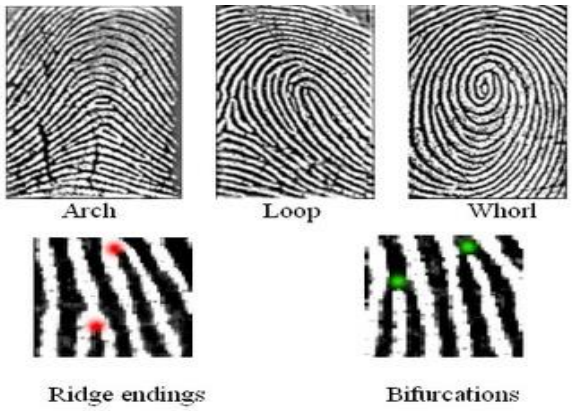

Figure 2. 11: Basic Ridge Patterns

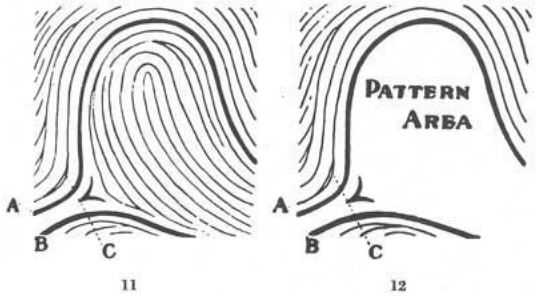

Figure 2. 12: Pattern Area:is the part of the fingerprint

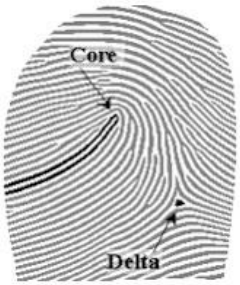

Figure 2. 13: Delta

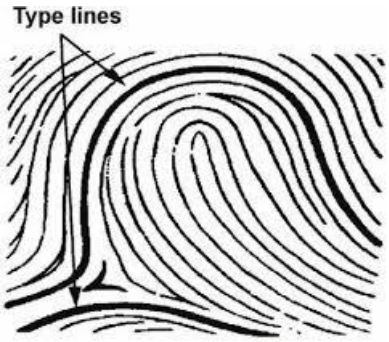

Figure 2. 14: Type lines

- Local Features - or “Minutia Points” are the unique characteristics of fingerprint ridges that are used for positive identification, Figure 2.12 shows the Local Features which can be(Rahul et al ,2013), (2012 , د. صفاء واخرون):
    1. Ridge Ending - ridge ends,
    2. Ridge Bifurcation - divides into Branches,
    3. Ridge Divergence - diverging of two, parallel lines,
    4. Dot or Island - small ridge,
    5. Enclosure - divides and reunites,
    6. Short Ridge - like a dot/island, but larger

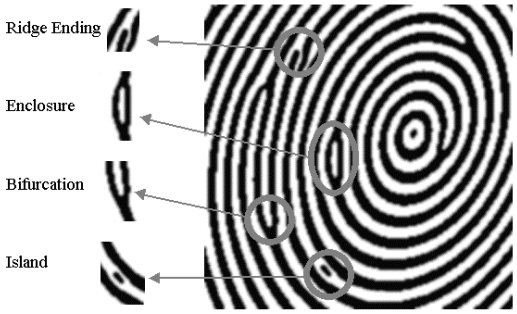

Figure 2. 15: Ridge Count

Minutia points

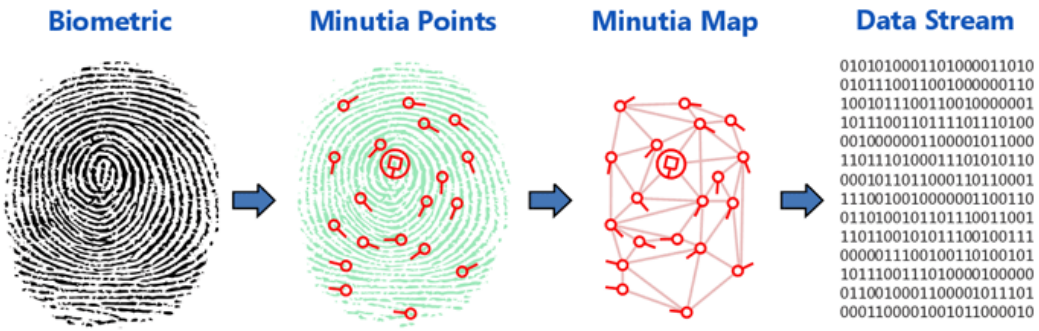

Figure 2. 16: Minutia points

Once a fingerprint is captured the system locates the minutia points. These minutia points occur where the lines of the ridges begin, end, branch off and merge with other ridge lines. These points are then mapped and a line is drawn between each point. This creates a map of how each point relates to the other points. The map is then stored as

a data stream called a minutia template in a database for future comparison with other presented fingerprints. Figure 2.13 represents the minutia encoding process.

2.3.3.5. E-government Security and ease of use:

It is worth to mention that security will contrary to ease of use, notably more check process may create bottleneck to the use of e-government applications. Regardless of the measures the e-gov takes, the weakest link will nearly always be the human factor. Consequently, it's more important than ever that citizens are educated about the risks that they take when using sensitive data.

At a minimum, citizens should learn basic security measures, ranging from choosing strong passwords to best practice when handling data or working on a mobile device. Therefore the conducted security measure should make a balance between provided security and ease of use.

2.4. Summary of related works:

Authors, year	Framework/Approach	Advantages	Limitations
Dominique Cansell,e.t. ,2007	Secure e-voting	Insuring validation in election process	Not provide total security
Amina Gamlo and Omaima Bamasak ,2009	Securing e-transaction in e-government	Secure driving citation	Not suited for other application
Luca Calderoni, Dario Maio, 2014	e-passport	Safeguard authenticity	not implemented yet, hence cloning passport available
N. Alharbi, 2013	e-government security modeling	Comprehensive review of existing security models	No model covers technical and non-technical security issues
Piyush Morwal, e.t., 2012	Securing e-government using biometrics	Use diversity of defend and defense in depth to ensure identity	Overhead processing not needed in low level of authentication

ZHOU Feng, 2012	Unified Identity authentication in e-government	serve not forget account credentials	solution may attract attacker
Abhishek Roy, Sunil Karforma, (2014)	Stream Cipher Based User Authentication Technique In E-Governance Transactions	Can be suited to any e-government services	Stream ciphers are difficult to implement correctly, especially in a citizens environment

2.5. Chapter Summary:

This chapter discussed the literature review, this after viewing the governmental e-services and its benefits, where the growth usage of e-government will raise some threats, the issue that lead to provide secure access and build agency trust.

The related works on this chapter discussed electronic voting, e-transactions, e-passport as application of e-governments which need to be highly secured, the chapter shows the existing models e-government assessment.

Finally the chapter views the cloud computing, Mobile government, biometric and digital signature in e-government as a new trends applications and technology that need to provide security.

CHAPTER III

Research Methodology and proposed Solution

3.1. Introduction

This chapter is about stating the initial concept of the proposed solution, the research methodology and approach that assist in developing the authentication framework for secure e-government, the chapter illustrates a case study about Sudan e-government, showing the data which are collected through questionnaires and interviews, and then presenting case study findings. The chapter also presents a simulation model for e-government authentication and the provided tools and techniques for evaluation and testing.

3.2. Research Methodology:

The choices that the research made in the research methodology are related to the research problem and objectives, this research rely on developing approach with integral models for securing e-government networks, and because of interdisciplinary nature of research, where e-government is considered on the field of Information systems which encompasses five components: data, software, hardware, people and procedures, hence e-government deals with ICT, ergonomics and political polices, moreover providing security to e-government is depend on the computer network technologies risks and human risks, that is why it require adopting different methodologies related to area of the research, although it conducted a mix-method (Saunders et al, 2003) systematic qualitative and quantitative research approach.

The research philosophy is to use methods and processes to contribute to knowledge, the researcher make clam about nature of knowledge (ontology), how we know it (epistemology), what values it holds (axiology), how we write about it (rhetoric), and what processes to studying it (methodology) (Creswell, 2007). In this Study knowledge are obtained through literature review, related works and data gathering aiming to contribute to information security for building a framework to authenticate e-government services, the value of this research will reflect on the citizens involvement in Sudan e-government, providing better e-services and assist governmental authorities access information on a constant security level.

This research implied empirical research in the research design via case study strategy and survey research method is considered to be an appropriate approach to examine the citizens, awareness, perception, attitude, acceptance, adoption of electronic Government in Sudan, and security experience in using E-government services.

A case study strategy is conducted to collect the required data using two questionnaires, Questionnaire I for Sudan e-government citizen and Questionnaire II for Sudan e-government Administrators.

Questionnaire I is to collect data from Sudan citizens, where this study is descriptive aiming to find facts that can assist Sudan e-government initiatives for best citizen's adoption. It also provide basic understanding for citizens needs as the effective factors of e-government adoption.

The study is done after surveying citizens who already have e-government experience in Sudan, Questionnaire I is designed to answer questions around (citizen's computer and Internet Knowledge, their security experience, to what extent they are familiar with e-government, and their expectations on Sudan e-government initiatives and development). On this study a non- probability based sampling technique is used, a sample is taken from undergraduate students whom experienced in e-government service in apply the new intake for Sudan universities under the supervision of Ministry of High Education and Scientific Research.

Questionnaire II is to collect data from E-government administrators in Sudan to examine readiness for secure infrastructure in Sudan E-government.

The research process will follow the following steps:

a) Extensive literature review:

   Conducting a comprehensive and critical literature review, investigating existing models and security standards, e-government applications and e-services.

b) Analyzes information to Identify requirements:

   Data collected from literature review are useful to prepare the case study, identifying the required questionnaires and Interview questions that can meet the research objectives and assist in designing the authentication framework for e-government.

c) Case Study:
d) Develop the solution and design framework:
e) This an iterative step stating developing the initial solution and refine the requirements according to the given information and case study findings.
f) Test Validity and reliability:

   The framework being developed need to be tested and verify its efficiency and reliability, using standard tools to design a novel framework that meet the research objectives and for framework benchmarking, else the framework need to fine-tuned and adjusted.
g) Writing Dissertation:

   Writing process in conjunction with the publication

Figure 3.1 shows the flowchart of the research methodology.

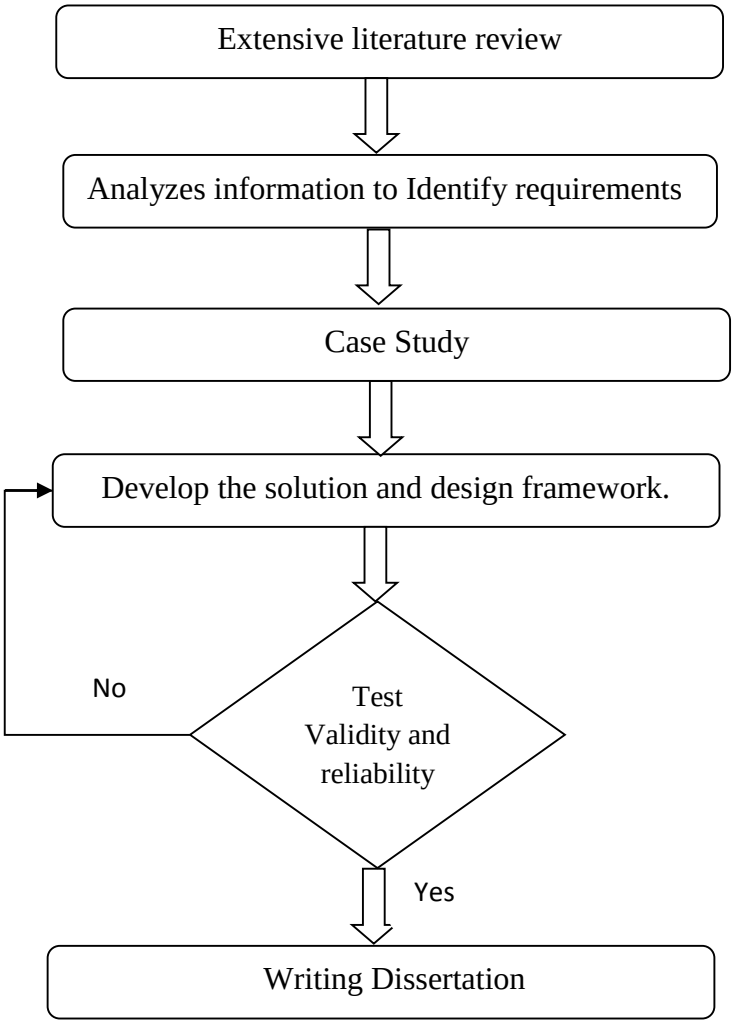

Figure 3. 1: The flowchart of the research

3.3. Proposed Solution:

The research relay on designing an authentication framework in an appropriate approach to secure Access of e-government services, where this approach might need to encompasses multi-model of security models and standards to work in efficient security environment, that compromises both of technical and non-technical issues and to be applied.

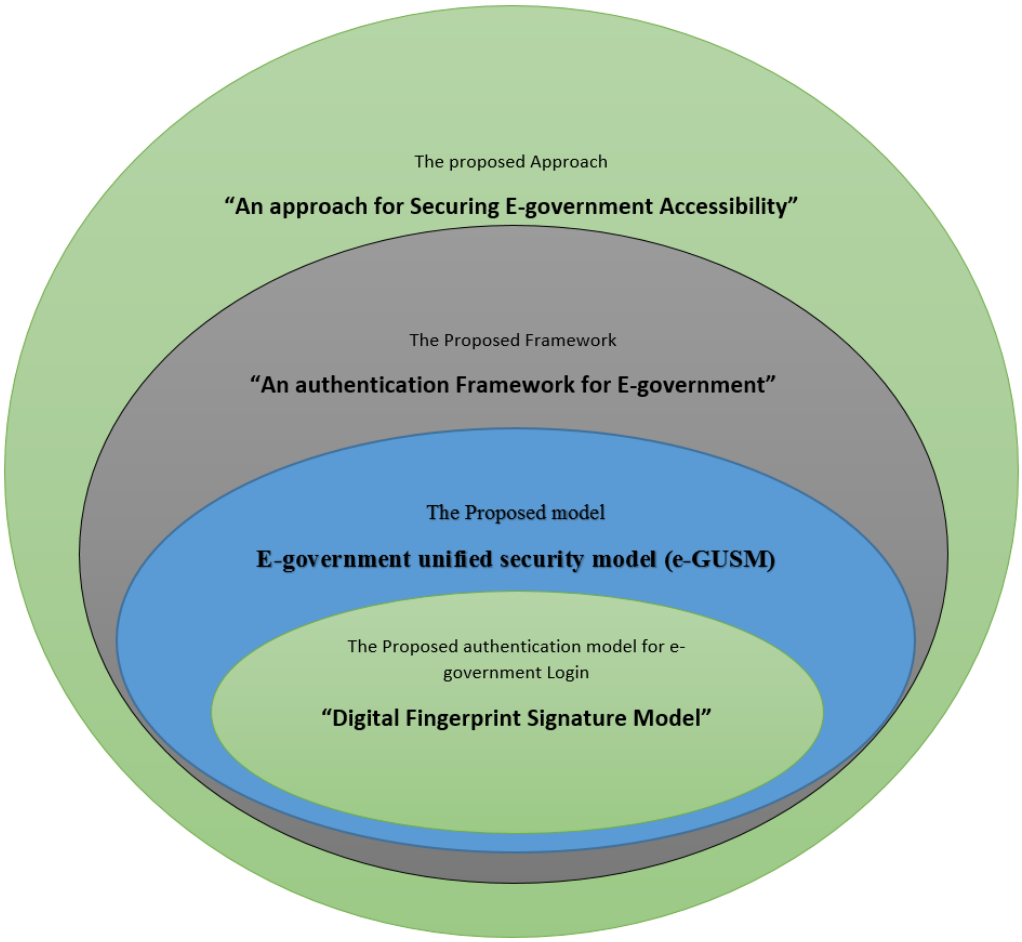

Figure 3. 2: Illustration of the Proposed Solution

3.3.1. The proposed approach:

Figure 3.2 illustrates the holistic idea of the research which represent the proposed solution that provide a framework and providing the following approach:

1. State security requirements of e-services: review what/how/when to access information; state the priorities and privileges according to e-service.
2. State security strategies: according to security requirements state the strategy and the defense mechanism wither (diversity of defense, defense in depth, choke point, and weakest link, least privilege, etc) it’s recommended to combine mixed defense mechanism.
3. State security policy: once the requirements and strategies states well, it’s time to write down a document as a regulations and procedures of incident handling to adhere every one for the acceptable use.

4. Evaluation: test the validity of the authentication framework.
5. Risk assessment and review: this step may lead to recycle step one in the approach.

3.3.2. The proposed authentication framework for e-government:

1. Establishment of identity through providing secure level of registration, where user has account credentials (national number).
2. Providing levels of authentication of each e-government application and according to network infrastructure,
3. including appropriate security certificates and
4. Building appropriate PKI (public key infrastructure) for e-government.

3.3.3. The proposed e-Government Unified Security Model (e-GUSM):

Securing e-government is like securing any Internet based application such as e-commerce (Maria , Bianca, 2002), However authentication process in e-government is more than providing technical issues, so providing UTAUT to insure the nontechnical issues may assist to have full compliance.

So constructing a framework need to review the strength and weakness of existing framework/models/approaches. Figure 3.3 illustrates proposed approach that tackle both technical and non-technical issues act as a unified model for securing e-government by integrating the existing models and theories according to requirements, **e-government unified security model (e-GUSM)**, this may consider an appropriate model to gain trust.

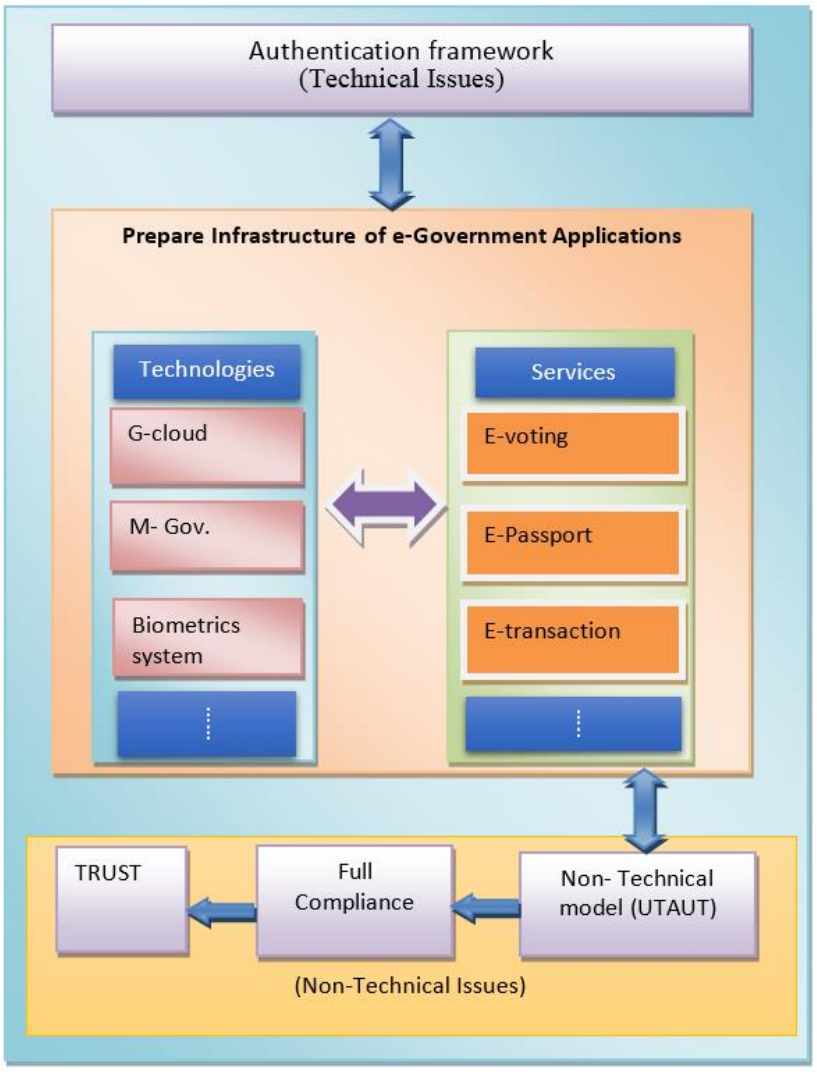

Figure 3. 3: eGUSM block diagram

3.4. Case Study (Sudan E-government):

The case study followed empirical research that utilized quantitative method conducting a case study strategy in Sudan e-government the Case Study is to examine the validity of the proposed solution, where we need to study the current applications in Sudan e-government. E-government has recently emerged in Sudan and other developing countries, but many issues remain problematic.

E-government services for citizens include tax payments, renewing licence and electronic voting …etc. (Quanxi, Elhadi , 2014), much more services can be done electronically, and make use of ICT to increase number of services done per a unit of

time, hence citizens Plame government in case of any delay, unproductive or unresponsive for their basic needs (Muhammad , 2011) and for that matter Sudan e-gov tries to adopt a perfect e-services for their citizens.

Sudan is considered as a developing country and tries to deploy the use of electronic culture and have all the benefit of ICT, although Sudan has a powerful position in telecommunications, there are more than three mobile phone companies competing to provide best services and wide Internet coverage, hence for more convenient citizen e-services e-government projects have been identified as one of the top government priority areas in Sudan (Mohammed et al, 2012), (2015 ، مجلة السودان الرقمية).

The government in Sudan adopted e-government as a solution to facilitate communication and connectivity between different parts of the government institutions and departments, therefore E-government in Sudan has great growth and development phase to provide e-services to citizens, all efforts concentrate on to expand the networks and availability of Internet, hence infrastructures are prepared to connect all agencies electronically.

3.4.1. Sudan E-government:

Sudan E-government initiative started in 1990s, when ICT take great place in Sudan and the National Information Center is assigned as a former body that coordinate e-government in Sudan since 2004 (Sara, 2012) , Although e-government Applications has recently emerged in Sudan, E-government in Sudan implemented to decrease administrative costs, for governments and citizens (Quanxi, Elhadi , 2014), to design an efficient e-Government system, we need to examine Security experience in e-government Users Awareness, Perceptions and Attitudes to E-Government services adoption, however the internet usage and internet penetration has increasing significantly in Sudan. So, the security has become more critical factor in ensuring information and data privacy and protection (Quanxi, Elhadi , 2014).

Getting start in the case study need to investigate the current status of Sudan e-government websites and list all electronic citizen services and according to report about implementing e-Gov services in Sudan (2014) presented in a parliament session on 24/11/2014 from ministry of science and communication in Sudan. All government informatics projects in Sudan are controlled by National Information Center NIC

http://nic.gov.sd, where all governmental websites are hosted in, the NIC considered as a unit under Ministry of science and technology in Sudan(2015 ، مجلة السودان الرقمية).

A grate steps toward Sudan e-government adoption is done on 2015 through the web portalhttp://esudan.gov.sd/ , is designed to deploy awareness and disseminate information about the services that e-government can provide for citizens and other agencies.

3.4.1.1. Sudan Government to Citizen's e-services now:

1. Civil Registry: through this address http://reg.civil.gov.sd/, all citizens can start the process of form1 and
2. Sudan Custom e-service (http://customs.gov.sd/), the use of fingerprint in custom services (2014): the project now is partially electronic; citizens need to complete their transactions manually.
3. Electronic results of secondary certificateand electronic Admission for under graduate universities in Sudan (2014) and results :http://www.admission.gov.sd/
4. E-haj and Omera:http://www.haj.sudan.sd/, for apply for haj from Sudan starts 2015
5. E-souq: for farmers of north Kordofan State, http://www.nkordofan.gov.sd/, website rich of information and e-services.
6. Vacancy announcements, http://sudarecboard.gov.sd/
7. http://eastnile.gov.sd/ar/, Khartoum StateEast Nile Locality which considered a perfect service for citizens to do all locality services electronically.
8. SADAD service is a portal to a unified payment ,Electronic payment of electricity and water, customs, apply to universities, http://sadad.gov.sd/

3.4.1.2. Sudan secure e-government initiative:

e-Government of Sudan disseminate laws and security policies to govern and assure the flow of e-services, moreover a great effort is done for planning and disciplinary

actions should be taken to all who violate or misuse information in Sudan e-government, and the following is done(Mohammed et al, 2012):

- Computer Event Response Team (CERT)
- First draft of information security policy.
- Security Operation Centre (SOC).
- Adoption of Encryption Key.
- Block websites that effect on ethics and behaviour of Sudan society.

Information security Laws:

- Cyber-crime Law (2007).
- Electronic transaction law (2007).
- National Information Centre Law (2010).
- Unified Number Law (2012).
- Information Access Law (2011).

Security policies:

- Application Development Policy.
- Employee third party policy
- General Policy
- Hardware security policy
- Internet Plociy
- Malware Policy
- Network Policy
- Operation management policy
- Ownership –save data policy
- Passing Control policy
- Work continue policy

All these laws and security policies available online in http://nic.gov.sd/ and e-gov Sudan portal http://esudan.gov.sd

3.4.2. Questionnaire I:

While E-government strives to provides delivery of public services in a much more convenient and cost-effective way, offering huge opportunities to improve public sector efficiency. The aim of this Questionnaire is to examine the citizens' awareness and acceptance of Sudan e-government adoption and security perspective in Sudan. In this questionnaire questions were asked to provide insights of accepting adopter of e-government initiatives. Questionnaire I is included in Appendix A.

The findings revealed that Sudan citizens accept the use of e-government and they are fairly familiar with e-government services, however they are not aware of security aspects and afraid to use the online services.

3.4.2.1. Questionnaire and Data Collection:

The questionnaire was used for data collection for this research as it is an efficient means to gain data from participant; it is an appropriate and an effective method to investigate people's attitudes and opinions, regarding particular issues. In this research, a total 87 respondents completed the questionnaire, about citizens' awareness, perception, attitude, acceptance, adoption of electronic Government, and security experience in using e-Gov service, it is provided in both Arabic and English languages.

3.4.2.2. Data Collection and Analysis:

Data are collected using questionnaire and analyzed using SPSS v.16 with 68 variables and 87 observations, observations are freshmen students who use the online admission to universities for the academic year 2014/2015 in Sudan, the sampling has been selected from Students on the first year of Engineering department - Bayan College of Science and Technology- Sudan, it's worth to mention that the online admission system is used for the first time in Sudan.

3.4.2.3. Findings of Questionnaire I:

Data from questionnaires shows in Table 3.1 that most of Respondents are so young; however they are intermitted Internet and computer users.

Table 3. 1: Demographic information (DI)

Demographic information (DI)			**Percent %**
DI1	Gender	Female	31.0
		Male	69.0
DI2	Age	(16-20)	75.6
		(21-30)	23.3
		(31-40)	1.2
		(41-50)	0
		(51-60)	0
		More than 60	0
DI3	Do you have national number?	Yes	100.0
		No	0
		I am going to have	0
DI4	Computer knowledge:	Poor	3.5
		Moderate	39.5
		Good	34.9
		Very good	22.1
DI5	Internet knowledge	Poor	0
		Moderate	23.3
		Good	32.6
		Very good	44.2
DI6	Do you consider yourself you can use computer application easily?	Yes I always can	40.7
		Sometimes I can	52.3
		No I can't	2.3
		Not sure	4.7

Table 3. 2**:** Security experience in e-government (SEE)

4. Security experience in e-government (SEE)			**Percent %**
SEE1	Is it necessary to know about security of e-Government?	Not important	15.1
		Almost important	33.7
		Quite important	51.2
SEE2	Do you change password?	Yes frequently	26.7
		Almost from time to time	46.5
		Not at all	26.7
SEE3	Do you ever give passwords to one you trust?	yes because I always forget	2.3
		Yes sometimes	36.0
		No, never	61.6
SEE4	Do you ever write down passwords?	yes because I always forget	8.2
		Yes sometimes	29.4
		No, never	62.4
SEE5	Do e-Gov services available when it is requested?	Yes always available	10.6
		Sometimes not available	50.6
		Rarely available	38.8
SEE6	Do you mind the use of fingerprint as an identification process?	Yes I oppose	14.1
		No, never mind	68.2
		Don't care	17.6
SEE7	Do you prefer the use of fingerprint in all e-Gov services?	Strongly prefer	45.9
		Somewhat prefer	30.6
		Somewhat oppose	9.4
		Strongly oppose	4.7
		Not sure	9.4
SEE8	Do you think that Internet has enough safeguards that make you comfort to use e-services?	Yes always available	29.1
		Sometimes not available	48.8
		Rarely available	11.6
		Not sure	10.5
SEE9	Do you feel confident when you submit all required information to e-Gov services?	Yes always confident	27.9
		Sometimes confident	40.7
		Rarely confident	20.9
		Not sure	10.5
SEE10	Do you know what cyber-regulation that governs the use of e-Gov services?	Yes I know all of them	25.6
		I know some of them	69.8
		I don't know any of them	4.7

SEE11	Evaluate your e-service reliability?	Not reliable	8.2
		moderate reliability	47.1
		high reliability	44.7
SEE12	Do e-Gov services work according to what you expect?	Yes they do as expected	8.1
		Sometimes they do	47.7
		No, they don't	33.7
		Not sure	10.5
SEE13	Can you access to all information you need?	Yes I always can	22.1
		Sometimes I can	48.8
		No I can't	17.4
		Not sure	11.6
SEE14	What cause citizens not to use e-government?	Not easy to use	4.6
		security issues	55.2
		Others	39.1
SEE15	Are you affected by unstable economical/political condition in the country?	Yes I do	36.8
		Sometimes I do	21.8
		No, I don't	20.7
		Not sure	20.7
SEE16	Do you receive enough information about what/how/when to access e-Gov services?	Yes always available	10.3
		Sometimes not available	34.5
		Rarely available	40.2
		Not sure	14.9
SEE17	Do you have technical/nontechnical facilities to access e-Gov services?	Yes always available	44.2
		Sometimes not available	34.9
		Rarely available	15.1
		Not sure	5.8
SEE18	Do you depend on others to help you access/use e-Gov services?	Yes I always depend on someone	10.3
		Sometimes I depend on someone	52.9
		I Don't depend on anyone	36.8
SEE19	Do you rely on the process of issuing national number?	Not reliable	39.1
		moderate reliability	26.4
		high reliability	34.5

Table 3.2 shows respondent's security experience in using e-government especially their experience in online admission for universities, where 61% confirmed that they never give password credentials to any one, moreover 62% of them didn't write down their passwords, however only 33.7% confirmed the importance of secure e-Gov applications.

The experiment of online admission shows that 50.6% of Respondents suffer from the availability of the e-service, 48.8% says that sometimes there are a good internet safeguards, however they are not confident that much, hence only 27.9% feel confident when they submit all required information to e-Gov services, therefore they agree and never mind to use fingerprint on all e-Gov applications and its worth to mention that 69.8% of them know about cyber regulations.
39.1% of respondent don't rely on the process of issuing national number and 36.8% agreed that they are affected by the unstable economical/political condition in the country, however they might not to use e-Gov services as 55% expected for security reasons!.
52.9% of Respondants sometimes depend on others to help access/use e-Gov services, although 44.2% of them have technical/nontechnical facilities to access e-Gov services.

The results: a Sudan young citizen afraid to use eGov, although they don't realize the major attacks that come across using e-Gov services.

Table 3.3 below represent to what degree Respondents are fairly familiar with e-government, although the only e-Gov service they use is the online Admission for universities, a round 40% thought that e-Gov services has a positive effect on citizens and as expected for 5 years long later it will take a better effect. Fortunately 62.8% confirmed that they are favor e-government as the primary means for obtaining information and services from government, however 37.9% argued its high a priority should be for government to invest tax money in making information and services available over the Internet.

Table 3. 3: Users Awareness, Perceptions and Attitudes (UAPA)

Users Awareness, Perceptions and Attitudes(UAPA)			Percent %
UAPA 1	How familiar you are with "e-government"?	Very familiar	13.8
		Fairly familiar	28.7
		Just somewhat familiar	27.6
		Not at all familiar	17.2
		Not sure	12.6
UAPA 2	Overall, what effect would you say e-government is having on the way government operates?	Very positive	19.5
		Somewhat positive	23.0
		Neutral	21.8
		Somewhat negative	10.3
		Very negative	9.2
		Not sure	16.1
UAPA 3	And, looking ahead three to five years what effect do you think e-government will have on the way that government operates?	Very positive	32.2
		Somewhat positive	27.6
		Neutral	17.2
		Somewhat negative	3.4
		Very negative	6.9
		Not sure	12.6
UAPA 4	In your view, how high a priority should it be for government to invest tax money in making information and services available over the Internet?	Very high priority	20.7
		High priority	17.2
		Medium priority	26.4
		Low priority	4.6
		Very low priority	13.8
		Not sure	17.2
UAPA 5	Would you favor or oppose e-government as the primary means for obtaining information and services from government?	Strongly favor	25.6
		Somewhat favor	37.2
		Somewhat oppose	9.3
		Strongly oppose	8.1
		Not sure	19.8
		Strongly favor	0

The following construct that the questionnaire is built on it and represent the frequency percentages: Data from questionnaires that most of Respondents are so young; however in Figure 3. 5 shows they are intermitted Internet and computer users.

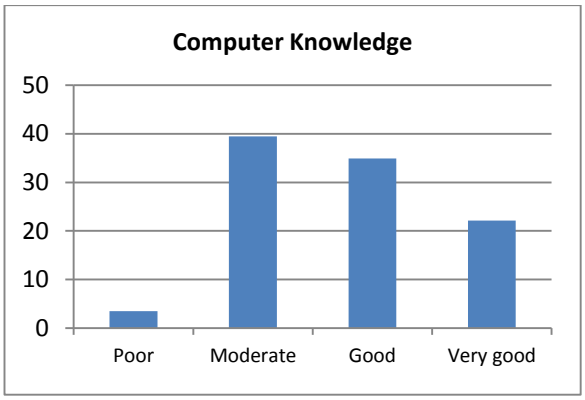

Figure 3. 4: Computer Knowledge

Figure 3.4 shows respondents experience in computer especially their experience in online admission for universities; where from Figure 3.861% confirmed that they never give password credentials to any one, moreover 62% of them didn't write down their passwords, however only 33.7% confirmed the importance of secure e-Gov applications.

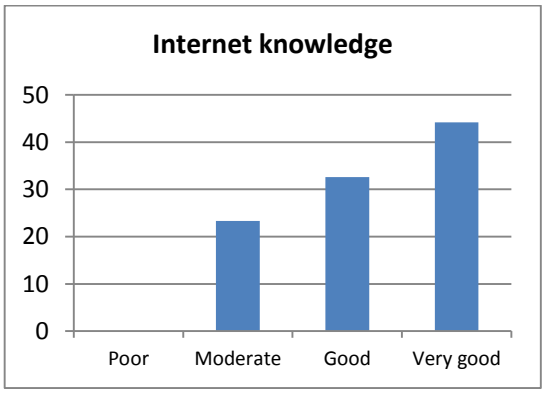

Figure 3. 5: Internet Knowledge

The experiment of online admission shows that 50.6% of Respondents suffer from the availability of the e-service, 48.8% says that sometimes there are a good internet safeguards, however they are not confident that much, hence only 27.9% feel confident when they submit all required information to e-Gov services, therefore they agree and never mind to use fingerprint on all e-Gov applications and its worth to mention that 69.8% of them know about cyber regulations.

39.1% of respondent don't rely on the process of issuing national number and 36.8% agreed that they are affected by the unstable economical/political condition in the

country, however they might not to use e-Gov services as 55% expected for security reasons!.

52.9% of Respondents sometimes depend on others to help access/use e-Gov services, although 44.2% of them have technical/nontechnical facilities to access e-Gov services. Figure 3.6shows the uses awareness of security in e-Gov.

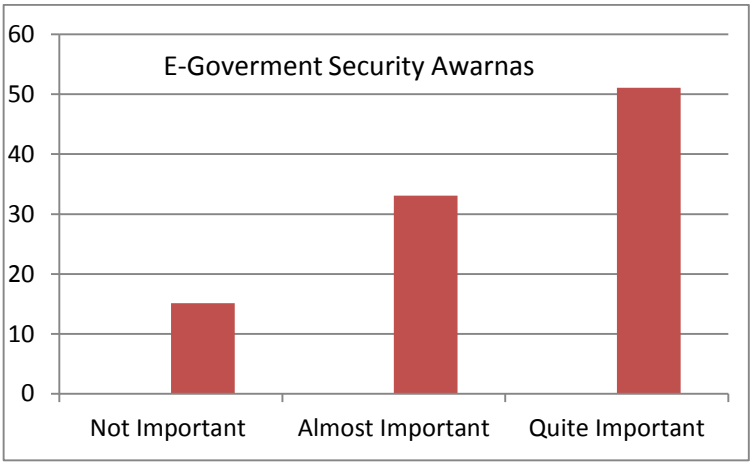

Figure 3. 6: shows the uses awareness of security in eGov

Figure 3.7 shows that the respondents depend on others to help access/use e-Gov services

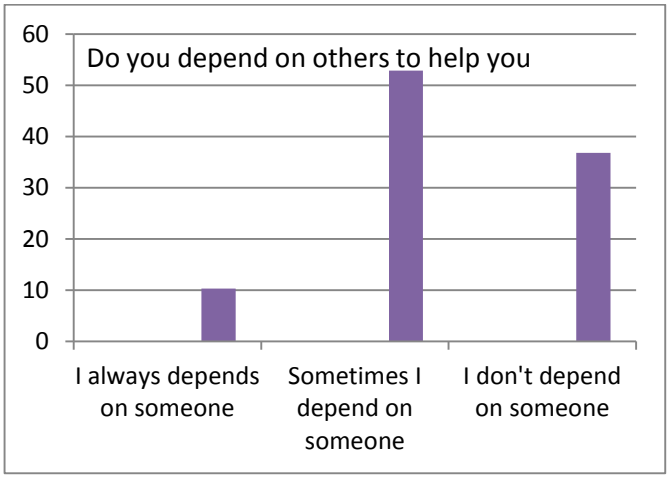

Figure 3. 7: shows that the respondents depend on others to help access

The next paragraph regarding Security experience in e-government (SEE). The following Figure 3. 8, Figure 3. 9, Figure 3. 10 and Figure 3. 11 show the users experience of security e-Gov.

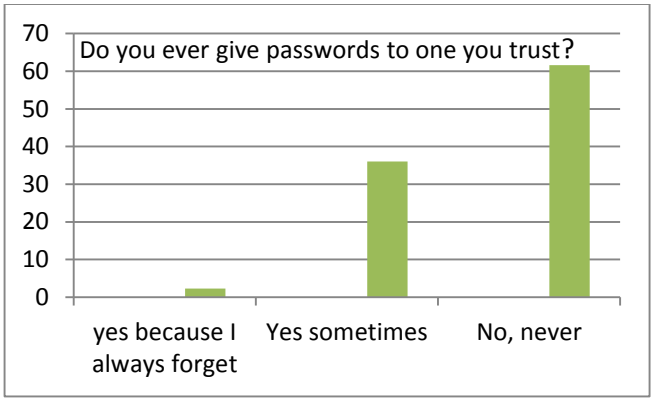

Figure 3. 8: Do you ever give passwords to one you trust?

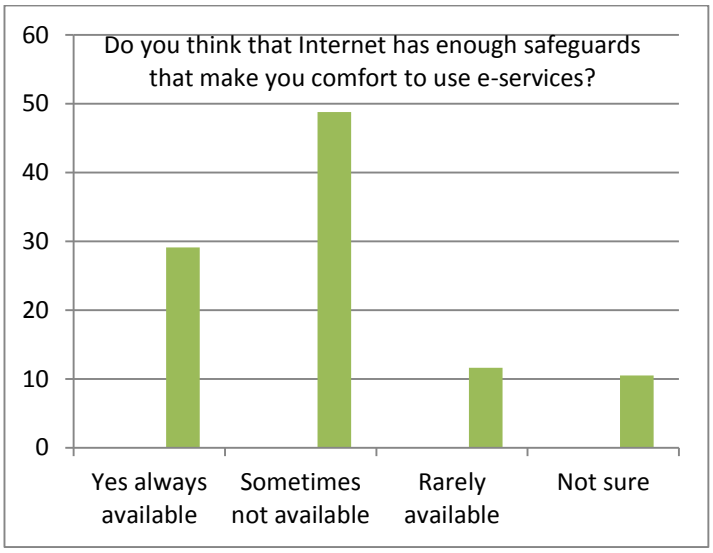

Figure 3. 9: Do you think that internet has enough safeguards that make you comfort

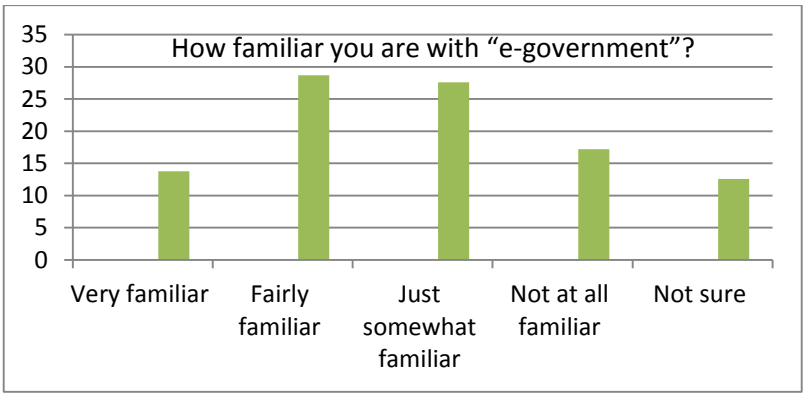

Figure 3. 10: how familiar you are with e-government?

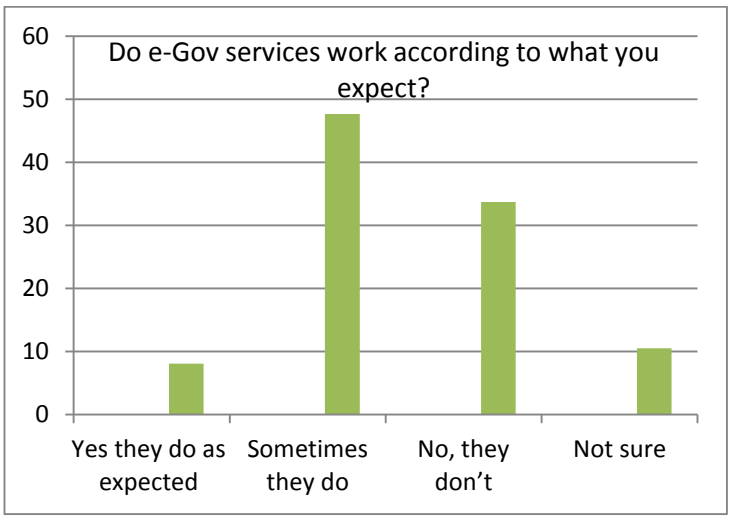

Figure 3. 11: Do e-Gov services work according to what you expect?

The following information is the valid frequencies percentage through five-point scale with the following anchors: 1- Strongly disagree, 2- Disagree, 3- Neither agree nor disagree, 4- Agree, 5- Strongly agree, on the survey on to which degree e-government is offering service to citizens and is the basic infrastructure quite enough to develop e-government in Sudan.

Table 3.4 presents to which degree respondent agree and disagree with e-Government services in Sudan, 69% of Respondents agree with e-government online services can be effective in providing government information to the citizens, where government of Sudan adopted e-government applications as a solution to facilitate communication and connectivity between different parts of the government institutions, agencies and citizens, and so 60.7% of respondents agreed on they can communicate with e-government service provider online to receive the desired information.

62.6% agreed on Internet Services is easily available in their area, and most of the people have access on the Internet and computes as 75% agreed on; however the speed of Internet and the quality of service is not quite enough to access the e-government services as 53.6% agreed on if we compare it with the wide usage.

Table 3. 4: e-Government Development in Sudan

e-Government Development in Sudan		**Strongly Disagree**	**Disagree**	**Neither Disagree nor agree**	**Agree**	**Strongly Agree**
ED1	Online services of e-government can be effective in the provision of governmental information to citizens.	9.5%	9.5%	11.9%	46.4%	22.6%
ED2	Citizens can communicate online with e-government service provider to gain the wanted information.	14.3%	4.8%	20.2%	41.7%	19.0%
ED3	Internet Services is easily available in your area.	10.8%	14.5%	12.0%	26.5%	36.1%
ED4	Internet band service and quality of service is good enough to access the e-government services.	20.2%	11.9%	14.3%	23.8%	29.8%
ED5	Most of citizens have access to Internet connections and computers.	11.9%	7.1%	6.0%	22.6%	52.4%

Table 3. 5: Barriers and challenges to E-Government services adoption (BCEA)

Barriers and challenges to E-Government services adoption (BCEA)		Strongly Disagree	Disagree	Neither Disagree nor agree	Agree	Strongly Agree
BCEA 1	Inadequate understanding of advantages of E-Government	15.7%	6.0%	20.5%	31.3%	26.5%
BCEA 2	Lack of knowledge and ability to use computers and technology efficiently	9.8%	7.3%	18.3%	43.9%	20.7%
BCEA 3	Lack of knowledge about the e government services	10.0%	5.0%	21.2%	43.8%	20.0%
BCEA 4	Lack of security and privacy of information in government's websites	21.0%	8.6%	17.3%	32.1%	21.0%
BCEA 5	Lack of users' trust and confidence to use e-government services	11.4%	17.7%	22.8%	25.3%	22.8%
BCEA 6	Lack of policy and regulation for e-usage in Sudan	18.5%	12.3%	27.2%	22.2%	19.8%
BCEA 7	The availability and reliability of internet connection	13.4%	13.4%	18.3%	32.9%	22.0%
BCEA 8	Insufficient access to internet	21.7%	10.8%	26.5%	18.1%	22.9%

Table 3. 5 investigate on barriers and challenges to e-Government services adoption in Sudan where 63% agree on Lack of knowledge about the e government services and Lack of knowledge and ability to use computers and technology efficiently are the most barrier of use e-government in Sudan moreover 57.8 agree on that there is inadequate understanding of advantages of E-Government is another next barrier.

48.1%agree on Lack of users' trust and confidence to use e-government services and around 53.1% agree on Lack of security and privacy of information in government's websites however less agrees on Lack of policy and regulation for e-usage in Sudan as e-government barriers.

In spite of 54.9% agree on the availability and reliability of internet connection, others 41% agree on insufficient access to internet as another barrier.

Table 3. 6 provide a general overview about Sudan Cultures and privacy on the use of current e-government services,

Privacy and personal information:

44.40% feel unsafe to use e-government services

36.40% feel that the risks outweigh the benefits of using e-government services

55.20% feel I must be cautious when using e-government services

45.30% personal information may be used in an unintended way by the governmental agency.

58.20% someone can snatch my personal information while I'm sending the information to a governmental website

57.70% Hackers may be able to intrude governmental websites and steal my personal information stored on the web

Trust

52.00% believe that there could be negative consequences from using e-government services.

40.30% risky to interact with an e-government service.

59.80% trust e-Government website when it assures me of the security it provides

62.00% trust e-Government website when it usually ensures that transactional information is protected from any accidentally being altered or destroyed during a transmission on the Internet

58.80% trust e-Government website when there is an effective mechanism to address any violation of my personal information

61.30% would use e-Government website when the technologies supported by the system are reliable all the time

67.60% would use e-Government website when the technologies support the system are secure all the time

70.00% would use e-Government website when the legal and technological structures are adequately to protect me from problems on the Internet

60.00% trust e-Government website when it is provide a valuable service for me

Table 3. 6: Cultures and Privacy (CP)

Cultures and Privacy (CP)		Strongly Disagree	Disagree	Neither Disagree nor agree	Agree	Strongly Agree
CP1	I feel it is unsafe to use e-government services	20.3%	16.5%	19.0%	20.3%	24.1%
CP2	I feel that the risks outweigh the benefits of using e-government services	16.9%	20.8%	26.0%	22.1%	14.3%
CP3	I feel I must be cautious when using e-government services	16.7%	9.0%	19.2%	30.8%	24.4%
CP4	I believe that there could be negative consequences from using e-government services.	12.0%	16.0%	20.0%	32.0%	20.0%
CP5	It is risky to interact with an e-government service.	13.0%	20.8%	26.0%	23.4%	16.9%
CP6	My personal information may be used in an unintended way by the governmental agency.	10.7%	20.0%	24.0%	24.0%	21.3%
CP7	Someone can snatch my personal information while I'm sending the information to a governmental website	13.9%	10.1%	17.7%	36.7%	21.5%
CP8	Hackers may be able to intrude governmental websites and steal my personal information stored on the web	12.8%	9.0%	20.5%	32.1%	25.6%
CP9	I trust e-Government website when it assures me of the security it provides	7.8%	10.4%	22.1%	31.2%	28.6%
CP10	I trust e-Government website when it usually ensures that transactional information is protected from any accidentally being altered or destroyed during a	13.9%	10.1%	13.9%	36.7%	25.3%

	transmission on the Internet					
CP11	I trust e-Government website when there is an effective mechanism to address any violation of my personal information	10.0%	13.8%	17.5%	28.8%	30.0%
CP12	I would use e-Government website when the technologies supported by the system are reliable all the time	11.2%	8.8%	18.8%	37.5%	23.8%
CP13	I would use e-Government website when the technologies support the system are secure all the time	7.8%	7.8%	16.9%	32.5%	35.1%
CP14	I would use e-Government website when the legal and technological structures are adequately to protect me from problems on the Internet	11.2%	6.2%	12.5%	41.2%	28.8%
CP15	I trust e-Government website when it is provide a valuable service for me	13.8%	7.5%	18.8%	18.8%	41.2%

Reliability analysis

To verify how closely the survey measurements met the objectives of this study, before testing the proposed model, we performed a reliability analysis for the constructors composed by many items. Reliability is an assessment of the degree of consistency between multiple measurements of a variable. One type of diagnostic measure that is widely used and employed here is the Cronbach's alpha. Table 3. 7 shows the result values of Cronbach's Alpha, most of values higher than 0.70 which is considered reliable values.

Table 3. 7: Construct name

Construct name	Construct (number of items)	Cronbach's Alpha
Security experience in e-government	SEE(19)	0.654
Users Awareness, Perceptions and Attitudes	UAPA(5)	0.710
e-Government Development in Sudan	ED(5)	0.683
Barriers and challenges to E-Government services adoption	BCEA(8)	0.777
Cultures and Privacy	CP(15)	0.883

3.4.3. Questionnaire II:

E-government in Sudan has to provide e-services to citizens, all efforts concentrate on to expand the networks and availability of Internet, hence infrastructures are prepared to connect all agencies electronically, on this study a survey is done using a Questionnaire of e-government administrators and technical operator. The study investigate the challenges that faces administrators and technical operators in developing e-government in Sudan.

Questions on Questionnaire are validated with the aid of survey and results of Questionnaire I for citizens and Interview some administrators of Sudan e-government on NIC "National Information Center", measuring the current e-services and looking forward to suitable secure infrastructure for e-government services in Sudan. Questionnaire II is appended on Appendix B.

- Questionnaire respondents was 11 Sudan e-government administrators and technical operator in NIC "National Information Center" the former body that coordinate Sudan e-Gov portal.
- Job positions: Network & operator manager, IT infrastructure consultant, Director of infrastructure Department, 2 engineers, executive manager, assistant manager, 3 executive secretary and employee.
- Gender of respondents: 7 male and 4 female.
- Age: (21-30): 4 respondents, (31-40) : 3 respondents, (41-50): 2 respondents, (51-60): 2 respondents.

The questions of questionnaire II are stating as follows:

- Q2: Table 3. 8 represents the no. of respondents according to their Experience:

Table 3. 8:No. of respondents according to their Experience

1 year	4
2-4 years	0
5 year or more	3
More than 10 years	4

- Q2: Table 3. 9 shows that most of respondents agree with there is inadequate understanding of advantages of E-Government, where they assure that IT infrastructure of government public sector are free from weakness and completely ready for use.

  They thought that the need for Human resources to implement e-Gov services is sort and need to be increased.

Table 3. 9: adequent understanding of e-Gov usage

		Strongly Disagree	**Disagree**	**Neither Disagree nor agree**	**Agree**	**Strongly Agree**
2.1	Inadequate understanding of advantages of E-Government	1	1	1	6	2
2.2	IT Infrastructural weakness of government public sectors	3	3	2	1	1
2.3	e-Gov services infrastructure adequate and properly set?	0	4	2	3	2
2.4	There are no shortage of ICT Human Resource to implement e-Government	2	4	2	3	0

- Q3: Table 3. 10 shows that Respondents don't agree with that government employees misusing personal information on e-government, however they

agree with there are less personal privacy, and it might be vulnerable and exposed to exploiting by hackers.

Respondents assured that citizens without Internet access would get less government service, although it will become harder to get an answer from e-gov.

Table 3. 10: The potential negative things that may result from e-government.

	The potential negative things that may result from e-government.	**Strongly Disagree**	**Disagree**	**Neither Disagree nor agree**	**Agree**	**Strongly Agree**
3.1	Government employees misusing personal information	2	3	5	0	0
3.2	Hackers breaking into government computers	2	1	3	0	5
3.3	It will become harder to get an answer	2	1	2	4	2
3.4	Less personal privacy	4	0	1	2	4
3.5	People without Internet access would get less government service	0	1	1	0	9

- Q4: Table 3. 11 shows that Most of respondents assure the use of digital signature as an identification method in Sudan e-Gov, finger print and smart card are often used but no single sign-on method available in e-gov services.

Table 3. 11: use of digital signature

Biometric	3
Smart Card	3
Single Sign-on	0
Digital Signature	8

- Q5:Figure 3. 12 and Table 3. 12 show the challenges that can face e-government organization and administrative (Bushra , Salman, 2014),

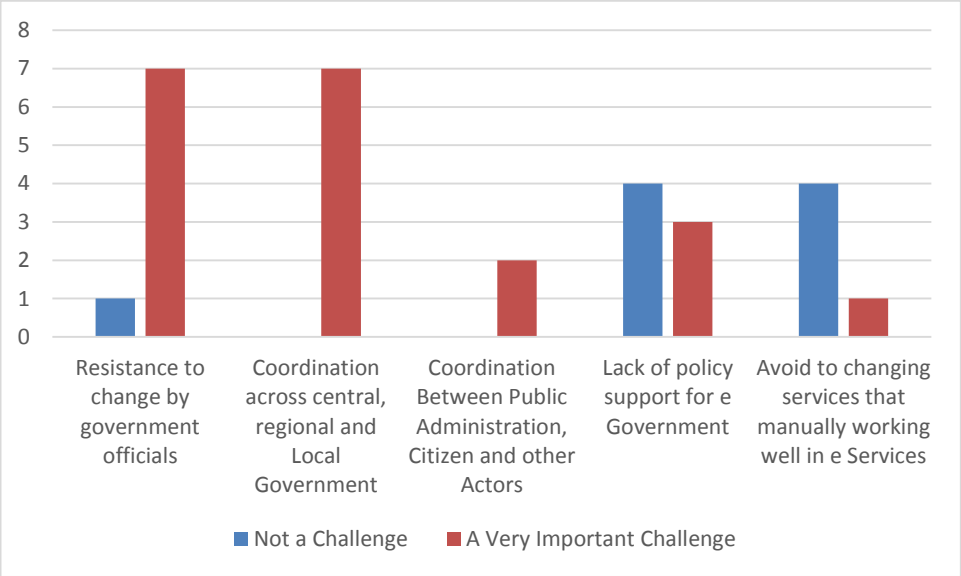

Figure 3. 12: Organizational and Administrative Challenge.

Table 3. 12: Organizational and Administrative Challenge

	Organizational and Administrative Challenge:	Not a Challenge	A Minor Challenge	An Important Challenge	A Very Important Challenge	Don't Know
5.1	Resistance to change by government officials	1	3	0	7	0
5.2	Coordination across central, regional and Local Government	0	3	1	7	0
5.3	Coordination Between Public Administration, Citizen and other Actors	0	0	9	2	0
5.4	Lack of policy support for e Government	4	0	1	3	3
5.5	Avoid to changing services that manually working well in e Services	4	1	3	1	2

- Q6:Figure 3. 13 and Table 3. 13 show the technical and design challenges that can face e-government administrators (Bushra , Salman, 2014),

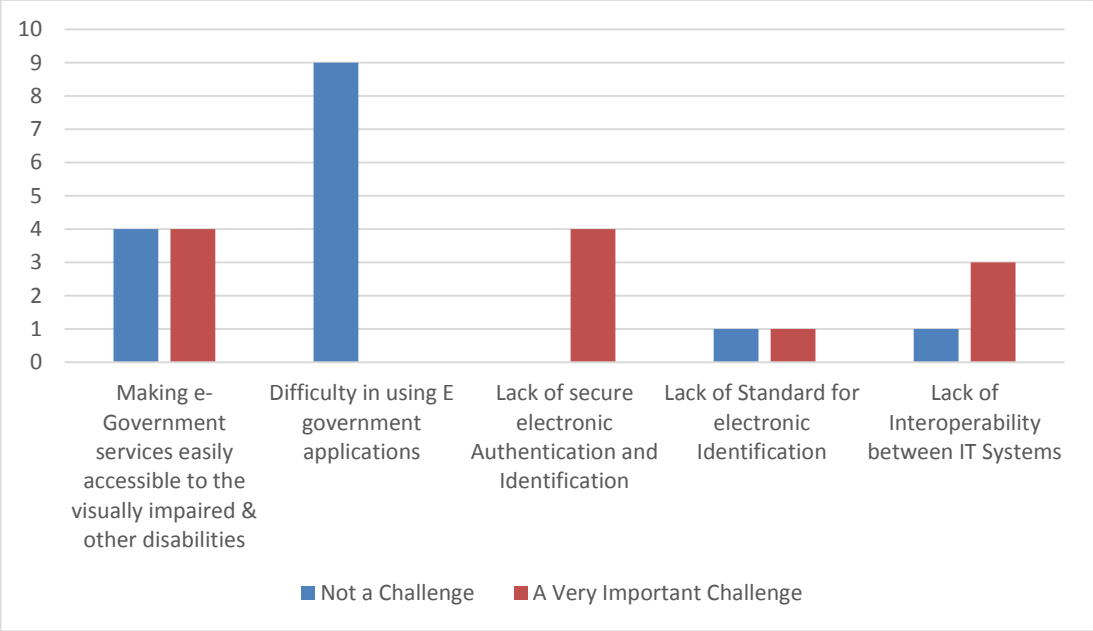

Figure 3. 13: Technical and Design challenge.

Table 3. 13: technical and desige challege

	Technical and Design Challenge:	Not a Challenge	A Minor Challenge	An Important Challenge	A Very Important Challenge	Don't Know
6.1	Making e-Government services easily accessible to the visually impaired & other disabilities	4	1	2	4	0
6.2	Difficulty in using E government applications	9	1	1	0	0
6.3	Lack of secure electronic Authentication and Identification	0	4	3	4	0
6.4	Lack of Standard for electronic Identification	1	6	3	1	0
6.5	Lack of Interoperability between IT Systems	1	4	2	3	0

- Q7: about e-Gov security standards (Yesser, 1426h), Sudan e-government uses infrastructure for security reasons on E-mail service S/MIME and PKI, for Transport protocol uses SSL, for Network protocol uses IPsce, and for Encryption it uses RSA encryption algorithm and it might be other security tools to secure all network layer.

  It is worth to mention that there is forensic lab for detecting and following any abuse and take disciplinary actions according to low regulations.

3.4.4. Interviews:

Questions were asked to Sudan e-government administrators in NIC :

- What e-government services provided to citizens now days in Sudan?
- Is Sudan e-Gov portal active now?
- What cultural gap do you perceive between citizens level oftechnological experience and the level of governmental web services that is being deployed?
- What are the main barriers (inconveniences) of applying e-government in Sudan?

- How important do you think the use of biometric technology is to e-government in Sudan? Are there any barriers to implement finger print technology in Sudan e-Gov?

3.5. Findings of the case study:

Citizens' acceptance and adoption of secure e-government services is an important goal for many governmental service providers, however the success of the adoption process is not easy and requires a thorough understanding of the needs of citizen's trust and system requirements. An analysis of data has been conducted.

It is worth to conclude that this study shows that respondents are fairly familiar with e-government, although there are very limited e-government services, they may use only the online Admission for Universities as the only e-service, and Sudan young citizen worried to use e-government, and meanwhile they don't realize the major attacks that come across using e-government services. In this study respondents of the questionnaire are young, although it can give insights to the next generation, synchronously with the development of Sudan E-government.

Increasing the number of governmental e-services in Sudan may help in citizen's e-government involvement, hence the more e-services are the more they depend on e-government.

A comprehensive survey on availability of Internet over wide areas in Sudan should be conducted, moreover the quality of services delivered through e-government should be suitable to citizen and make use of the telecommunications companies to deal with e-government as Internet service providers.

For security wise, it's good to recommend that to build secure e-government don't conduct a traditional user name and passwords in governmental websites, a biometric solutions is better to use to provide secure access for sensitive information, this may increase trust and confidence, hence gradually high e-government adoption percentage is achieved.

3.6. Research tools:

The research conducted case study and simulation tools, the case study needed an SPSS tool for analyzing data and testing validity of questionnaires, the simulation model for secure web login is a web-based system to applied using JavaScript/ HTML 5 and php, moreover testing and benchmarking tools that the research use is a penetration test of the simulated webpage, testing vulnerabilities to evaluate the simulation model.

3.7. Chapter summary:

This chapter is present the layering solution to Provide an authentication solution for e-government, this is done using Case study about Sudan e-government with the aid of two questionnaires and Interviews, where respondents involved were Sudan citizens and e-government administrators.

The findings of the case study help in designing a solution, where case study reveals the need to implement a technical model that insist using biometric fingerprint for login to sensitive governmental data

CHAPTER IV

Design the proposed Digital fingerprint signature model

4. Introduction

E-government is a website that provides reliable content based on a strong infrastructure of a digital network, application servers and internet, an extensive database and other supporting services (Ndou et al, 2004).

In this chapter evaluate the use of digital signature performance in e-government through various hash function over different web browsers, implementation results shows that SHA256 is the most suitable hash function to be used in DSA for authenticating E-government transactions. Taking this results in consideration to apply Digital Fingerprint Signature with the designated hash function.

4.1. Research Techniques:

The research depends on findings of the Sudan e-government case study, in addition to survey with the aid of literature review build a simulation model for secure access, the simulation will help in generalization and benchmark the proposed model.

4.1.1. Simulation technique and Parameters:

Most governments around the world trying to adapt the e-government as new government management techniques based on web platform where the use of information technology to enhance the effective management is taken place and because of the information warfare that found in the use of ICT, the idea of the simulation is built to make a check point strategy that serve as a gateway to secure access for e-government webpage, which may contain sensitive data such as civil registry. It requires more advanced and secure e-Government networks to protect data from growing security threats and risks. Threats include unauthorized access to resources, malicious damage, and data intercepts.

This research use a simulation to design Digital Fingerprint Signature Model, which is a web-based system developed using JavaScript/ HTML 5 and php, and to achieve authentication the user must login using his fingerprint, where the system verify the fingerprint and then sign the fingerprint with an digital

signature technique, then the severer check the validity of the digital signature and then permit the user to access the webpage.

The parameters that must be checked in the simulation system is to check predictability of cracking login to compromise authentication, moreover check performance and accuracy of functionality.

4.2. Design of the proposed model:

The importance of high confidence is require for any kind of transmission of data in various department of any government sector and it is obvious in case of administrative decision and financial context. The successful implementation of E-Governance depends mainly on the secured transmission of information between the Citizen and the Government. Intruders are generating smart ways to listen the information un-authentically whereas the information scientists have to find even smarter ways for neutralizing these attempts.

The proposed Digital fingerprint Signature Model is work as an authentication method to access e-government web-page that contains a high level of security, where these levels can be as follows:

Level 0 (Normal privilege): this level has no any secure mechanism, cause the data are deployed in pubic, this type suited with all disseminated e-services such as tourisms information, government procedures and policies.. etc.

Level 1(class privilege): this level is to use the standard user name/password login to access public information which need to classify users according specific criteria, this level suited with getting access of digital library, job vacancies, medical services etc..

Level 2 (highest privilege): this level is need to implement the proposed authentication model to access e-government information, this type of information considered as a sensitive data which need to be protected from unauthorized access, here the user must verify himself after identification process is done. This level suited with civil registry e-services, certificate issuance and personal documents services etc.

The idea of the Digital Fingerprint model is to insure authorized access to a governmental web page, this can be done after signing biometric fingerprint minutiae with digital signature, where Minutiae-based fingerprint extraction method is applied, and to obtain two verification process which yield a high level privilege and authorized access.

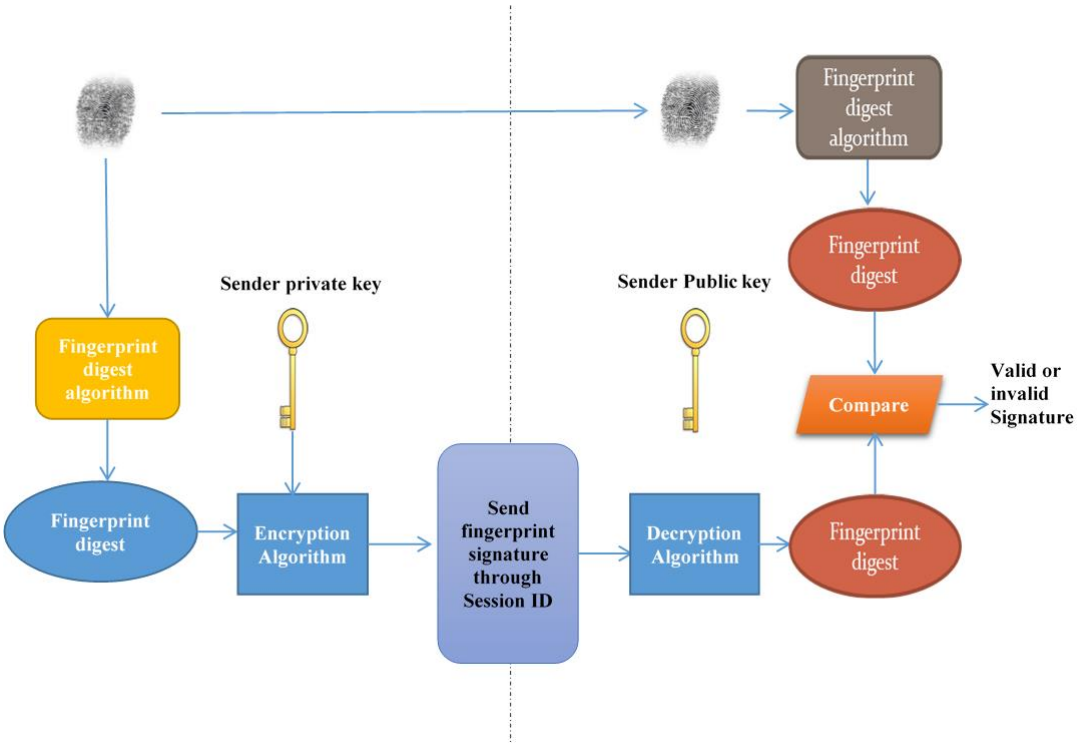

Figure 4. 1: Digital Fingerprint Signature Model.

Figure 4. 1 describe the model in context, where the client " citizen" who need to access governmental data through level 2 privilege, he must verify himself using biometric fingerprint, the client browser scan the fingerprint and extract minutiae points, these points are hashed and encrypted to create fingerprint signature. The fingerprint signature is sent by session ID for verification process by the server and tracking the client through his visit and use of information.

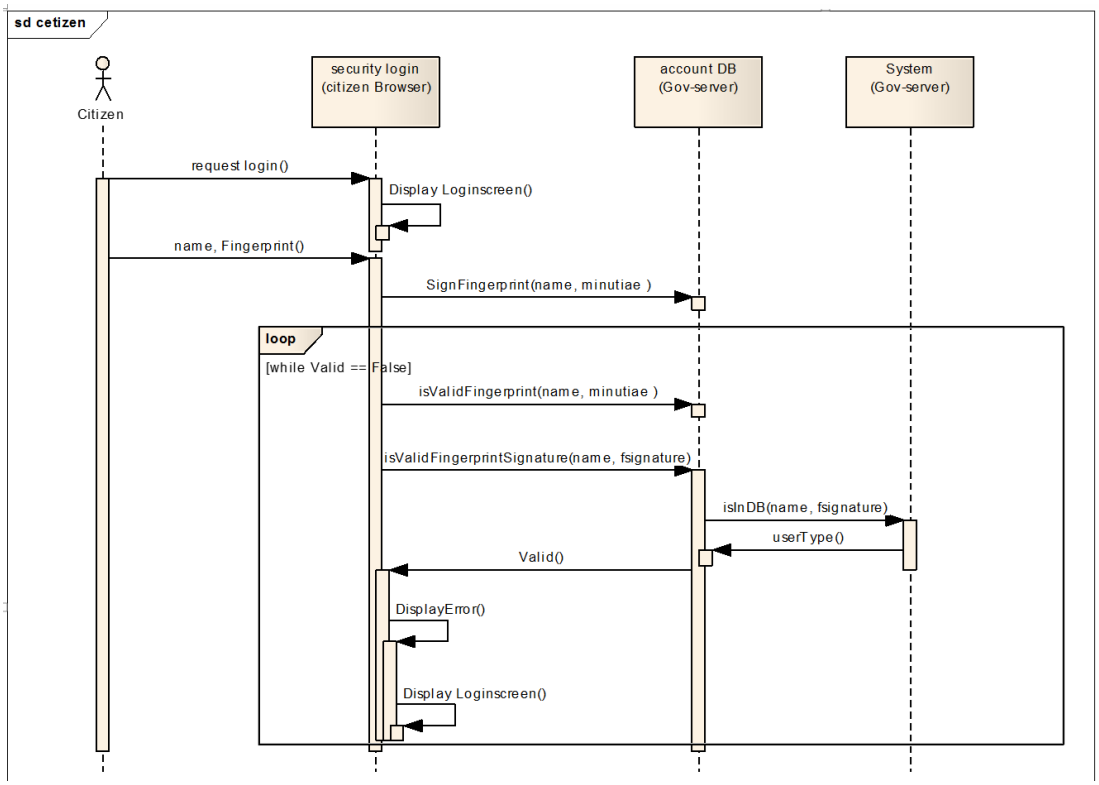

Figure 4. 2: UML Sequence Diagram of Digital Fingerprint Signature Model.

4.2.1. Sender-side block diagram

This block mainly contains functions that the client "citizen" do, Figure 4.2 describe a UML sequence diagram of Digital Fingerprint Signature Model. Citizen started to request a login through his Client browser, the login screen is viewed to prompt citizen to scan his Fingerprint and type his name as a signature, here the fingerprint will capture with the encapsulated encryption algorithm, then client browser will generate a signature from the name "citizen message" and his fingerprint minutiae, this signature will be sent to governmental server "Gov-server" account Database for check validity and authorization process.

4.2.2. Server-side block diagram

This block contains functions that governmental server "Gov-server" do, it will be obviously described in figure 4.2 the information flow and functions of the Digital Fingerprint Signature Model, while Gov-server receive the fingerprint signature through two levels, first check minutiae validity, then match

fingerprint signature with the fingerprint signature stored in DB to signature validity as a second level . If the signature is valid the citizen can get access as an authorized login to gov-information.

The case study in this research argued that Sudan citizens awareness of e-government services and security issues, they can share the user passwords in most e-government applications moreover some of them depend on others to do the process in stated of them!, here we can find the importance of the use of biometric fingerprint to access systems in e-government and insure/identify/verify users according to the level of security needed in the e-service. Meanwhile the study argued that citizens accept the use of fingerprint to access e-governmental services

4.3. Implementation of proposed model:

Here Digital fingerprint Signature is imposed by the sender Citizen and Digital fingerprint Signature should be verified by Receiver government in reality.

First the biometric fingerprint is hashed into a minutiae digest. Using this hashed value a Signer (government) digitally signs (encrypt) the minutiae digest using his private key. This signature is attached to the original Fingerprint and send by the sender.

After receiving the message, the receiver has to use the sender's public key to decrypt the minutiae digest and to ensure integrity authenticity. Confidentiality is also done and achieved by comparing designed message and message digest using same algorithm used. As in an electronic transaction system an intruder should not be able to find out what transaction a particular user is executing if confidentiality is properly maintained.

If the hash values of sender and receiver are equal, it serves to prove that the minutiae digest has not been tampered. With changing even one letter in the minutiae digest, the hash value would be changed.

Hence message integrity is assured. Non-repudiation is the cryptographic term describing the situation when the originator of a message cannot deny having sent it. Non-repudiation prevents from denying previous commitments or transactions from an entity.

4.3.1. Signature Generation

This scenario is between Citizen and Government (C2G) model of E-Governance for electronic identification of Citizen during these transactions with the Government to gain secure access.

Digital Fingerprint Signature Model scenario:

- Client will give a highest privilege security level and he must
- Register for authorization process: request for authorized account.
- Enrollment:
- Fingerprint reader Scans fingerprint.
- Extract fingerprint features and minutiae data
- Create Enrollment template (identification)
- Store enrolment template to server Data base.

Client login after registration and the signing process of fingerprint signature.

- Enrollment- client side :
- Fingerprint reader Scans fingerprint.
- Extract fingerprint features
- Create Enrollment template (identification)
- Sign the enrollment template (fingerprint digest)
- Submit enrolment template and fingerprint digest to server Data base.

Citizen signs the minutiae digest md to be sent using citizen A's private key:

1. Compute e = HASH (md), where HASH is a cryptographic hashing algorithm, (i.e. SHA-1)
2. Select a random integer k from [1, n − 1]
3. Compute r = x1 (mod n), where (x1, y1) = k * G. If r = 0, return to step 2
4. Compute s = k − 1(e + dAr)(mod n). If s = 0, return to step 2
5. The signature is the pair (r, s)

4.3.2. Signature Verification

Matching fingerprint digest (verification) –server side functions:

- Fingerprint reader Scans fingerprint.

- Extract fingerprint features
- Create match template and match digest.
- Compare match template to the Enrollment template and return score
- If valid fingerprint then compare match digest to fingerprint digest if valid verify user and permit access else access denied.

Receiver (Government) authenticates and verifies the minutiae digest using citizen A's public key.

1. Verify that r and s are integers in the interval [1,n − 1]. If not, the signature is invalid.
2. Compute e = HASH (md), where HASH is the same hashing algorithm used in signature generation.
3. Compute w = s −1 (mod n)
4. Compute u1 = ew (mod n) and u2 = rw (mod n)
5. Compute (x1, y1) = u1G + u2QA
6. The signature is valid if x1 = r (mod n), otherwise it is invalid.

4.4. Testing performance, accuracy and security in Browsers

E-government is a web-based system, therefore the implementation is done using web programing languages HTML 5, Java Script, PHP and MySQL. The system executed under 3 browsers: IE v.11, chrome v.47 and fire fox v.43 under the following system specifications: windows 8, 64-bit OS, core i5 1.70GHz 2.40GHz and 8GB of RAM.

Citizen webpage is designed to prompt citizen's Biometric Fingerprint to sign and choose one of 5 Digital Signature algorithms: SHA1, SHA256, SHA512, MD5 and RIPEMD-160, then citizen submit signature to be verified by government web page, Encryption is done using RSA. On this section dedicated to compare between which HASH algorithm to use for digital Fingerprint Signature Model.

4.4.1. Performance Evaluation:

Test the performance is done on the client side to measure the execution time of signature generation which is done using JavaScript code running on browsers as follows:

4.4.1.1. Internet Explorer v. 11:

The estimated execution time in milliseconds of signing process running under IE v.11 with different Hash functions and different message size as shown on Table 4. 1, the more we increase message size the more execution time, from Figure 4. 3 we can observe the MD5 Hash algorithm is the most faster than SHA1, SHA256, SHA512 and RIPEMD-160.

Its worth to mention that all these Hash functions can operate on up to 2^{64} -1 except SHA512 where the maximum message size can be 2^{128} -1.

Table 4. 1: the estimated execution time in milliseconds of signing process running under IE v.11

Message Size	SHA1	SHA265	SHA512	MD5	RIPEMD-160
2kb	203	209	204	150	168
29kb	193	213	263	212	226
2000kb	1761	2173	5576	1376	4991
10000kb	7305	9780	25212	8644	23715

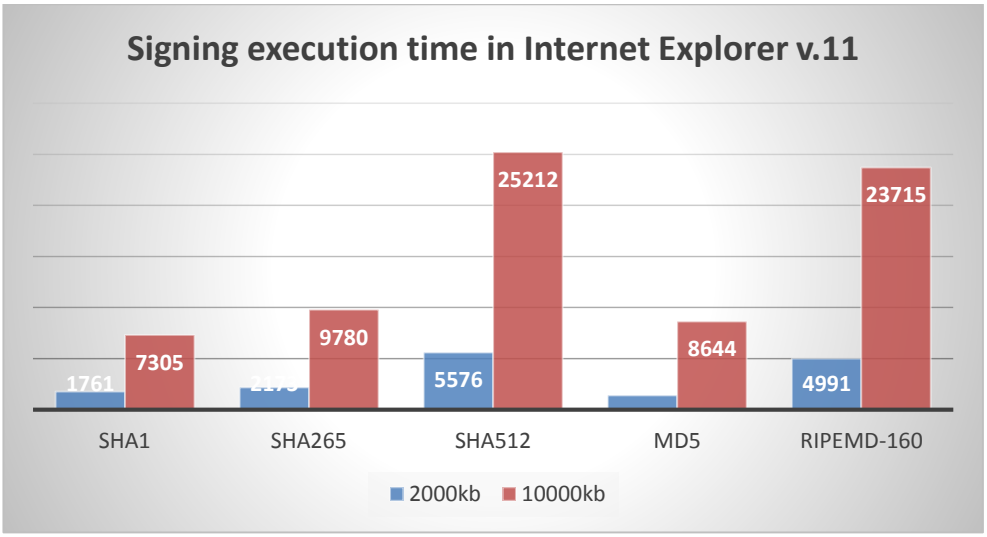

Figure 4. 3: Signing execution time in milliseconds Internet Explorer v.11

4.4.1.2. Firefox v. 43:

Table 4. 2 and Figure 4. 4 show results of execution time with the same factors running under FireFox v. 43, we can observe that SHA1 and MD5 has closest results, this might be the cause of SHA1 borrow some features of MD5.

Table 4. 2: the estimaetd execution time of signing process running under FireFox v.43

Message Size	SHA1	SHA265	SHA512	MD5	RIPEMD-160
2kb	98	103	93	20	32
29kb	130	153	234	42	69
2000kb	718	750	1517	620	906
10000kb	2553	2802	6804	2688	4102

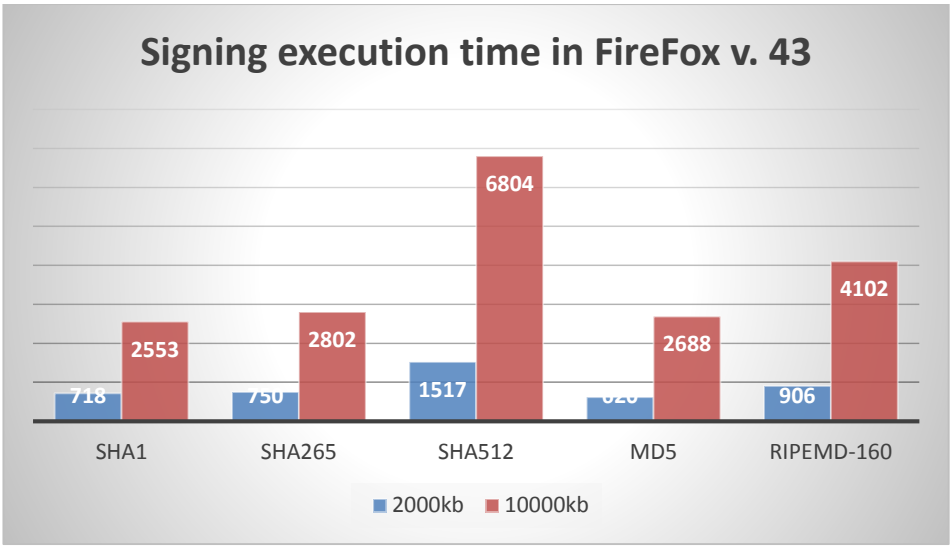

Figure 4. 4: Signing execution time in milliseconds - FireFox v.43

4.4.1.3. Google Chrome v. 47

Table 4. 3and Figure 4. 5 producing the same findings where MD5 is still the best performance on Google Chrome.

Table 4. 3: The estimated execution time of signing process running under Chrome v.47

Message Size	SHA1	SHA265	SHA512	MD5	RIPEMD-160
2kb	56	45	70	49	37
29kb	65	52	80	60	65
2000kb	1469	1587	2148	1233	1693
10000kb	6691	6834	12529	5963	7488

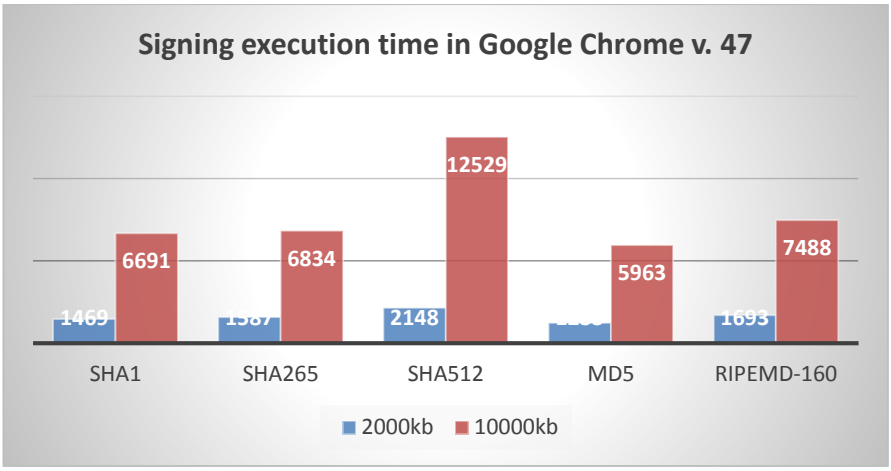

Figure 4. 5: Signing execution time in milliseconds – Google Chrome v.47

The implementation shows that MD5 digital signature algorithm is doing almost faster performance over different algorithms running under different browsers, however MD5 compromised because is has collision, while SHA1 still has only theoretical attack and no collision detected yet, however SHA1 hashes are not suitable for passwords – they are designed to be fast to compute, which makes them susceptible to brute-force attacks when used for passwords: bcrypt or scrypt are better alternatives.

With regards to the browser performance we can see from Figure 4. 6 that FireForx browser is doing the best performance on executing SHA256 hash function, which is consider as reasonable performance and secure function.

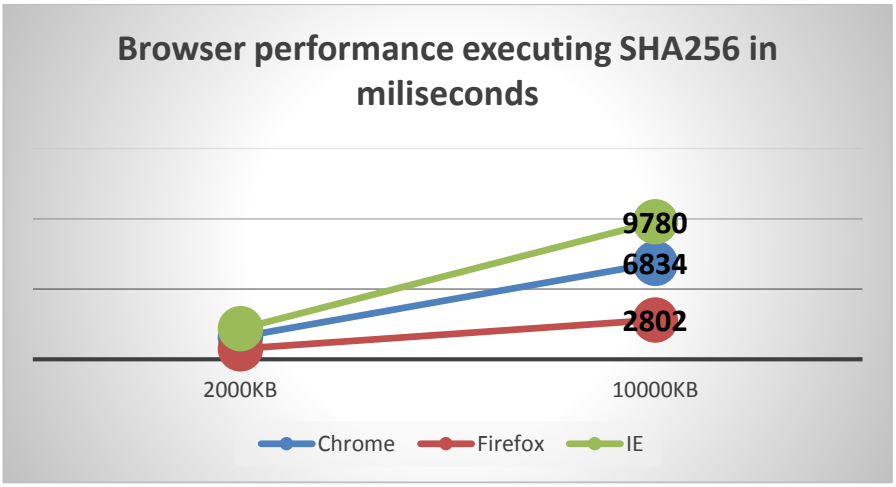

Figure 4. 6: Signing execution time in milliseconds of SHA256 on different browsers

4.4.2. Accuracy:

Designing secure systems always affect performance, scalability and usability.

Examining performance and measuring execution time over web browsers may affected with different factors, and these factors might be:

- Type of CPU scheduling algorithm that the Operating System use, hence we can see different execution time while operating system running other background processes.
- Type/versions of JavaScript engine and Interpreter on each browser.
- Loading functions into RAM, first load consumes time.

This means performance results may varies even with in the same environment and platform, however it produces valuable comparisons.

4.4.3. Security:

Robust and fast security functionality is basic tenant for secure computer transactions, and complexity is an enemy for security.

It would appear that SHA1 is more secure than MD5. Both are hashing algorithms based on older MD4 protocols. The main difference is that SHA1 and other hash functions return minimum 160 byte hash whereas MD5 returns a 32 byte hash. The

longer hash makes SHA1 less suspected to brute-force attacks as they would take a lot longer to complete(Piyush , Sandeep, 2014).

Security wise MD5 is not suitable for use for with any sort of sensitive information. Collisions exist with the algorithm, and there have been successful attacks against it. SHA1 doesn't have any attacks against it, but there have research that suggest it is vulnerable, and so SHA256 is preferred, although SHA256 has slower performance but it is the more secure.

4.5. Chapter summary

This Chapter presents the proposed model and specify in details the design of Digital fingerprint Signature Model, where Citizens being the digital identities should be able to access securely the various electronic facilities by communicating with the E-Governance. The chapter presents scenarios for the sender (citizen) and receiver(Government) are shown their higher authority that the citizen' fingerprint has not been altered during transmission. This chapter implement asymmetric encryption with Digital Signature to maintain data integrity with SHA1,SHA256, SHA512, MD5 and RIPEMD-160 hash functions.

Testing performance, accuracy and security id done in this chapter to conclude that SHA256 may consumes time to sign citizen's message, however it is the most secure hash function that could not break, therefore it is the most suitable to make digital signature for authentication purpose in e-government.

CHAPTER V

Model Simulation, Testing and Benchmarking

5.1. Introduction

Penetration testing or pen testing is a sequence of steps to identify and check security holes and exploit vulnerabilities, where vulnerability assessment is done to identify security vulnerabilities under specific situation and controlled circumstances, and the resulted findings is used to eliminate the security holes and covering the disclosed vulnerabilities before unauthorized attackers exploit them.(Aileen et al ,2011)

This research need to examine the digital fingerprint signature model proposed in chapter Four, the simulated web login using the proposed model will be tested using pen testing to identify if there are any weakness and security vulnerabilities. This also may be useful in benchmarking the model and disseminate it for real applicable use.

To conduct a pen test require to follow a pen test methodology, then choose the Penetration test strategies whether it was Black box, white box or gray box, and moreover identify the Penetration test types whether Network, application or social engineering.(Aileen et al ,2011)

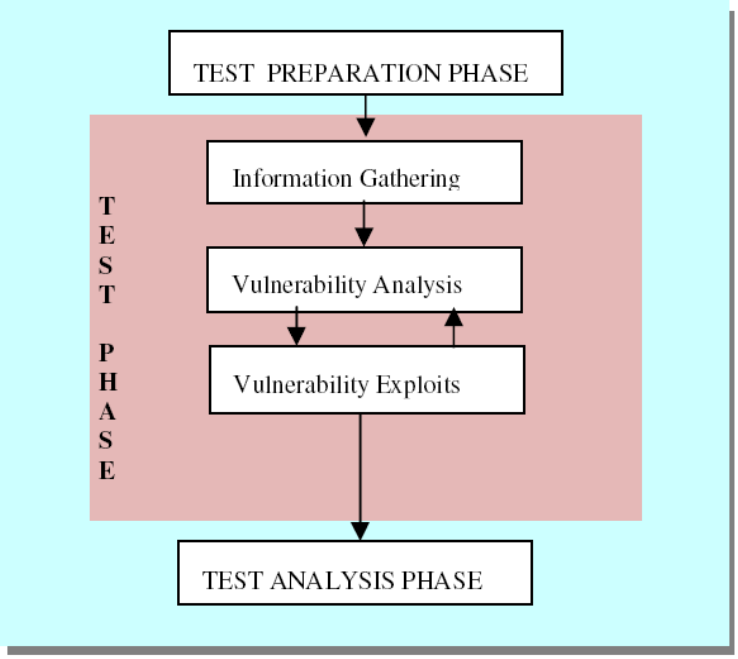

Figure 5. 1: Penetration Test Methodology (Aileen et al ,2011)

The penetration test methodology has three phases as shown in Figure 5.1

1. Test preparation phase: this phase is implemented on a simulation model which based on a web application environment.

2. Test phase: which start by collecting information, then analyze the known vulnerability resources that can be found on a web application environment, and finally exploiting the disclosed vulnerability.
3. Test analysis phase: analyze the results of the known vulnerability resources that found on simulated model.

5.1.1. Known vulnerabilities in web application systems:

1. Injection flows: such as SQL injection, OS injection, here attackers try to access and obtain restricted data from a back end database or send untrusted data to interpreter to execute unintended command.
   The most important type of defense from injection attacks is input validation.
2. Cross-site Scripting (XSS): XSS flows let the attacker to exploit weaknesses in web application verification of user inputs; this will occur when application takes untrusted data and send it to a web browser without proper validation or escaping. XSS has two classes Stored XSS and Reflected XSS
3. Brocken authentication and session management: the usefulness of session management is to provide an addition mechanism to authentication by making effect of authentication expire over the time, if the web application is not implemented correctly, this will allow attackers to compromise keys, passwords, session tokens or to exploit other implementation flaws to assume users identities.
4. Insecure direct object Reference: when an internal reference Objects such as file, directory or database key to be referenced without access control check, and as a result of this: attacker can manipulate these references to get access to unauthorized data.
5. Security misconfiguration: bad configuration can be found on any level of application stack: platform, database server, application server, web server or framework and custom code.
6. Sensitive Data Exposure: the most sensitive data such as authentication credentials, credit card and tax ID some times are not protected, here attackers may eavesdrop the communication in a non-protected web application, and as a result of this attackers could steal this valuable information to conduct a credit card fraud,

identity theft or other online crime. Encryption is one security measure to protect sensitive data from exposure.

7. Missing Function Level access Control: a web application should hide access to sensitive actions and verify function level access rights, function level protection sometimes not set properly wherever it is due to bad configuration or bad programming and improper code check.
8. Cross-site Reference Forgery: this attack forces a victim browser and without the user knowledge to send forged http request to a vulnerable web site, this attack leaves no evidence behind, and hence it thought as legitimate request.
9. Using component with known vulnerabilities: vulnerable components like libraries, framework and other software module always run with full privilege and can be identified and exploited with automated tools, this will enable possible range of attacks.
10. Invalidated Redirects and Forwards: web application can redirect to other pages, that can be invalidated links this may trick victims to click the link which is unsafe, and then attackers can phishing or provide malware sites, moreover use forward to access unauthorized webpage (Mirjalili et al, 2014).

5.1.2. Penetration Testing tools for web application:

- Acunetix Web Vulnerability Scanner 9.5: Acunetix indicated cross-site scripting vulnerabilities in the login page c where common web application vulnerabilities are: SQL injection, cross-site scripting, cross-site request forgery, broken authentication and session management (LaShanda et al, 2013).SQL injection permit illegitimate users to have login to website as a legitimate user(LaShanda et al, 2013), while Cross-site scripting also known as XSS is an attack to web application, attacker seeking vulnerabilities to bypass access control by injecting client-side scripts into webpage.(Aileen et al ,2011)
- WebScarab is another penetration testing tool for web application, this tool is written in java as a part the Open Web Application Security Project (OWASP), it is also used for SQL injection, cross-site scripting testing (LaShanda et al, 2013).

- Other testing tools for web application security assessment are found such as: Paros, JBroFuzz and Fortify (LaShanda et al, 2013).

5.2. Model Simulation

The proposed model of secure login to access confidential information in e-government has to be analyzed to identify vulnerabilities and recover them.

The model is used as a login system, which provide two levels of verification, the first one is to verify identity using biometric fingerprint and the other level to verify the digital signature of user fingerprint.

Figure 5.2 shows the simulated webpage interface where the citizens request for level 2 login, which contain sensitive data.

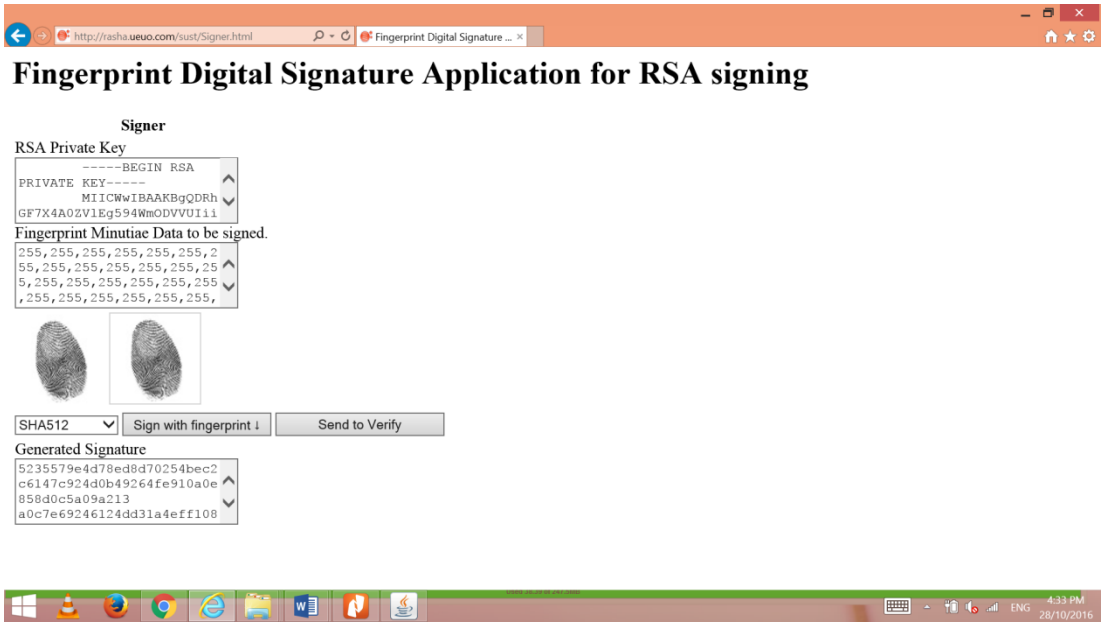

Figure 5.2 signer interface for request login

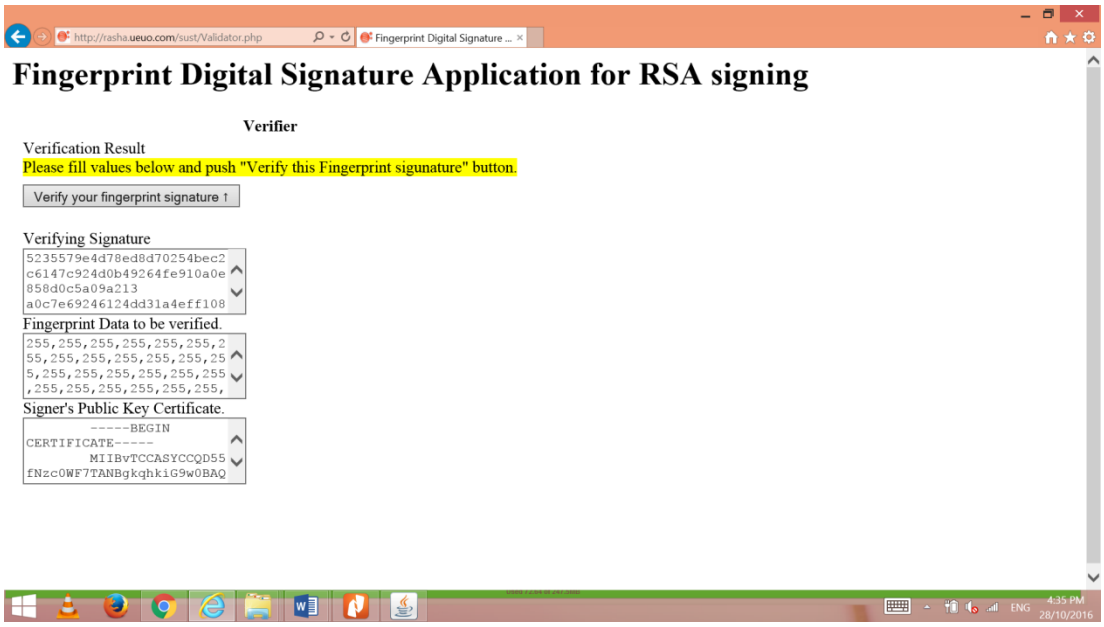

Figure 5.3 Verifier interface for request login

The governmental server will check the two level of verification to identify the sender, Figure 5.3shows the interface of the verification process.

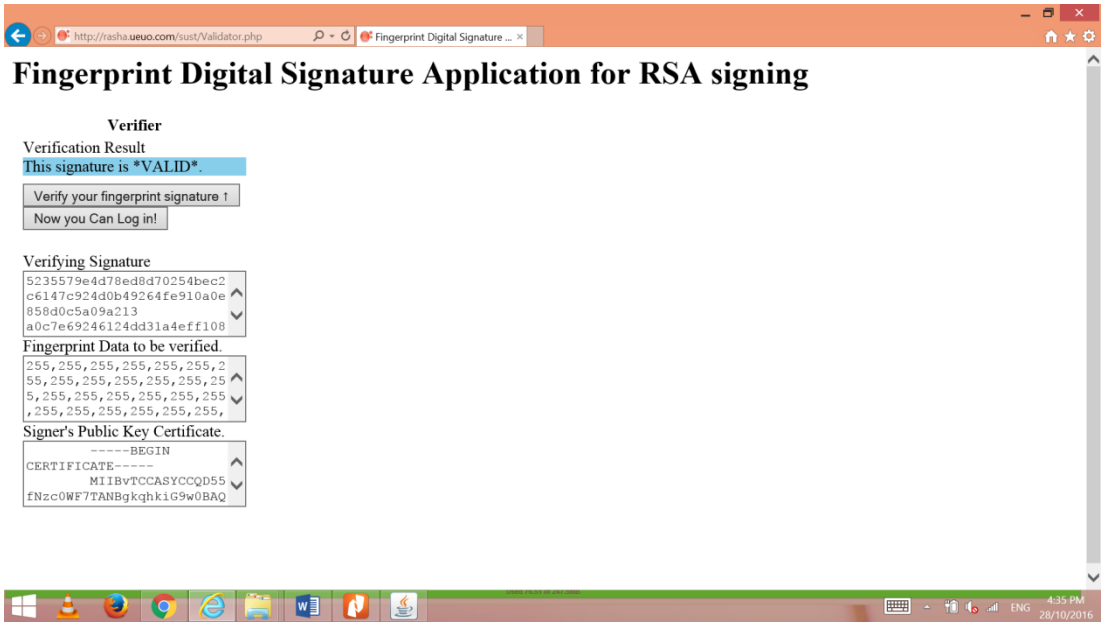

Figure 5.4 Valid verification

Figure 5.4 show the interface of a valid verification, where the governmental server checks the validity of minutiae signature, on this case only will appear “you can login” button, where authorized person only can login. Figure 5.5shows the interface of invalid verification.

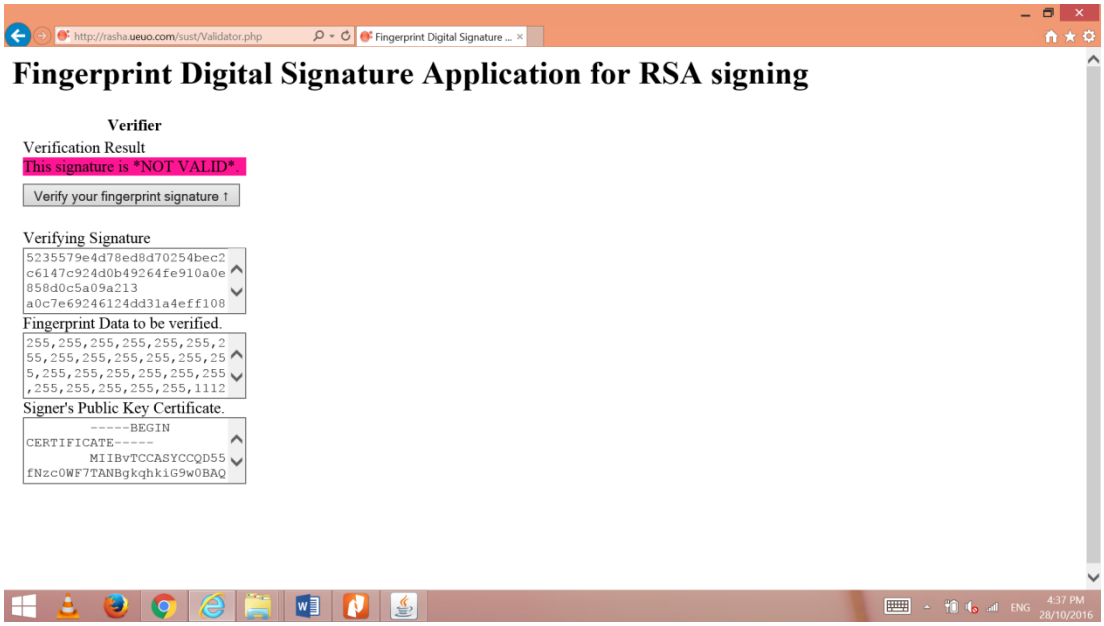

Figure 5.5 invalid verification

5.3. Testing

Digital Fingerprint Signature Model as implemented in chapter 4, is being testing on this chapter to find out if the model securely applicable and it's not easy to break session which is identify by the Digital fingerprint signature.

After viewing the known vulnerabilities on web applications, this chapter will concentrate on three measures related to secure accessibility of e-government, and because of the nature of the research to provide secure access to e-governmental information. These measures are to test existence of *SQL injection*, *Cross-site Scripting (XSS)* and *Brocken authentication and session management* attacks on the simulated model.

5.3.1. Testing SQL injection and Results:

Structured Query Language Injection Attacks (SQLIA) is top 10 vulnerability list and has resulted in massive attacks on a number of websites and in the past few years is ranked 1st in the Open Web Application Security Project (OWASP).

This attack is concern about inputting unwanted command string, where the web application is not provide means to verify inputs, this is considered a weakness in a web application form, thereby the attacker exploit this vulnerability to post special SQL statement which are executed in the database server and gain access to data, as a result of this loss in confidentiality, integrity and authentication (Rahul, Pankaj, 2012)

In most number of scenarios, unauthorized activity is performed by the attacker through valid user credentials or by using inherent features of database application such as malicious modification of existing SQL Queries of web application that are accessing critical sections of the affected databases.

In our simulation model, SQL injection are not applicable where the user credentials are biometric fingerprints manipulated with digital signature, thereby we can insure the input validation and authentication.

The simulation model uses HTML5 canvas technique instead of form to input the fingerprint for signing process and as shown in figure 5.2, here we can see obviously there is no way for attacker to enter SQL statement string to perform SQL injection attack.

5.3.2. Testing Cross-site Script attacks and Results:

The cross-site script attack (XSS attack) is a type of injection, here the attackers inject a web application code written in a different scripting languages, such as java script, flash or ActiveX code, these codes executed in the users browser and have the ability to read, change and transmit any critical data accessible by the browser (Rahul, Pankaj, 2012).

The attacker use XSS attack to hijack user data through cookies, or redirect users to another website or even hijack user session of visited web page. There are two types of XSS attacks one is called “persistent” and “non-persistent”. The difference between the two types lie in the way the server side and client side vulnerabilities are exploited. The first type is *stored or persistent attack*: in this type malicious code is stored permanently, the other type is *reflected or non-persistent attack* this attack occur when an attacker injects browser executable code within a single HTTP response and when the server does not properly sanitize the output server to a visiting web browser/client.

Our simulation model is based on a server side scripting language c#, and the fingerprint data are not stored on cookies on the client side, There are two methods to POST and GET, to send and retrieve data, dong the same function but they are different on the way they are treat data, hence using $_GET is an array of variables passed to the current script via the URL parameters which is visible to any one, while $_POST is an array of variables passed to the current script via the HTTP POST method, which is invisible, our simulation model is not use a GET method to send the user credentials, however the only act can attacker do is to bypass filters is the HTTP Parameter Pollution, this evasion technique consists of splitting an attack vector between multiple parameters that have the same name. The manipulation of the value of each parameter depends on how each web technology is parsing these parameters, so this type of evasion is not always possible. If the tested environment concatenates the values of all parameters with the same name, then an attacker could use this technique in order to bypass pattern- based security mechanisms. In that case our simulation model can abort any attempt to compromise user fingerprint by sending a pop up dialog box to indicate that an attacker could execute arbitrary JavaScript of his choice in the user' browsers.

5.3.3. Testing Broken session management and Results:

The research use a penetration test tool “webScarab” for testing the simulated model, Figure 5.6 shows how the simulated model running on internet explorer are analyzed using the session ID, hence the session ID is created from fingerprint digital signature stored as cookies, and send it over Internet, here WebScarab can acting as proxy to figure out the communication and try to fetch all 100 sample trying to predict and guess the session ID as a brute force attack.

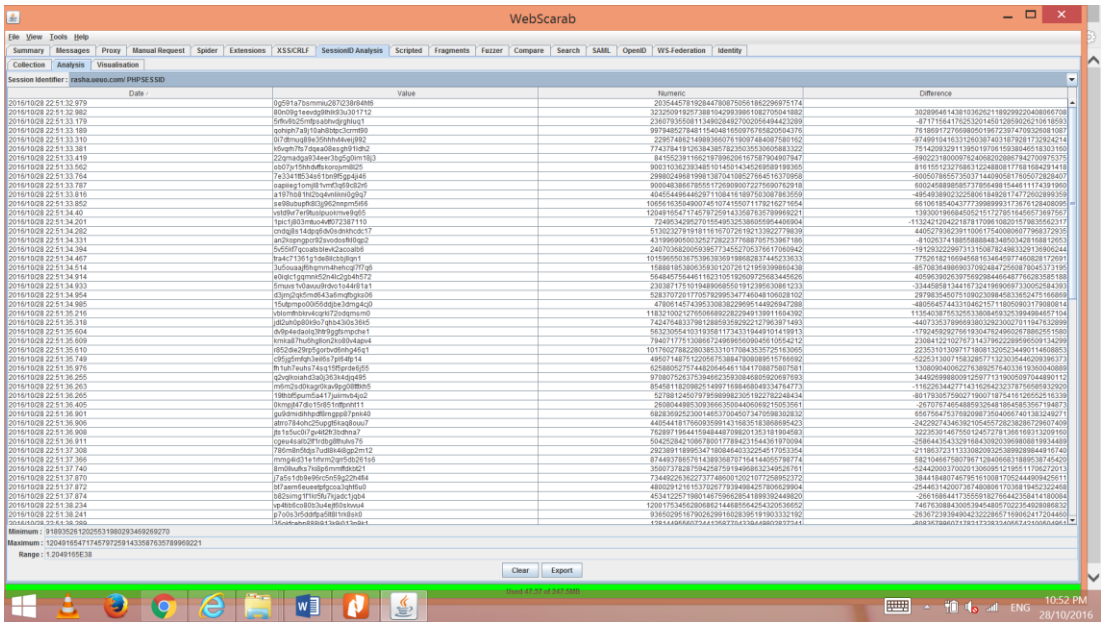

Figure 5.6 analyzing session ID using Web scarab tool

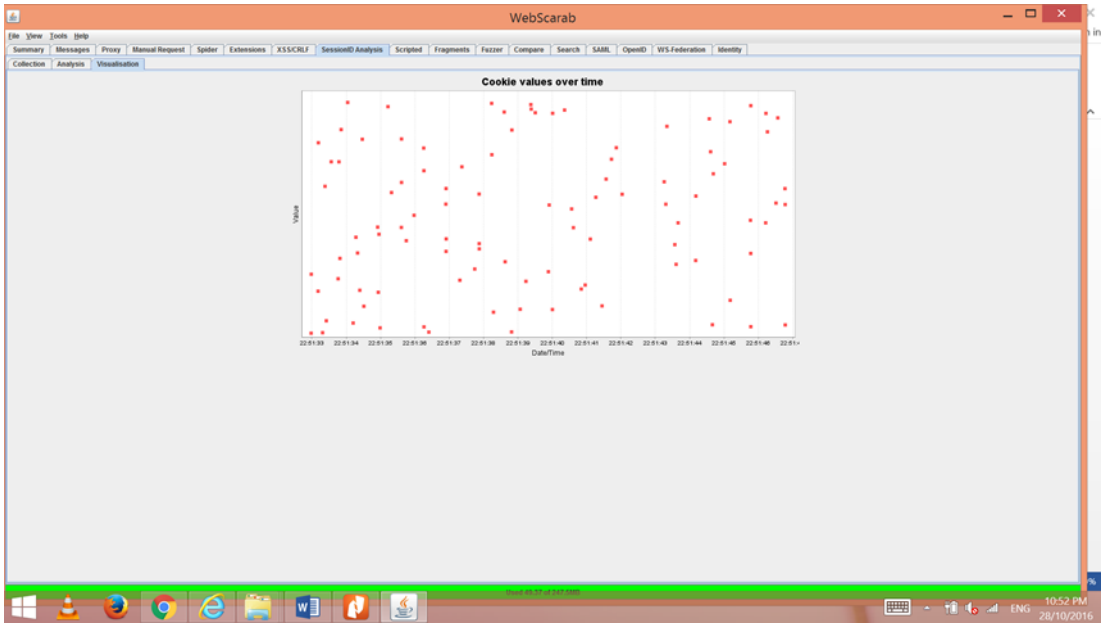

Figure 5.7 cookies values of session ID

Figure 5.7 shows that is not easy to predict the session ID and before it is expired.

5.4. Chapter summary

This chapter discussed the various vulnerabilities in web application and present the attacks that compromise the Digital Fingerprint Signature model, moreover stating the most used penetrating testing tools.

The testing phase was concentrating in the major three attacks that compromises the accessibility of a web application such as SQL injection, XSS and session management attacks. The findings presents the inapplicability of SQL injection and XSS attacks, moreover the results of model testing using WebScarab tool that shows the possibility of predicting the session ID which insure a robust and secure session which cannot be break.

CHAPTER VI

Conclusion, Contribution & Recommendations

6.1. Conclusion:

6.1.1. The research discuss the importance of security in e-government, Security has an important role in trust formation of citizens and their adoption of e-government. Designing and implementing more effective approaches for securing E-government is an important issue, because, the governmental information is usually so sensitive.

6.1.2. In this work, an authentication framework and the requirements for the e-government security is proposed. The authentication process in the e-Government is certainly more than a technical issue, this is can be obvious from the result of questionnaire I, where people may depend on others to access their accounts, this is solved using Digital Fingerprint Signature Model.

6.1.3. Designing and implementing more effective framework for securing E-government is an important issue, because the governmental information is usually so sensitive. In this research we find it reasonable to argue that the use of a combination of existing models to secure e-government services will play an important role in trust formation of citizens and their adoption of e-government; however security provision of e-Government is certainly more than a technical issue. The proposed framework may be to the benefit of new emerge electronic governments and country readiness in security issues, especially in development country, to provide a reliable communication between citizens and government. The benefit may extent to e-commerce applications and it might be addition to web-based information system security framework.

6.2. Contribution:

A novel Framework of authentication for e-government security will be developed throughout the proposed solution, which expected for the benefit of new emerge electronic governments and country readiness in security issues, especially in development country, to provide a reliable communication between citizens and government. The benefit may extent

to e-commerce applications and it might be addition to web-based information system security framework.

The goal of this work is to propose a novel Framework of authentication for e-government security. The framework enhanced the verification method by applying two verification level without affecting on response time.

The research shows that the authentication process in the e-Government is certainly more than a technical issue. Moreover secure access has an important role in trust formation of citizens and their adoption of e-government.

The proposed solution is applicable in most e-government services, in contrast with its benefits.

The proposed solution overcome the drawbacks of biometric fingerprint, where the tampered fingerprint will lose its validity once its fingerprint digest is invalid, and this give new opportunity to preserve user identity.

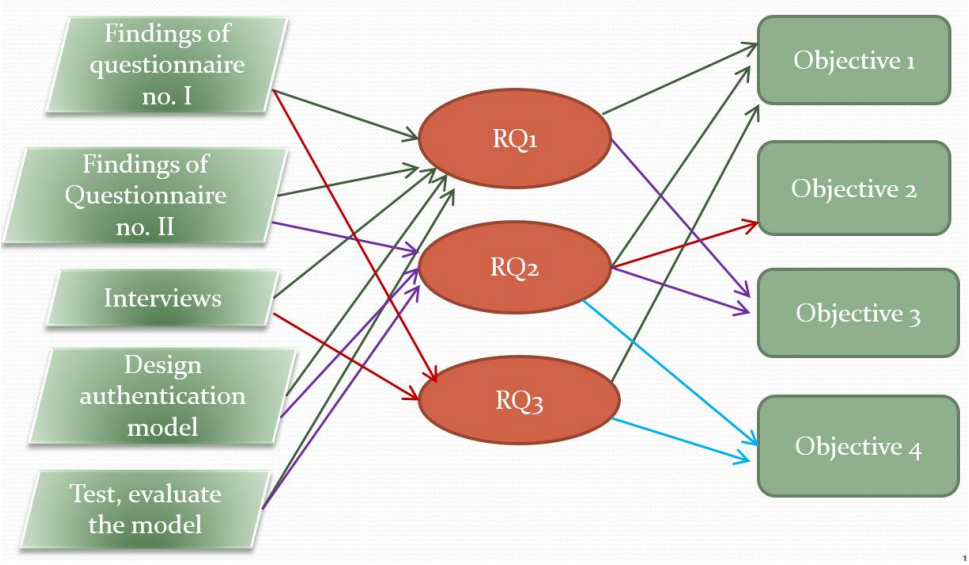

Figure 6. 1: Achieve Research Objectives

Figure 6. 1 describe how objectives are achieved through out the research study, these are done through the main research tasks:

- the case study (Questionnaire I, questionnaire II and Interviews),
- Design and implementation of authentication model and

- Testing and evaluating the model

The Research Questions (RQ) are answered after accomplish the above tasks, finally the objectives are achieved.

6.3. Future Recommendations

It’s desirable to use biometric fingerprint for identification, however in practice it is sometimes inapplicable for people with disparities, finger cut, and sometimes it is not robust to change scale, in all Biometric Data have some limitations but fingerprint till right now is the best.

The case study is applied in Sudan where Sudan e-government considered new emerged technology, this may suppress the use of e-government, for future benefits apply this case study to the most developing countries that uses the full capabilities of e-government.

References:

Abhishek Roy, Sunil Karforma, (2014), Stream Cipher Based User Authentication Technique In E-Governance Transactions, Journal of Research in Electrical and Electronics Engineering, Volume 3, Issue 3, May 2014, pp:31-37

Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones, (2011), AN OVERVIEW OF PENETRATION TESTING, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

Alexander NTOKO, (2003) Building Trust and Confidence for Critical E-government Services, ITU Telecommunication Development Bureau (BDT).

Aly, S., "Multimedia Security: Survey and Analysis Multimedia and Networking Research Lab.", CTI, DePaul University, Chicago(2003)

Amina Gamlo and Omaima Bamasak, "Towards Securing E-Transactions in E-Government Systems of Saudi Arabia", the Institute of Electrical and Electronics Engineers, 2009

Anil K. Jain, Lin Hong, SharathPankanti,andRuudBolle, (1997), An Identity-Authentication System Using Fingerprints, proceedings oftheIEEE, VOL. 85, NO. 9, September 1997

Bernd Zwattendorfer, Klaus Stranacher, Arne Tauber, Peter Reichstädter, "Cloud Computing in E-Government across Europe", Technology-Enabled Innovation for Democracy, Government and Governance, Lecture Notes in Computer Science Volume 8061, 2013, pp. 181-195

Bushra Mohamed ElaminElnaim, Salman Bin Abdulaziz, "an overview of e-government strategy in Sudan", European Journal of Computer Science and Information Technology, Vol.2, No.2, pp.1-9, September 2014

Charalampos Tsaravas, Marinos Themistocleous, “cloud computing and egovernment a literature review”, European, Mediterranean & Middle Eastern Conference on Information Systems 2011.

Creswell, J. W. (2007). Designing and conducting mixed methods research. Thousand Oaks, CA:Sage Publications.

Danish Dada, “the failure in e-government in developing countries a literature review”, EJISDC (2006) 26, 7, 1-10

DimitriosZissis, DimitriosLekkas, “Securing e-Government and e-Voting with an open cloud computing architecture”, Government Information Quarterly 28 (2011) 239–251.

Dominique Cansell, J Paul Gibson, Dominique Mery, “Refinement: A Constructive Approach to Formal Software Design for a secure e-voting Interface”, Electronic Notes in Theoretical Computer Science 183 (2007) 39–55

Geoffrey Karokola, Stewart Kowalski and Louise Yngström , “Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View”, (2011)

Geoffrey Karokola, Stewart Kowalski and Louise Yngström, “Secure e-Government Services: Towards A Framework for Integrating IT Security Services into e-Government Maturity Models“,

Geoffrey RwezauraKarokola, “A Framework for Securing e-Government Services”, PhD Thesis, Stockholm University,Sweden, (2012)

Gil-Garcia, J. Ramon, IndushobhaChengalur-Smith and Peter Duchessi. (2007). Collaborative E-Government: Impediments and Benefits of Information Sharing Projects in the Public Sector. European Journal of Information Systems, 16(2): 121-133.

Henriksson, A. Yi, Y. Frost, B. and Middleton, M. (2006) Evaluation instrument for e-government websites, Proceedings Internet Research 7.0: Internet Convergences, Brisbane, Queensland, Australia.

Ibrahim Kushchu, "From E-government to M-government: Facing the Inevitable", Mobile Government Lab (mGovLab), (2004),International University of Japan Yamato-machi, Minami Uonuma-gun, Niigata 949-7277 JAPAN .

Irfan Syamsuddin, Junseok Hwang, " A New Fuzzy MCDM Framework to Evaluate E-Government Security Strategy", 978-1-4244-6904-8/10/$26.00 ©2010 IEEE

J. Jang-Jaccard, S.Nepal, "A survey of emerging threats in cyber security", Journal of Computer and System Sciences 80 (2014) 973–993

Jensen J. Zhao, Sherry Y. Zhao, (2010) Opportunities and threats: A security assessment of state e-government websites, Government Information Quarterly 27 (2010) 49–56

K P Tripathi, (2011), A Comparative Study of Biometric Technologies with Reference to Human Interface, International Journal of Computer Applications (0975 – 8887)Volume 14– No.5, January 2011

LaShanda Dukes, Xiaohong Yuan, Francis Akowuah, (2013), A Case Study on Web Application Security Testing with Tools and Manual Testing, 978-1-4799-0053-4/13/$31.00 ©2013 IEEE

Luca Calderoni, Dario Maio, "Cloning and tampering threats in e-Passports", Expert Systems with Applications 41 (2014) 5066–5070.

M. Al-Khouri1, "Technological and Mobility Trends in E-Government", Business and Management Research, Vol. 2, No. 3; (2013)

Malik F. Saleh, "Information Security Maturity Model ", International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011

Maria Wimmer, Bianca von Bredow, “A Holistic Approach for Providing Security Solutions in e-Government”, Proceedings of the 35th Hawaii International Conference on System Sciences - 2002

Mirjalili, Alireza Nowroozi, Mitra Alidoosti, (2014) , A survey on web penetration test, ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 6, No.12 , November 2014

Mohammad Hazza Zu’bi, Hamdan Hasan AL-Onizat, “E-government and security requirements for information systems and privacy (performance linkage)”, Journal of management research, (2012), Vol 4, No.4.

Mohammed Alshehri, Steve Drew, Osama Alfarraj,” A Comprehensive Analysis of E-government services adoption in Saudi Arabia (Obstacles and Challenges)”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.2, 2012

Muhammad Bilal Kayani ,”Analyzing Barriers in e-Government Implementation in Pakistan”, International Journal for Infonomics (IJI), Volume 4, Issue 3/4, September/December 2011

N. Alharbi, “E-government security modeling: explain main factors and analyzing existing models“, International Journal of Social, Human Science and Engineering Vol:7 No:9, 2013

Ndou, V., M., (2004), E-government for developing countries: opportunities and challenges, The Electronic Journal on Information Systems in Developing Countries, 18(1), pp. 1-24. Pearson Education limited/ Prentice Hall. ISBN: 0273-65804-2.

Piyush Gupta, Sandeep Kumar ,(2014), A Comparative Analysis of SHA and MD5 Algorithm (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4492-4495

Piyush Morwal, Parvinder Singh, RajkumarTripathi, “Security in e-Governance using Biometric”, International Journal of Computer Applications (0975 – 8887) Volume 50 – No.3, July 2012

Quanxi Li, Elhadi Osman Abdalla ,“The E-Government in Sudan Challenges, Barriers and prospective”, International Conference on Global Economy, Commerce and Service Science (GECSS 2014)

RabahAlshboul, “Security and Vulnerability in the E-Government Society”, Contemporary Engineering Sciences, Vol. 5, 2012, no. 5, 215 – 226

Rahul Johari, Pankaj Sharma (2012) A Survey On Web Application Vulnerabilities (SQLIA,XSS) Exploitation and Security Engine for SQL Injection, International Conference on Communication Systems and Network Technologies, 2012

Rahul Sharma, Nidhi Mishra, Sanjeev Kumar Yadav, (2013), Fingerprint Recognition System and Tehniques: ASurvey, International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013

Rodger Jamieson, Ph.D., CA, Greg Stephens and Santhosh Kumar, (2004), Fingerprint Identification: An Aidto the Authentication Process, Information Systems Audit and Control Association,www.isaca.org.

RoliBansal, PritiSehgal, and PunamBedi, (2011), Minutiae Extraction from Fingerprint Images - a Review, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3

Sabri Al-Azazi, “A multi-layer model for e-government information security assessment”, Cranfield University, (2008), PhD thesis.

Sara Abdalla, “an e-government adoption framework for developing countries a case study from sudan”, CranfieldCniversity, PhD thesis 2012

Saunders, M., Lewis, P., &Thornhill, A. (2003). Research Methods for Business Student. 3rd edition;

Shadi Al-khamayseh, Elaine Lawrence and AgnieszkaZmijewska ,“Towards Understanding Success Factors in Interactive Mobile Government”, University of Technology, Sydney PO Box 123, Broadway NSW (2007), Australia

Shailendra Singh, “E-Governance Information Security Issues”, International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec. 2011

Sharifi, H. and Zarei, B., (2004), An adaptive approach for implementing E-government in I.R. Iran, Journal of Government Information, 30(5-6), pp. 600-619.

Smitha K K , Chitharanjan K , “Security of Data in Cloud based E-Governance System”, International Journal of Computer Applications,(2012), (0975 – 8887)

Sofia Elena Colesca , “Understanding Trust in e-Government”, ISSN 1392 – 2785 InzinerineEkonomika-Engineering Economics(3). 2009

Thamer Alhussain, Steve Drew, “Towards Secure M-Government Applications”, Griffith University Gold Coast, Australi

United Nations,” E-government survey 2012, E-government for the people, economic and social affairs department “, ST/ESA/PAS/SER.E/150

Valentina (Dardha) Ndou, “e-government for developing countries opportunities and challenges”, EJISDC (2004) 18, 1, 1-24

Yesser, Survey of e-government relevant standards in use in Saudi-Arabian public sector, e-government interoperability framework survey, E-Government Program, The Ministry of Communications and Information Technology 24-6-1426 h

ZHOU Feng, "The research and implementation of a unified identity authentication in e-government network", physics procedia 24(2012) 2032 – 2038

د. صفاء يونس الصفاوي، عزة حازم زكي، زياد صفاء يونس، (2012)، نمذجة نظام برمجي لحكومة الكترونية مع التطبيق على بصمة الاصبع ، المؤتمر العلمي السنوي الحادي عشر – ذكاء الاعمال واقتصاد المعرفة - الاردن

موقف تنفيذ حكومة السودان الرقمية، المركز القومي للمعلومات ، مجلة السودان الرقمية ، يناير 2015

Appendices
Appendix A: Questionnaire I

جامعة السودان للعلوم والتكنولوجيا
كلية الدراسات العليا – كلية علوم الحاسوب وتقانة المعلومات
برنامج الدكتوراه بالمقررات والبحث - الدفعة الثالثة

استبيان حول استخدام الخدمات الالكترونية في الحكومة الالكترونية في السودان

استبانة المواطن (مستخدم نظم الحكومة الالكترونية)

المواطن الكريم/ المواطنة الكريمة،،

السلام عليكم ورحمة الله تعالى وبركاته،،

بدءاً أشكر لكم تعاونكم وكريم تفضلكم بمشاركتي وقتكم وخبرتكم لتحقق الدراسة اهدافها المرجوة، وجزاكم الله خيراً.

أود ان أعلِم سيادتكم بأن هذه الاستبانة جزء من دراسة تهدف الى تأمين الوصول الى خدمات الحكومة الالكترونية السودانية كجزء من متطلبات البحث للحصول على درجة الدكتوراة.

كما أود أن أشير الى ان المعلومات في هذه الاستبانة لن تستخدم إلا لأغراض البحث ونسأل الله التوفيق.

فضلاً، تكرم بتقديم إجاباتك حول الاسئلة التالية بوضع علامة (✓) أمام الخيار الأنسب.

1. معلومات عامة:

1.1. الاسم (رباعياً):

1.2. النوع:

ذكر	
انثى	

1.3. العمر:

(16-20)	
(21-30)	
(31-40)	
(41-50)	
(51-60)	
اكبر من 60	

1.4. هل لديك رقم وطني؟

نعم	
لا	
سأقوم بالحصول عليه	

1.5. قييم خبرتك في استخدام الحاسوب:

ضعيفة	
متوسطة	
جيدة	
جيدة جداً	

1.6. قييم خبرتك في استخدام الانترنت:

ضعيفة	
متوسطة	
جيدة	
جيدة جداً	

1.7. هل يمكنك استخدام تطبيقات الحاسوب بسهولة؟

نعم دائما أستطيع	
أحيانا أستطيع	
لا أستطيع	
غير متأكد	

2. تجربتك الامنية اثناء استخدامك الحكومة الالكترونية

2.1. هل تعتقد انه من الضروري ان تعلم بنواحي الامن الالكتروني في استخدام خدمات الحكومة الالكترونية؟

غير مهم	
مهم تقريباً	
مهم جداً	

2.2. هل تقوم بتغيير كلمة السر من حين الى آخر؟

نعم باستمرار	
تقريبامن وقت لآخر	
لا نهائياً	

2.3. هل حدث ان قمت بإعطاء كلمة السر لأحد تثق به؟

نعم لأنني دائما أنسى	
نعم في بعض الاحيان	
لا على الإطلاق	

2.4. هل حدث وأن قمت بكتابة كلمة السر في مكان ما؟

نعم لأنني دائما أنسى	
نعم في بعض الاحيان	
لا على الإطلاق	

2.5. هل تتوفر خدمة الحكومة الالكترونية التي تستخدمها دوماً؟

نعم تتوفر دائما	
في بعض الأحيان غير متوفرة	
نادرا ما تتوفر	

2.6. هل لديك مانع من استخدام البصمة الالكترونية باعتبارها عملية تحديد الهوية؟

نعم أنا أعارض	
لا أنا لا أمانع	
لا أهتم	

2.7. هل تفضل استخدام البصمة الاكترونية في جميع خدمات الحكومة الالكترونية؟

أفضل بقوة	
أفضل إلى حد ما	
إلى حد ماأعارض	
أعارض بشدة	
غير متأكد	

2.8. هل تعتقد أن الإنترنت يحتوي على ضمانات امنية كافية بحيث توفر لك الراحة اثناء استخدامك لخدمات الإلكترونية؟

نعم تتوفر دائما	
في بعض الأحيان غير متوفرة	
نادرا ما تتوفر	
غير متأكد	

2.9. هل تشعر بالثقة عند تقديم جميع المعلومات المطلوبة منك إلى خدمات الحكومة الإلكترونية؟

نعم تتوفرالثقة دائما	
في بعض الأحيان االثقةغير متوفرة	
نادرا ما تتوفر الثقة	
غير متأكد	

2.10. قييم مدى الموثوقية عند استخدامك لخدمات الحكومة الالكترونية؟

غير موثوقة	
معتدلة الموثوقية	
عالية الموثوقية	

2.11. هل تعمل خدمات الحكومة الإلكترونية وفقا لما كنت تتوقع؟

نعم أنها تعمل كما هو متوقع	
أحيانا لا تعمل كما هو متوقع	
انها لا تعمل كما هو متوقع	
غير متأكد	

2.12. قييم مدى موثوقية عملية اصدار الرقم الوطني بالنسبة لك؟

غير موثوقة	
معتدلة الموثوقية	
عالية الموثوقية	

2.13. عند استخدامك لخدمات الحكومة الالكترونية هل يمكنك الوصول إلى جميع المعلومات التي تحتاجها؟

نعم دائما أستطيع	
أحيانا أستطيع	
لا أستطيع	
غير متأكد	

2.14. هل تعلم شيئاً عن القوانين التي تحكم استخدام الانترنت و الحكومة الالكترونية؟

نعم أعرف كل منهم	
أعرف بعض منهم	
لا أعرف أي منهم	

2.15. هل تتأثر بحالة عدم استقرار الحالة الاقتصادية عند استخدامك للحكومة الالكترونية؟

نعم أتأثر	
أحياناً أتأثر غير متأكد	
لا أتأثر	
غير متأكد	

2.16. هل تتلقى ما يكفي من المعلومات حول ماذا/كيف/متى تصل إلى خدمات الحكومة الإلكترونية؟

نعم تتوفر دائما	
في بعض الأحيان غير متوفرة	
نادرا ما تتوفر	
غير متأكد	

2.17. هل لديك التسهيلات التقنية (*انترنت-كمبيوتر وغيرها*) وغير التقنية للوصول لخدمات الحكومة الالكترونية؟

نعم تتوفر دائما	
في بعض الأحيان غير متوفرة	
نادرا ما تتوفر	
غير متأكد	

2.18. هل تعتمد على الآخرين عند استخدامك للحكومة الالكترونية؟

نعم أنا دائما أعتمد على أحدهم	
أحياناً أعتمد على أحدهم	
لا اعتمد على احد	

2.19. برأيك ما هي اسباب عدم استخدام المواطنين لخدمات الحكومة الإلكترونية؟

صعوبة الاستخدام	
اسباب امنية	
أخرى	

3. وعي وادراك مستخدمي الحكومة الالكترونية:

3.1. هل تألف استخدام الحكومة الالكترونية؟

مألوفة جداً	
مألوفة إلى حد ما	
مألوفة قليلاً	
غير مألوفة على الاطلاق	
غير متأكد	

3.2. وبشكل عام، ماذا تقول حول تأثير الحكومة الإلكترونية على المواطن؟

ايجابي جداً	
ايجابي الى حد ما	
محايد	
سلبي الى حد ما	
سلبي جداً	
غير متأكد	

3.3. واستشرافاً للمستقبل من ثلاث إلى خمس سنوات ماذا تعتقد ان يكون تأثير الحكومة الإلكترونية على المواطن؟

ايجابي جداً	
ايجابي الى حد ما	
محايد	
سلبي الى حد ما	
سلبي جداً	
غير متأكد	

3.4. من وجهة نظرك، حدد مدى أولوية أن يكون استثمار الحكومة لأموال الضرائب في إتاحة المعلومات والخدمات المتاحة عبر مواقع الحكومة الالكترونية؟

اولوية عالية جداً	
اولوية عالية	
متوسط الاولوية	
اقل اولوية	
متدني الاولوية	
غير متأكد	

3.5. هل تؤيد أوتعارض الحكومة الإلكترونية كوسيلة أساسية للحصول على المعلومات والخدمات من الحكومة؟

أؤيد بشدة	
أؤيد الى حد ما	
اعارض الى حد ما	
اعارض بشدة	
غير متأكد	

3.6. القائمة التالية تذكر الأشياء الإيجابية المحتملة التي قد تنجم عن استخدام الحكومة الإلكترونية، قم بترتيب أهمية البنود المدرجة على مقياس من 1 إلى4، 1مع كونها الأهم و4 الأقل أهمية. ملاحظة:يراعى عدم تكرار القيمة المعنية في البنود.

وصول اكبر للجمهور	
الخدمات الحكومية أكثر ملاءمة	
الحكومة أكثر خضوعا للمساءلة أمام مواطنيها	
حكومة اكثر كفاءة وفعالية من حيث التكلفة	

3.7. رتب من حيث الأهمية، بحيث 1 معناها الأهم و4أقل، ترتيبا لأولويات الواردة أدناه لمواقع الحكومة الالكترونية .ملاحظة :يراعى عدم تكرار القيمة المعنية في البنود.

جعلها أسهل للاستخدام والفهم.	
جعلها أكثر أمنا لممارسة الأعمال التجارية	
سهولة العثور على الموقع المرغوب على شبكة الإنترنت	
توسيع المواقع على شبكة الإنترنت لتشمل المزيد من المعلومات والخدمات	

3.8. ضع علامة (✓)امام الرقم المناسب، الارقام تعبر عن الآتي:

1= لا اوافق بشدة 2=لا اوافق 3=محايد 4=اوافق 5=اوافق بشدة

	لتطوير الحكومة الإلكترونية في السودان يجب أن:	**1**	**2**	**3**	**4**	**5**
3.8.1	تكون خدمات الحكومة الإلكترونية عبر الإنترنت فعالة في توفير المعلومات للمواطن					
3.8.2	يمكن للمواطن التواصل مع مزود خدمة الحكومة الإلكترونية على الانترنت لتلقي المعلومات المطلوبة					
3.8.3	تتوفر خدمات الانترنت بسهولة في منطقتك.					
3.8.4	تكون سرعة الإنترنت ونوعية الخدمة جيدة بما فيه الكفاية للوصول إلى خدمات الحكومة الإلكترونية					
3.8.5	تسهيل حصول المواطن على شبكة الإنترنت وأجهزة الكمبيوتر					

4. الحواجز والتحديات التي تواجه تبني خدمات الحكومة الالكترونية

	في رأيك العقبات التي تحول دون تنفيذ خدمات اوسع عبر الحكومة الالكترونية:	**1**	**2**	**3**	**4**	**5**
4.1	عدم الفهم الكافي لمزايا للتعاملات الالكترونية					
4.2	نقص المعرفة والقدرة على استخدام أجهزة الكمبيوتروالتكنولوجيا بكفاءة					
4.3	نقص في معرفة خدمات الحكومة الإلكترونية					
4.4	عدم وجود أمن وخصوصية المعلومات في المواقع الحكومية					
4.5	انعدام ثقة المواطن في استخدام خدمات الحكومة الإلكترونية					
4.6	عدم وجود سياسة ولوائح تنظيمية لاستخدام الحكومة الإلكترونية في السودان					
4.7	توافرالاتصال وموثوقية الاتصال بالإنترنت					
4.8	صعوبة الحصول على خدمة الإنترنت					

5. الثقافات والخصوصية

		1	2	3	4	5
5.1	أشعر أن استخدام خدمات الحكومة الإلكترونية غير آمن					
5.2	أشعرأن المخاطرتفوق الفوائد المترتبة على استخدام خدمات الحكومة الإلكترونية					
5.3	أشعر أنني يجب أن أكون حذراعند استخدام خدمات الحكومة الإلكترونية					
5.4	أعتقد أنه قد تكون هناك عواقب سلبية من استخدام خدمات الحكومة الإلكترونية.					
5.5	أشعر أنها لمجازفة في التفاعل مع خدمة الحكومة الإلكترونية.					
5.6	قد يتم استخدام معلوماتي الشخصية بطريقة غير مقصود ةمن قبل وكالة حكومية.					
5.7	يمكن أن ينتزع معلوماتي الشخصية شخص ما بينما أرسل المعلومات إلى موقع الحكومة الالكترونية					
5.8	قد يتمكن المتسللين من الدخول الى المواقع الحكومية وسرقة المعلومات الشخصية المخزنة على شبكة الإنترنت					
5.9	سأكون على ثقة في استخدام الحكومة الإلكترونية عندما أتأكد من مقدارالأمن الذي يوفره الموقع					
5.10	سأكون على ثقة في استخدام الحكومة الإلكترونية عندمايضمن أن المعلومات المعاملات محمية من أي تغييرأوتدمير عن قصد أو غير قصد خلال الارسال على شبكة الإنترنت					
5.11	سأكون على ثقة في استخدام الحكومة الإلكترونية عند وجود آلية فعالة لمعالجة أي انتهاك للمعلومات الشخصية					
5.12	أود أن استخدام الحكومة الإلكترونية عند تطبيقها في كل وقت للتكنولوجياتا لتي تدعمها منظومة موثوق بها					
5.13	أود أن استخدم الحكومة الإلكترونية عندما تدعم في كل وقت تقنيات نظم آمنة					
5.14	أود أن استخدام الحكومة الإلكترونية عند تنفيذ الهياكل القانونية والتكنولوجية على نحو كاف للحماية من المخاطر التي تظهرعلى شبكة الإنترنت					
5.15	سأكون على ثقة في استخدام الحكومة الإلكترونية عندما تقدم خدمة ذات قيمة وفائدة بالنسبة لي					

لكم جزيل الشكر ☺ ،،،،

مساحة حرة للتعبير عن رأيك أو اضافة تعليق:

Appendix B: Questionnaire II

Sudan University of Science and Technology

College of Post Graduate studies

PhD Program by Taught Courses and Dissertation

3rd Batch

Questionnaire of e-government administrators and technical operator

I am Rasha Galal Eldin Hassan ,a PhD candidate in Sudan University of Science and Technology – College of Computer Science and Information Technology. I am conducting this survey for a research study under "**Developing an Approach for Securing E-government Accessibility"** and the study is going to be conducted as a requirement to fulfill a PhD. Degree in Computer science.

I choose you as one of the respondent to fill the survey questionnaire, to share your experience. This questionnaire has been designed to collect information from senior government officials, IT experts and some service level employees working in government service in Sudan. This questionnaire to evaluate our readiness in secured Sudan e-government communication and your assistance in this research study is vital even though your participation in it is completely voluntary.

Anything you fill in the survey questionnaire is confidential. Nothing you say will be personally attributed to you in any reports that result from this survey. All the reports will be written in a manner that no individual comment can be attributed to a particular person. The survey questionnaire will be used only for this study and will not be used for other purposes.

I would like to request you to participate in the survey with great thanks.

Please Kindly mark an (✓) in the column that most closely approximates your response

6. General Information:

2.20. Job position:

2.21. Gender:

Female	
Male	

2.22. Age:

(21-30)	
(31-40)	
(41-50)	
(51-60)	
(61-80)	

2.23. Level of experience:

1 year	
2-4 years	
5 year or more	
More than 10 years	

7. Please mark below the appropriate number where the numbers indicates:

1= Strongly Disagree 2= Disagree 3= Neither Disagree nor agree

4= Agree 5= Strongly Agree

		1	**2**	**3**	**4**	**5**
2.1	Inadequate understanding of advantages of E-Government					
2.2	IT Infrastructural weakness of government public sectors					
2.3	e-Gov services infrastructure adequate and properly set?					
2.4	There are no shortage of ICT Human Resource to implement e-Government					

8. **The table below lists the potential negative things that may result from e-government.** Please indicate how big a concern each one is to you on a scale of one to ten.
   A "10" means that you are extremely concerned, and a "1" means that you are not concerned at all. You may use any number from one to ten.

3.1	Government employees misusing personal information	
3.2	Hackers breaking into government computers	
3.3	It will become harder to get an answer	
3.4	Less personal privacy	
3.5	People without Internet access would get less government service	

9. Which of these Identification systems are validated by law in Sudan? (Chek all that apply):

Biometric	
Smart Card	
Single Sign-on	
Digital Signature	

10. Organizational and Administrative Challenge:

		Not a Challenge	**A Minor Challenge**	**An Important Challenge**	**A Very Important Challenge**	**Don't Know**
5.1	Resistance to change by government officials					
5.2	Coordination across central, regional and Local Government					
5.3	Coordination Between Public Administration, Citizen and other Actors					
5.4	Lack of policy support for e Government					
5.5	Avoid to changing services that manually working well in e Services					

11. Technical and Design Challenge:

		Not a Challenge	A Minor Challenge	An Important Challenge	A Very Important Challenge	Don't Know
6.1	Making e-Government services easily accessible to the visually impaired & other disabilities					
6.2	Difficulty in using E government applications					
6.3	Lack of secure electronic Authentication and Identification					
6.4	Lack of Standard for electronic Identification					
6.5	Lack of Interoperability between IT Systems					

12. Please check what security standard that e-gov services are used.

	Security standards	Options	Versions
7.1	Email security	1. S/MIME ☐ 2. PGP ☐ 3. PKI ☐ 4. Others: …. ☐ 5. None ☐	
7.2	Transport protocol	1. SSL ☐ 2. TSL ☐ 3. Others: ….. ☐ 4. None ☐	
7.3	Network protocol:	1. IPSec ☐ 2. Others: ….. ☐ 3. None ☐	
7.4	Encryption algorithm/ Digital signature	1. RSA ☐ 2. DSA ☐ 3. DES ☐ 4. 3DES ☐ 5. Others… ☐ 6. None ☐	

Thank you ☺

Appendix C: Interview questions

1. What e-government services provided to citizens now days in Sudan?
2. Is Sudan e-Gov portal active now?
3. What cultural gap do you perceive between citizens level of technological experience and the level of governmental web services that is being deployed?
4. What are the main barriers (inconveniences) of applying e-government in Sudan?
5. How important do you think the use of biometric technology is to e-government in Sudan? Are there any barriers to implement finger print technology in Sudan e-Gov?

Appendix D: Samples of Code

Signer Code:

```
<html>
<head>
<title>Fingerprint Digital Signature Application for RSA signing </title>

        <script language="JavaScript" type="text/javascript"
        src="jsrsasign-latest-all-min.js"></script>

        <script language="JavaScript" type="text/javascript">
        functiondoSign() {
                varrsa = new RSAKey();

rsa.readPrivateKeyFromPEMString(document.form1.prvkey1.value);
                varhashAlg = document.form1.hashalg.value;
                varhSig = rsa.signString(document.form1.msgsigned.value,
hashAlg);
                document.form1.siggenerated.value = linebrk(hSig, 64);
                        }

        functiondoVerify() {
        varsMsg = document.form1.msgverified.value;
        varhSig = document.form1.sigverified.value;
        var x509 = new X509();
        x509.readCertPEM(document.form1.cert.value);
        varisValid = x509.subjectPublicKeyRSA.verifyString(sMsg, hSig);

        // display verification result
```

```
if (isValid) {
_displayStatus("valid");
 } else {
_displayStatus("invalid");
}
}

functioncopyMsgAndSig() {
_displayStatus("reset");
 document.form1.msgverified.value = document.form1.msgsigned.value;
document.form1.sigverified.value = document.form1.siggenerated.value;
}

function _displayStatus(sStatus) {
var div1 = document.getElementById("verifyresult");
if (sStatus == "valid") {
 div1.style.backgroundColor = "skyblue";
 div1.innerHTML = "This signature is *VALID*.";
} else if (sStatus == "invalid") {
div1.style.backgroundColor = "deeppink";
div1.innerHTML = "This signature is *NOT VALID*.";
} else {
div1.style.backgroundColor = "yellow";
div1.innerHTML = "Please fill values below and push [Verify this sigunature] button.";
}
```

```
}
        </script>
<style type="text/css">
TD  {vertical-align: top}
</style>
</head>
<body>
        <h1>Fingerprint Digital Signature Application for RSA signing</h1>
<form name="form1" action="Validator.php" method="post">
        <table border="0">
        <tr><th>Signer</th><th></th><th></th></tr>

        <tr>
        <td>
        RSA Private Key<br/>
        <textarea name="prvkey1" rows="4" cols="25">
        -----BEGIN RSA PRIVATE KEY-----
        MIICWwIBAAKBgQDRhGF7X4A0ZVlEg594WmODVVUIiiPQs04
aLmvfg8SborHss5gQ
        Xu0aIdUT6nb5rTh5hD2yfpF2WIW6M8z0WxRhwicgXwi80H1aLPf
6lEPPLvN29EhQ
        NjBpkFkAJUbS8uuhJEeKw0cE49g80eBBF4BCqSL6PFQbP9/rByxd
xEoAIQIDAQAB
        AoGAA9/q3Zk6ib2GFRpKDLO/O2KMnAfR+b4XJ6zMGeoZ7Lbpi
3MW0Nawk9ckVaX0
        ZVGqxbSIX5Cvp/yjHHpww+QbUFrw/gCjLiiYjM9E8C3uAF5AKJ0
r4GBPl4u8K4bp
        bXeSxSB60/wPQFiQAJVcA5xhZVzqNuF3EjuKdHsw+dk+dPECQQ
DubX/lVGFgD/xY
```

uchz56Yc7VHX+58BUkNSewSzwJRbcueqknXRWwj97SXqpnYfKqZq78dnEF10SWsr

/NMKi+7XAkEA4PVqDv/OZAbWr4syXZNv/Mpl4r5suzYMMUD9U8B2JIRnrhmGZPzL

x23N9J4hEJ+Xh8tSKVc80jOkrvGlSv+BxwJAaTOtjA3YTV+gU7Hdza53sCnSw/8F

YLrgc6NOJtYhX9xqdevbyn1lkU0zPr8mPYg/F84m6MXixm2iuSz8HZoyzwJARi2p

aYZ5/5B2lwroqnKdZBJMGKFpUDn7Mb5hiSgocxnvMkv6NjT66Xsi3iYakJII9q8C

Ma1qZvT/cigmdbAh7wJAQNXyoizuGEltiSaBXx4H29EdXNYWDJ9SS5f070BRbAIl

dqRh3rcNvpY6BKJqFapda1DjdcncZECMizT/GMrc1w==

-----END RSA PRIVATE KEY-----

</textarea>

Fingerprint Minutiae Data to be signed.

<textarea name="msgsigned" rows="4" cols="25"></textarea>

</td>

<td></td>

<td>

</td>

</tr> <tr><td>

<img id="finger1" src="f1.jpg" alt="Fingerprint" width="90" height="90">

<canvas id="myCanvas" width="90" height="90" style="border:1px solid #d3d3d3;">

Your browser does not support the HTML5 canvas tag.</canvas>

<script>

```
document.getElementById("finger1").onload = function() {
var c = document.getElementById("myCanvas");
varctx = c.getContext("2d");
varimg = document.getElementById("finger1");
ctx.drawImage(img, 0, 0);
        varimgData = ctx.getImageData(0, 0, c.width, c.height);
//

        vari;
        varar=[10,20];
        for (i = 0; i<imgData.data.length; i += 1) {
        ar[i] = imgData.data[i];

                                                }

        ctx.putImageData(imgData, 0, 0);
        document.form1.msgsigned.value=ar.toString();
                                                        };
</script>
</td>
<td></td>
</tr>
<tr>
<td>
<select name="hashalg">
<option value="sha1" selected>SHA1
```

```
<option value="sha256">SHA256
<option value="sha512">SHA512
<option value="md5">MD5
<option value="ripemd160">RIPEMD-160
</select>

<input type="button" value="Sign with fingerprint &darr;" onClick="doSign();"/><br/>
</td>
<td>
<input type="submit" value="  Send to Verify  "><br/>
</td>
<td>
</td>
</tr>
<tr>
<td>
Generated Signature<br/>
<textarea name="siggenerated" rows="4" cols="25"></textarea>
</td>
<td>
</td>
<td>
<br/>

<br/>
</td>
```

```
        </tr>

        </table>

        </form>

</body>

</html>
```

Validator code:

```
<html>
<head>
<title>Fingerprint Digital Signature Application for RSA signing </title>
        <script language="JavaScript" type="text/javascript" src="jsrsasign-latest-all-min.js"></script>
        <script language="JavaScript" type="text/javascript">

        window.onload=function(){
        document.getElementById("button").style.display='none';

        }
        functiondoLogin(){
        document.getElementById("demo").target = "_blank";
        document.getElementById("demo").innerHTML = "<H2>user Verified and information are available here!....</H2>";
                                }

        functiondoVerify() {
        varsMsg = document.form1.msgverified.value;
        varhSig = document.form1.sigverified.value;

        var x509 = new X509();
        x509.readCertPEM(document.form1.cert.value);
        varisValid = x509.subjectPublicKeyRSA.verifyString(sMsg, hSig);

        // display verification result
        if (isValid) {
          _displayStatus("valid");
        document.getElementById("button").style.display='block';
        } else {
         _displayStatus("invalid");
                }
                        }

        function _displayStatus(sStatus) {
```

```
        var div1 = document.getElementById("verifyresult");
        if (sStatus == "valid") {
        div1.style.backgroundColor = "skyblue";
         div1.innerHTML = "This signature is *VALID*.";
          } else if (sStatus == "invalid") {
         div1.style.backgroundColor = "deeppink";
         div1.innerHTML = "This signature is *NOT VALID*.";
        } else {
          div1.style.backgroundColor = "yellow";
          div1.innerHTML = "Please fill values below and push [Verify this sigunature] button.";
                }
                                        }

        </script>

<style type="text/css">
TD  {vertical-align: top}
</style>
</head>


<body>
<p id="demo">
        <h1>Fingerprint Digital Signature Application for RSA signing</h1>

        <form name="form1">
        <table border="0">
        <tr><th></th><th></th><th>Verifier</th></tr>

        <tr>
        <td>
        <br/>
        </td>
        <td></td>
        <td>
        Verification Result
        <div id="verifyresult" style="background: yellow">Please fill values below and push "Verify this Fingerprint sigunature" button.</div>
        </td>
        </tr>
        <tr><td>                </td>
        <td></td>       </tr><tr>       <td>
                </td>
```

```
<td>  </td><td>
<input type="button" value="Verify your fingerprint signature &uarr;"
onClick="doVerify();"/><br/>
<input type="button" value="Now you Can Log in!" id="button"
onClick="doLogin();"><br/>
</td>
</tr>
<tr>
<td></td>
<td>  </td>  <td>

Verifying Signature<br/>
<textarea name="sigverified" rows="4" cols="25"><?php echo
$_POST["siggenerated"]; ?></textarea><br/>

Fingerprint Data to be verified.<br/>
<textarea name="msgverified" rows="4" cols="25"><?php echo
$_POST["msgsigned"]; ?></textarea><br/>

Signer's Public Key Certificate.<br/>
<textarea name="cert" rows="4" cols="25">
-----BEGIN CERTIFICATE-----
MIIBvTCCASYCCQD55fNzc0WF7TANBgkqhkiG9w0BAQUFAD
AjMQswCQYDVQQGEwJK
UDEUMBIGA1UEChMLMDAtVEVTVC1SU0EwHhcNMTAwNTI
4MDIwODUxWhcNMjAwNTI1
MDIwODUxWjAjMQswCQYDVQQGEwJKUDEUMBIGA1UECh
MLMDAtVEVTVC1SU0EwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANGEYXtfgDRlW
USDn3haY4NVVQiKI9Cz
Thoua9+DxJuiseyzmBBe7Roh1RPqdvmtOHmEPbJ+kXZYhbozzPR
bFGHCJyBfCLzQ
fVos9/qUQ88u83b0SFA2MGmQWQAlRtLy66EkR4rDRwTj2DzR4
EEXgEKpIvo8VBs/
3+sHLF3ESgAhAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAE
Z6mXFFq3AzfaqWHmCy1
ARjlauYAa8ZmUFnLm0emg9dkVBJ63aEqARhtok6bDQDzSJxiLpC
EF6G4b/Nv/M/M
LyhP+OoOTmETMegAVQMq71choVJyOFE5BtQa6M/lCHEOya5Q
UfoRF2HF9EjRF44K
3OK+u3ivTSj3zwjtpudY5Xo=
-----END CERTIFICATE-----
</textarea><br/>
</td>
```

```
        </tr>

        </table>
        </form>

</p>
</body>
</html>
```

Publications:

1. Rasha G. Hassan, Othman O. Khalifa, (2015) Challenging Development Citizen-Centric E-Governance in Sudan, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, August 2015
2. Rasha G. Hassan, Othman O. Khalifa, (2016), E-Government - an Information Security Perspective, International Journal of Computer Trends and Technology (IJCTT) V36(1):1-9, June 2016. ISSN:2231-2803.
3. Rasha G. Hassan, Othman O. Khalifa, Toward user awareness and Acceptance of Sudan e-government: Adoption and Security perspective, in Proceedings of TICET 2016, Third International Conference on Information and Communication Technologies for Education and Training, Khartoum, Sudan.