Sudan University of Science and Technology
College of Graduate Studies

A proposed Design of a Framework for Sudanese E-Government Security Model

تصميم مقترح لاطار أنموذج لأمن الخدمات الحكومة الإلكترونية السودانية

Thesis Submitted for Ph.D Degree in Information Technlogy

By

Omar Abdul Rahman Ali

Supervisor:
Prof. Izzeldin Mohammed Osman
Co-supervisor:
Dr. Talaat Mohi Elddin Wahby

August 2017

DEDICATION

To my parents,

to my wife,

and to my daughter

ACKNOWLEDEMENT

Foremost, I would like to express my sincere gratitude to my advisor Prof. Izzeldin Mohamed Osman for the continuous support of my Ph.D. research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study. I wish to thank Dr. Taaat Wehbi , the second supervisor, for his support.

I am grateful to National Information Center in Sudan.

Finally, I wish to extend my heartfelt appreciation to my family: my parents, and my wife for their unconditional love, spiritual support and sacrifice which has enabled me to pursue my dreams.

ABSTRACT

E-government is a kind of governmental administration which is based on electronic information technology. One of the key factors that realizes integration and information sharing to the inter-governmental administrations is the trust level. Information security contributes directly to the increased level of trust and confidence between the government departments by providing an assurance of confidentiality, integrity, and availability of sensitive governmental information.

The main objective of this research is to design of a framework for Sudanese e-government security model. It has identified the critical factors affecting e-government security in Sudan, and attempted to propose an e-government security framework.

This proposed model of Sudanese e-services security is based on the existence of technical and non-technical factors. This research proposes a framework for Sudanese e-government security model that can be used as a tool to assess the level of security readiness of government departments, a checklist for the required security measures, and as a common reference for the security in the government departments in Sudan. The framework was evolved from the analysis to the potential security threats in Sudanese situation and how to countermeasure these threats. Similar problems in othe countries were taken into account.

In this model four layers are proposed: a technical layer, IT infrastructure layer, managerial layer and law and legislation layer. Each layer will mitigate group of threats related to e- services.

المستخلص

الحكومة الإلكترونية هي نوع من الإدارة الحكومية التي تقوم على تكنولوجيا المعلومات الالكترونية. ومن بين العوامل الرئيسية التي تحقق التكامل وتبادل المعلومات مع الإدارات الحكومية الدولية مستوى الثقة. ويسهم أمن المعلومات بشكل مباشر في زيادة مستوى الثقة بين الدوائر الحكومية من خلال توفير ضمان للسرية والنزاهة وتوافر المعلومات الحكومية الحساسة.

والهدف الرئيسي من هذا البحث هو تصميم إطار لنموذج أمن الحكومة الإلكترونية السودانية. وقد حددت العوامل الحاسمة التي تؤثر على أمن الحكومة الإلكترونية في السودان، وحاولت اقتراح إطار أمني للحكومة الإلكترونية.

ويستند هذا النموذج المقترح لأمن الخدمات الإلكترونية السودانية إلى وجود عوامل تقنية وغير تقنية. ويقترح هذا البحث إطارا لنموذج أمن الحكومة الإلكترونية السودانية يمكن استخدامه كأداة لتقييم مستوى الجاهزية الأمنية للإدارات الحكومية وقائمة مرجعية للإجراءات الأمنية المطلوبة وكمرجع مشترك للأمن في الدوائر الحكومية في السودان. وقد تطور الإطار من التحليل إلى التهديدات الأمنية المحتملة في الحالة السودانية وكيفية التصدي لهذه التهديدات. وأخذت مشاكل مماثلة في بلدان أخرى بعين الاعتبار.

ويقترح في هذا النموذج أربع طبقات: طبقة تقنية، طبقة بنية تحتية لتكنولوجيا المعلومات، طبقة إدارية، وطبقة قانونية تشريعية. وسوف تخفف كل طبقة من مجموعة التهديدات ذات الصلة بالخدمات الالكترونية.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Introduction

Electronic government can be defined as government use of information communication technologies to offer citizens and businesses the opportunity to interact and conduct business with government by using different electronic media such as telephone touch pad, fax, smart cards, e-mail / Internet and self-service kiosks that provides an interactive environment for customers, employees, and the general public to get instant access to information or to make purchases [1]. One of the key benefits to kiosks is that you don't need assistance from store employees. You can pull up a menu of options by touching the screen and following a series of directions. Electronic government is about how government organizes itself: it's administration, rules, regulations and frameworks set out to carry out service delivery and to co-ordinate, communicate and integrate processes within itself [2]. There are three main categories of communication in e-governments: Government-to-Government (G2G), Government-to- Business (G2B), and Government-to-Citizen (G2C) [3].

Ake specifies 7 purposes for using e-government [4]:

1-Providing One-stop Government, one-stop government refers to the integration of public services from a customer's (citizen, business) viewpoint. Online one-stop government allows customers to have 24-hours access to public services from their home or even on the move. [5]

2- Moving Government Procurements online.

3- Implementing Electronic Filing.

4- Key developing a public infrastructure.

5- Putting government services online.

6- Electronic facilitating payment.

7- Improving government accountability and efficiency.

The challenges in e-government services' security [6] include identifying users, authenticating users, storing public and classified information in same websites, checking authorizations, auditing, signing transactions, resolving conflicts, keeping copies of information, and so on. Hence e-government security systems should be able to meet the following requirements: should provide multiple authentication methods, authorization, credential issuance and revocation [7], audit, confidentiality, conflict resolution, accountability, availability, platform independent, privacy, information integrity, anonymity, scalability, single sign on and so on. The challenges and requirements were analyzed to find ways of providing security services in e-government.

1.2 Research problem

In Sudan, the e-services are accessed through different government department portals and not through the official e-government portal and the government portal acts as a catalogue and directs the citizens to the selected e-service.

In Sudan, to complete a single e-service a citizen will have to access multiple portals.

In this thesis document a new security model is developed for the e-government authority and its affiliated government departments.

It is meant to be used as a reference and a standard for assessing the level of security in each department.

The new security model will also assist in ascertaining the current level of security of each department, giving the confidence to other departments and serve as a mitigation action of the risks that may exist in the future.

1.3 Research objectives

The main objective of this research is:

To design an applicable security model for Sudanese electronic government. This security model should be adapted with Sudanese circumstances.

1.4 Research questions

1. What are the main elements and factors affecting e-government security in Sudan?
2. How can the identified critical factors help to build the holistic security model of e-government in Sudan?

1.5 Importance of research

When building any web-based application e.g. electronic government, the issue of security is always a concern. Citizens will be reluctant to use the web based services offered by the government due to, lack of confidence, security and privacy concerns, also if there is a standard model for security the processes of risk analysis, and updates for application will be very easy.

Resulted in the different geographical diversity of nature in the Sudan from the mountainous areas and plains and valleys to the difference in the use of networking technology to suit the different nature of each region. Systems in e-government is dealing with the same applications of these outlying areas and of diverse nature and different networking technology, it led to the following fact: given that e-government applications targeting the application of certain security services within the different networking technologies, the different networking technology necessarily lead to the different procedures and processes used to achieve certain security service.

1.6 Contribution to knowledge

The new proposed model is a comprehensive model because of it covers a variety of threats (technical and non-technical) to information security. It has an ability to extend new threat. The model is not complicated it is so clear it is easy to be understood by users. The new model also provides the e-government authority and its affiliates a structured methodology to assess the security level in the government departments, a checklist of all the security elements required to build a robust security programme and architecture. The new model addresses some of the main domains of ISO17799 by addressing policies, and the people skills. The new model has four strong characteristics:

The ability of using it in multiple purposes: The new proposed model is deal with more than the technological aspect. And it can be used as a checklist for what’s implemented and what’s in the future plan. And also can be used as tools to give holistic view for security aspects.

The flexibility: The model is flexible to use with any technology.

Complement the previous models: One steps of methodology in this research is a literal view, that means this model is take its construction from other models and it becomes a complement of previous models.

1.7 Thesis organization

Chapter tow talks about the e-government features in terms of: concepts, definitions and perspectives. The literature reviewed in this chapter is an attempt to better understand the security challenges. Thereafter, the literature covered the current situation of e-government security around the world and the critical factors influencing its adoption within the context of developing countries. Chapter three describes the methodology adopted for the execution of the current research. The empirical design illustrates how the research was conducted. The last part of this chapter addressed information about Sudan. Chapter four provides the risks that faced e-government security in Sudan. Chapter five provides the security requirements to countermeasure the threats of the Sudanese e-services as a model. Chapter six proposes the security framework for Sudanese e-government security. Finally, in Chapter seven the conclusions are presented.

CHAPTER II

E-GOVERNMENT FEATURES

2.1 Introduction

This chapter focuses on electronic government systems, information security concepts, and related works.

Initially the aim of the research was to build an information security model for any e-organisation and was then narrowed to address e-government security.

The fast development of the Information and Communication Technology (ICT) derived the rapid growth in the number of government websites as well as the variety of services offered. Nearly all countries across the glob, from the poorest countries to the most advanced ones, have some sort of Internet presence, or so-called e-government. The United Nations Division for Public Economics and Public Administration (UNDPEPA) defines e-government as "Utilising the Internet and the World Wide Web for delivering government information and services to citizens". The advantages of e-government are unquestionable.

E-government primarily refers to the use of Information Technology in governmental organisation processes, even though the use of IT tools in the public sector is not a new practice. Some countries have been using IT in their governmental processes and procedures since the 1950s [8]. The difference is that IT was used to automate the internal work of government by processing data, whereas now, the use of ICT is transforming the external work of government by processing and communicating data [8]. E-government is therefore to be seen as an evolutionary rather than a revolutionary phenomenon [9]. In recent decades, the topic of electronic government (e-government) has been the subject of much debate within the research community [10]. Since the emergence of e-government in the late 1990s, the public sector has invested heavily in Information and Communication Technology (ICT) to support their work processes and e-enable their services. However, with the increasing use of e-commerce in the private sector, citizens have become more experienced in the use of electronic services, thus expecting a similarly high standard of service quality from government agencies. Yet, the literature suggests that individuals' performance vary based on their self-efficacy and therefore have different expectations [11]. Bandura [12] argues that the advancements in ICT and associated social developments have had a considerable influence on personal efficacy for self-development. In e-government, the purpose is to improve service delivery to all stakeholders [13] but research suggests that the potential of e-government services and enabling IT applications are underutilized [14]. This has forced government organizations to change their current technologies or to adopt other strategies that combine multi-channels for e-government service delivery [15].

Each Electronic Government initiative requires the use of standards for deployment of innovative, web-based Information technology (IT) services. Standards are required to ensure the necessary interoperability and security between government agencies, businesses, and citizens.

2.2 Concepts of e-government

E-government is comparatively new and ideas are yet to mature and be well defined [16]. The concept is currently still without a universally agreed standard definition and it can mean different things to different people. Some see e-government as a goal in itself; some view it as a tool for achieving broader public sector reform goals [17]. Nonetheless, there are some commonly agreed notions, including: government efficiency and effectiveness; empowering citizens, organizations and communities through access to information; strengthening levels of democracy; citizen-participation; and transparency [18]. These concepts have fundamentally transformed the way of thinking and working in the public sector [19, 20]. E-government is reforming the way governments provide services electronically and revitalising the relationship with citizens and business [21]. This reform process is not simply about computerising a government system; rather it is the ability to use technology: “to achieve levels of improvement in various areas of government” [22].

The growth of e-government, [23] identified three different phases:

Phase I: Governments goal the use of ICT (mainly Web Technology), to deliver public services electronically, in order to: “improve government efficiency, meet citizen expectations and facilitate economic development”.

Phase II: Governments started to do business through delivering services electronically. This was considered as a reinvention of government. Governmental organisations also began to have new features, such as: being community-owned; showing increased competitiveness; being more decentralised and market-oriented.

Phase III: This represents the current situation in e-government; it is about the reengineering processes needed to change the existing design of government organisations. Centralized, vertical and hierarchical structures were previously developed for the industrial economy and society, but now the aim is to build new management paradigms appropriate for the transformation to the information-based economy and society.

2.3 E-government Definitions and Perspectives

There are numerous elements which encompass the e-government concept [24]. Grant [25] states that e-government is: “more than a pure technological phenomenon”; therefore, it requires a broad definition and understanding [26]. According to Yildiz, M. [17], the difficulty in defining e-government is as a result of its multiple meanings. These meanings might depend on the specific context, regulatory environment, dominance of a group of actors in a given situation, or the different priorities in government strategies. [27] E-government can be viewed within a number of disciplines; such as, Information Systems (IS), computer science, public administration and political science [10]. Seifert and Petersen [28], define two perspectives from which to identify e-government: the technical level and the political level. Some identify e-government from a technological perspective and from a business perspective [29]. Lenk [30], identifies four different perspectives of e- government: citizen, process, cooperation and knowledge management. Thus, it is more appropriate to define e-government based on its stakeholders’ perspective and their aims and objectives. This is because the meaning of e-government and its adopted values and goals will largely depend on the stakeholders’ interests [31]; [17].

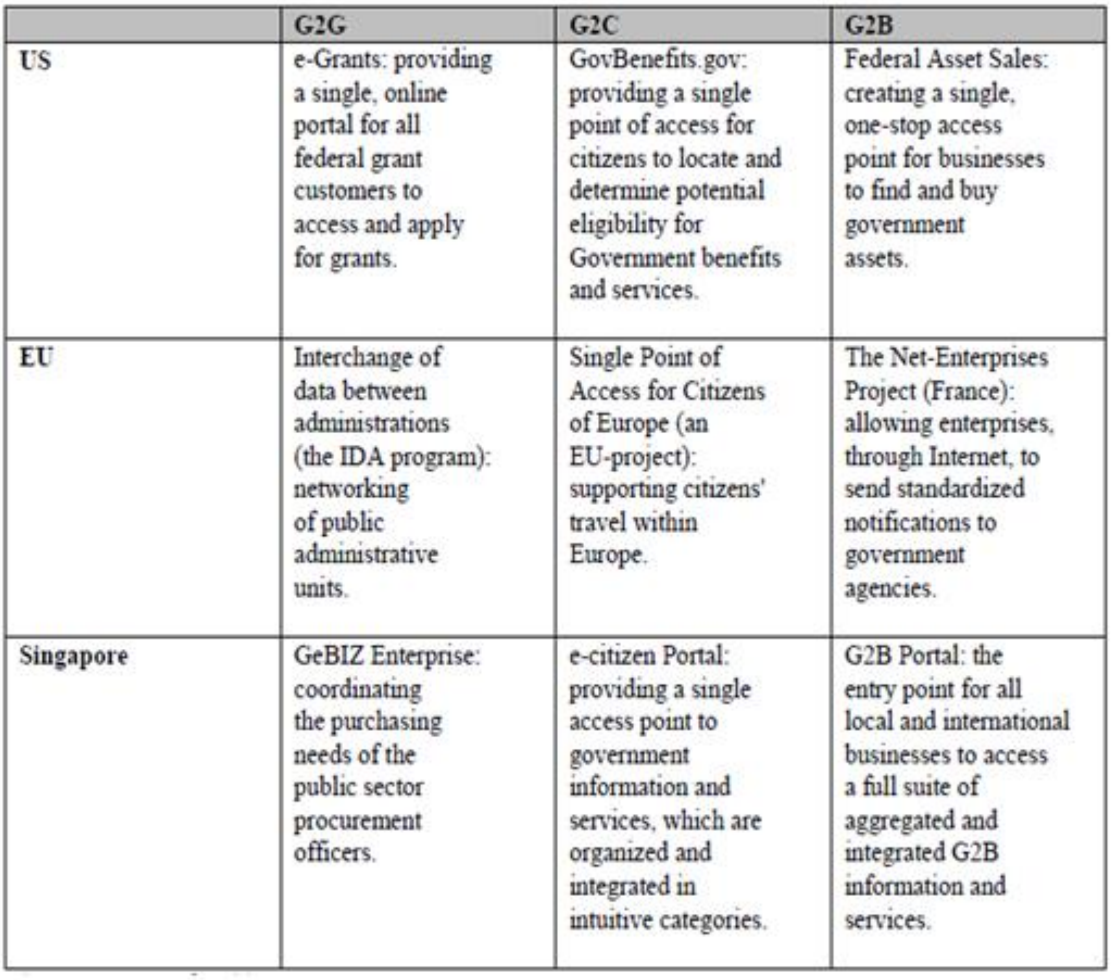
2.4 E-government Domains

E-government involves various activities and stakeholders and also serves different groups of people, sectors, and organizations in a variety of domains. The World Bank [32] identified three distinct domains for e-government interaction:

1. Government-to-citizens (G2C): government aims to interact with citizens.
2. Government-to-business (G2B): government aims to interact with business enterprises.
3. Government-to-government (G2G): government aims to make services more friendly, convenient, transparent, and inexpensive.

The G2G domain is seen as the backbone of e-government implementation, as it paves the way for e-government use in the country as a whole [33]. Examples of the services offered in the three domains are shown in Table 2.1

Table 2.1: E-government services offered in the three domains [33]



	G2G	G2C	G2B
US	e-Grants: providing a single, online portal for all federal grant customers to access and apply for grants.	GovBenefits.gov: providing a single point of access for citizens to locate and determine potential eligibility for Government benefits and services.	Federal Asset Sales: creating a single, one-stop access point for businesses to find and buy government assets.
EU	Interchange of data between administrations (the IDA program): networking of public administrative units.	Single Point of Access for Citizens of Europe (an EU-project): supporting citizens' travel within Europe.	The Net-Enterprises Project (France): allowing enterprises, through Internet, to send standardized notifications to government agencies.
Singapore	GeBIZ Enterprise: coordinating the purchasing needs of the public sector procurement officers.	e-citizen Portal: providing a single access point to government information and services, which are organized and integrated in intuitive categories.	G2B Portal: the entry point for all local and international businesses to access a full suite of aggregated and integrated G2B information and services.

2.5 Developmental stages of e-government

According to Layne. K, Lee. J. [142] there are four stages to of a growth model for e-government: (1) cataloguing, (2) transaction, (3) vertical integration, and (4) horizontal integration. These four stages are explained in terms of complexity involved and different levels of integration as shown in figure 2.1.

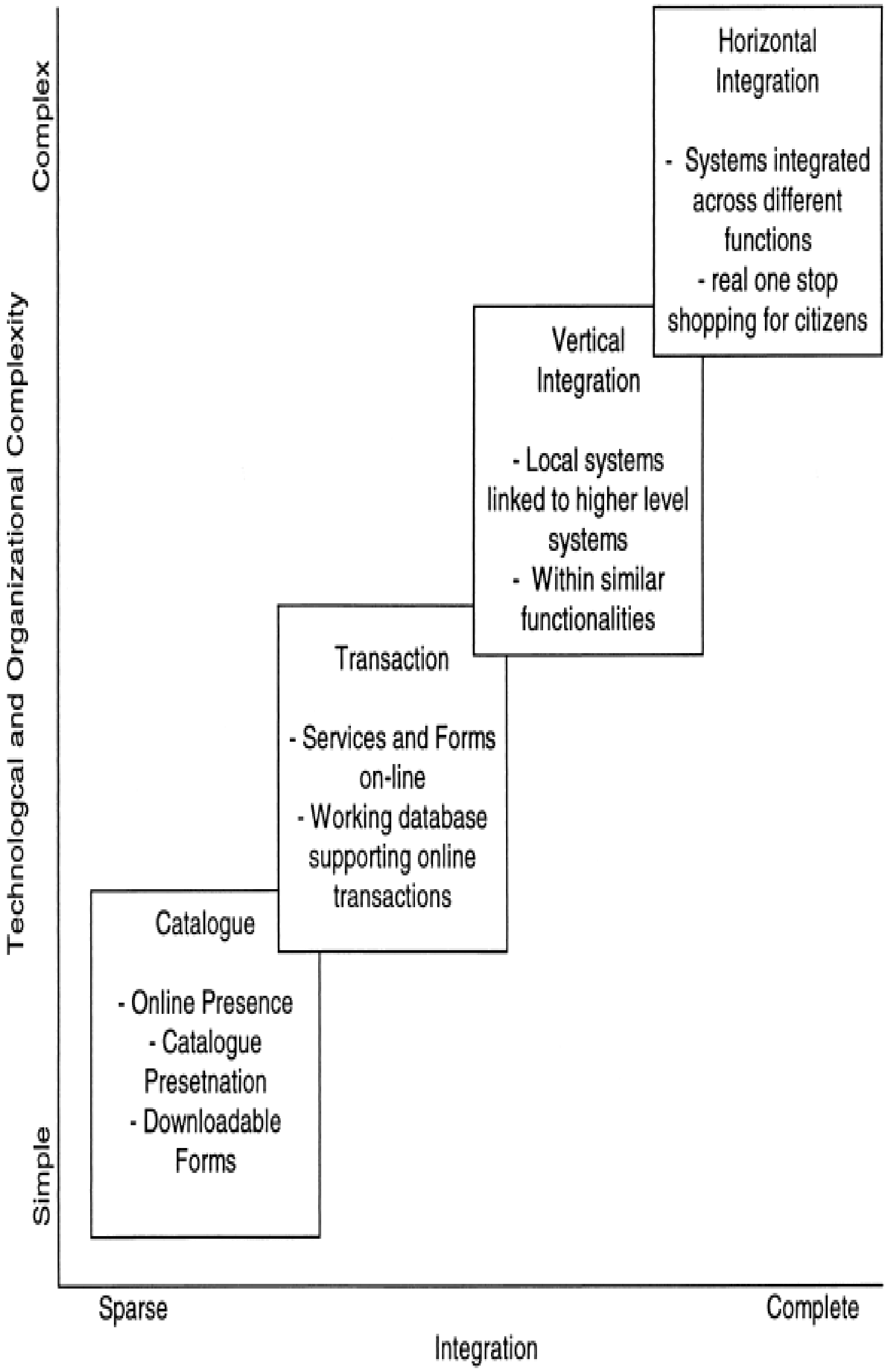

Technological and Organizational Complexity
Simple
Complex
Catalogue
- Online Presence
- Catalogue Presetnation
- Downloadable Forms
Transaction
- Services and Forms on-line
- Working database supporting online transactions
Vertical Integration
- Local systems linked to higher level systems
- Within similar functionalities
Horizontal Integration
- Systems integrated across different functions
- real one stop shopping for citizens
Sparse
Complete
Integration

Figure 2.1: This figure shows the Dimensions and stages of e-government development.

2.5.1 Stage I: cataloguing

In stage one, governments create a ‘state website’ mostly due to a great deal of pressure from the media, technology-literate employees, demanding citizens, and other stakeholders to get on the “net.” At this stage, governments do not have much Internet expertise, and they prefer to minimize the risk by doing a small project. Parts of the government’s nontransactional information are put on the site. There are several reasons why any government would want to move to this ‘electronic cataloguing’ stage, but mostly, many citizens and businesses have access to the web. As they are able to access information on services from the private sector from the web, they expect the same access from the government.

2.5.2 Stage II: transaction

As government websites evolve, officials as well as citizens come to realize the value of the Internet as another service channel for citizens and want to exploit it. Citizens demand to fulfill government requirements on-line instead of having to go to a specific location to complete paperwork. Electronic transactions offer a better hope for improved efficiency for both the customer and the agency than simply “cataloguing information.”

In addition, such capabilities provide the opportunity for a broader democratic process by holding interactive conversations with constituents who are reluctant or unable to attend public hearings. There is no question that fully functional e-government will make service delivery more efficient and increase savings for both government and the citizen. This second stage is the beginning of the e-government as a revolutionary entity changing the way people interact with their government. This stage empowers citizens to deal with their governments on-line anytime, saving hours of paperwork, the inconvenience of traveling to a government office and time spent waiting in line. Registering vehicles or filing state taxes on-line are only the beginning of such transaction-based services.

2.5.3 Stage III: vertical integration

At this stage, the focus is now moving toward transformation of government services, rather than automating and digitizing existing processes. Making government electronic is not simply a matter of putting existing government services on the Internet. What should and will be happening are permanent changes in the government processes themselves and possibly the concept of government itself. Just as electronic commerce is redefining private business and society in terms of processes and product, electronic government initiatives should be accompanied by re-conceptualization of the government service itself. In the long run, the full benefit of e-government will be realized only when organizational changes accompany technological changes. After on-line transaction services become prevalent and mature, citizens' expectations will increase. Most transaction stage systems are localized and fragmented. A natural progression will be the integration of scattered systems at different levels (vertical) and different functions (horizontal) of government services. Agencies often maintain separate databases that are not connected to other governmental agencies at the same level or with similar agencies at the local or federal level. For example, a state business license database is often separate from a local business license database. Further, that state license system is probably.

2.5.4 Stage IV: horizontal integration

The full potential of information technology, from the citizen's perspective, can only be achieved by horizontally integrating government services across different functional walls (or "silos"). The limitations of the functional nature of both the public and private sector will become clearer as more public administrators begin to see the vision opened by the Internet. Typically, citizens requiring assistance from governments need more than one service. Those requiring housing also need governmental assistance for education, housing, food, medical attention, etc. To overcome this problem, some localities provide one stop service centers where, for example, the homeless can come and obtain information about jobs, clear any outstanding warrants, obtain medical assistance, etc.

Governments continually fight the battle of getting services to the people who need them the most. The horizontal integration of the stage four will considerably improve those efforts. Databases across different functional areas will communicate with each other and ideally share information, so that information obtained by one agency will propagate throughout all government functions.

2.6 E-government around the world

Increasing access to ICT has encouraged many governments to integrate new technology into their national economic development strategies [34]. It is becoming a more and more important public service tool for many governmental departments around the world [35], and the scale of activity on the part of public sectors in leveraging IT has increased in volume [36]. The greater part of public organisations around the world have established websites and provide public information to citizens [37]. In addition, many transactions are now conducted online; these include, applying for jobs, completing tax returns and renewing drivers' licenses [38], Figure 2-2 shows a large number of countries at lower levels of online service development, highlighting the relative difficulty in supplying transactional and connected services—as described by the Survey's four-stage model. The world mean Online Service Index value is 0.3919, far below what might be considered indicative of global convergence with the leading countries in this field.

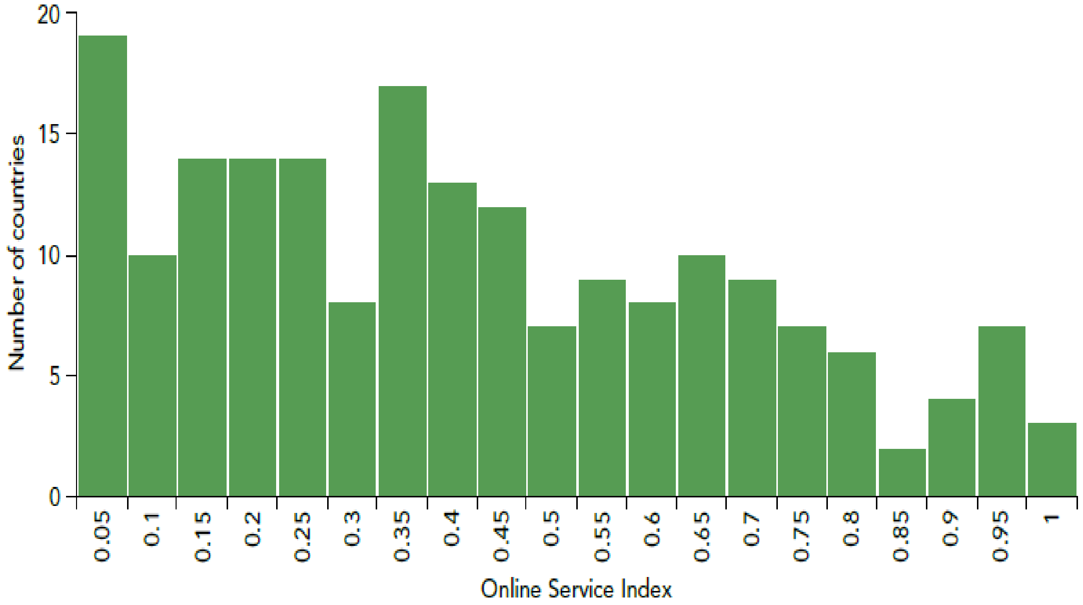


Figure 2.2: This figure shows Distribution of Online Service Index values [37]

Figure 2.2 provides a breakdown of typical transactional services and the number of countries for which these services could be readily identified through the national website. Of the transactional services included in the Survey instrument, the most commonly found were setting up of personal online accounts (101 countries),income tax filing (73 countries) and business registration (60 countries). An open-ended 'other' category also scored well (76 countries) reflecting a diversity of priorities in building and expanding online services at national level.

Figure 2.3 provides a breakdown of typical transactional services and the number of countries for which these services could be readily identified through the national website. Of the transactional services included in the Survey instrument, the most commonly found were setting up of personal online accounts (101 countries),income tax filing (73 countries) and business registration (60 countries). An open-ended 'other' category also scored well (76 countries) reflecting a diversity of priorities in building and expanding online services at national level.

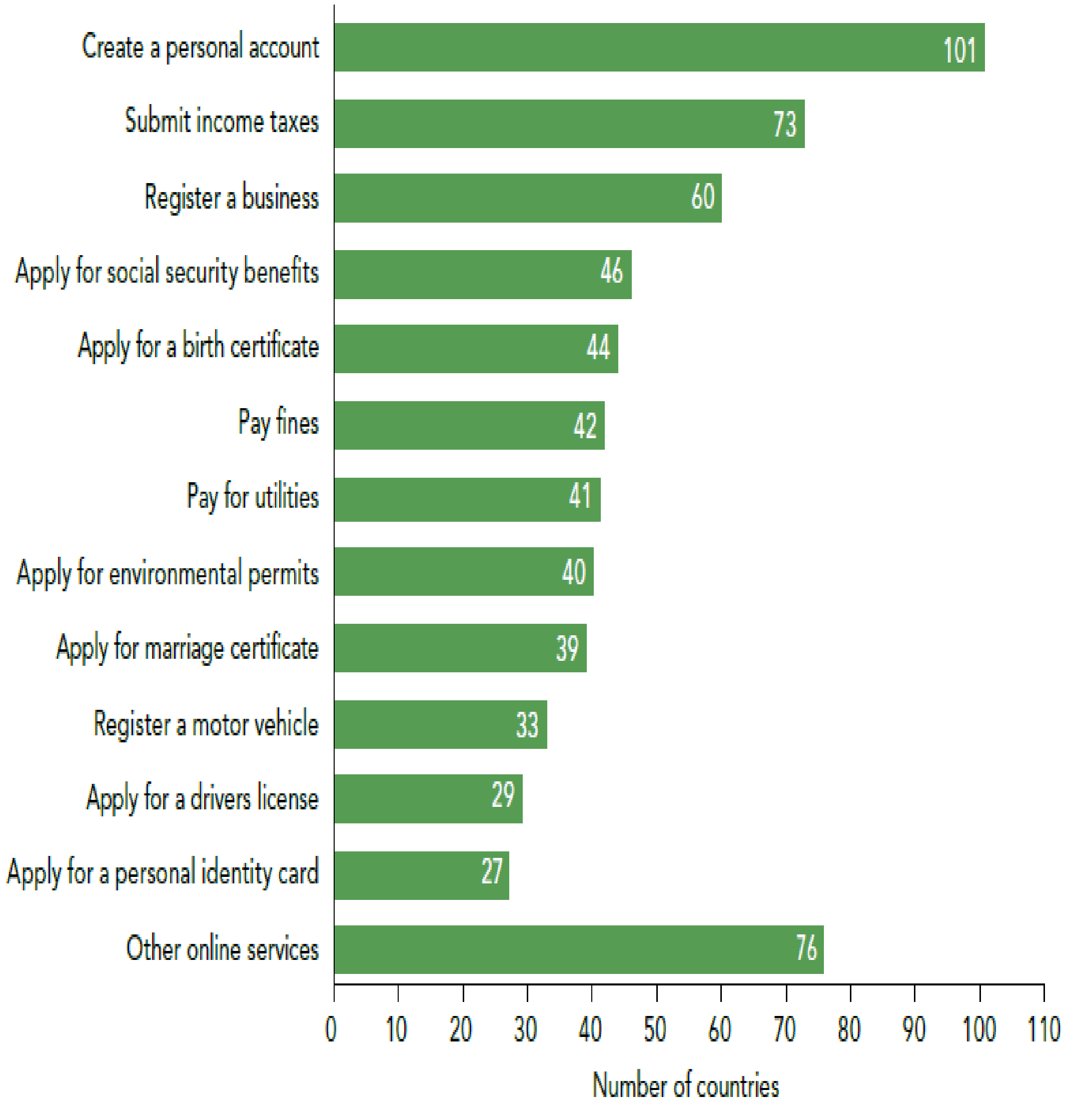


Figure 2.3: This figure shows the Transactional services online [37]

When considering e-government development in different government sectors, there is additional evidence of the validity of the general four-stage model of progress as shown in Figure 2.3.

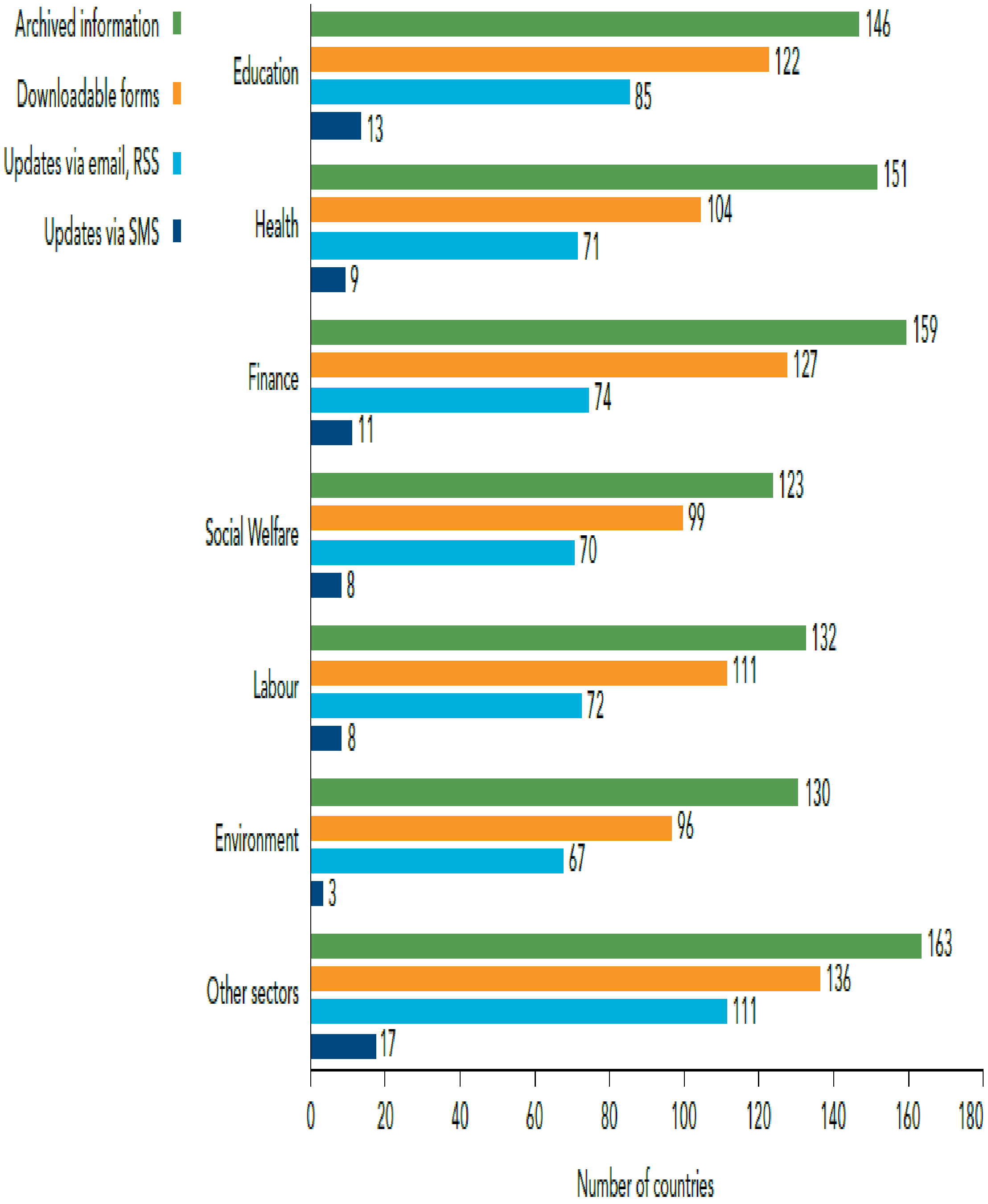


Figure 2.4: This figure shows Types of services online, by sector [39]

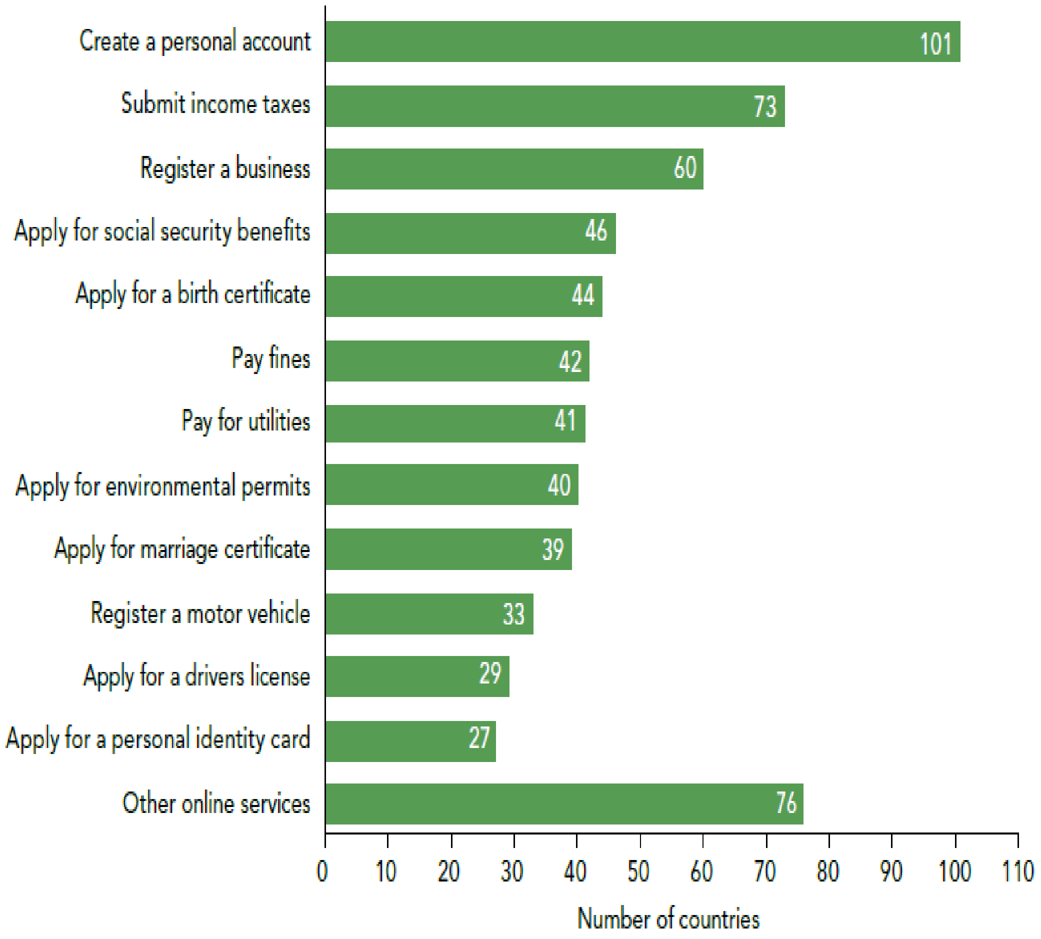


Figure 2.5: This figure shows the Transactional services online [39]

2.6.1 Online Services and Applications

Generally speaking, e-service operation is one where all or part of the interaction between the service provider and the customer is conducted through the Internet and an e-service has a “front-end” Web-based systems and “back-end” information systems. [40]

In this survey, online services refer to the systems of e-procurement, e-tax, e-customs, e-health and one-stop service. The most recent trends show that some governments in developing countries have shifted to user-oriented strategies and developed one-stop service portals. They are also planning to gradually expand and enhance integrated service delivery [40].

In general, there are no significant gaps in online service delivery among countries in the top10 list. This year witnesses the enhancement of online service delivery for most top 10 countries, with the exception of Estonia, Singapore and Korea, which scored a little bit lower than last year. Iceland, for the first year being monitored by the ranking system, stood in the 5thposition of e-service delivery ranking. [40]

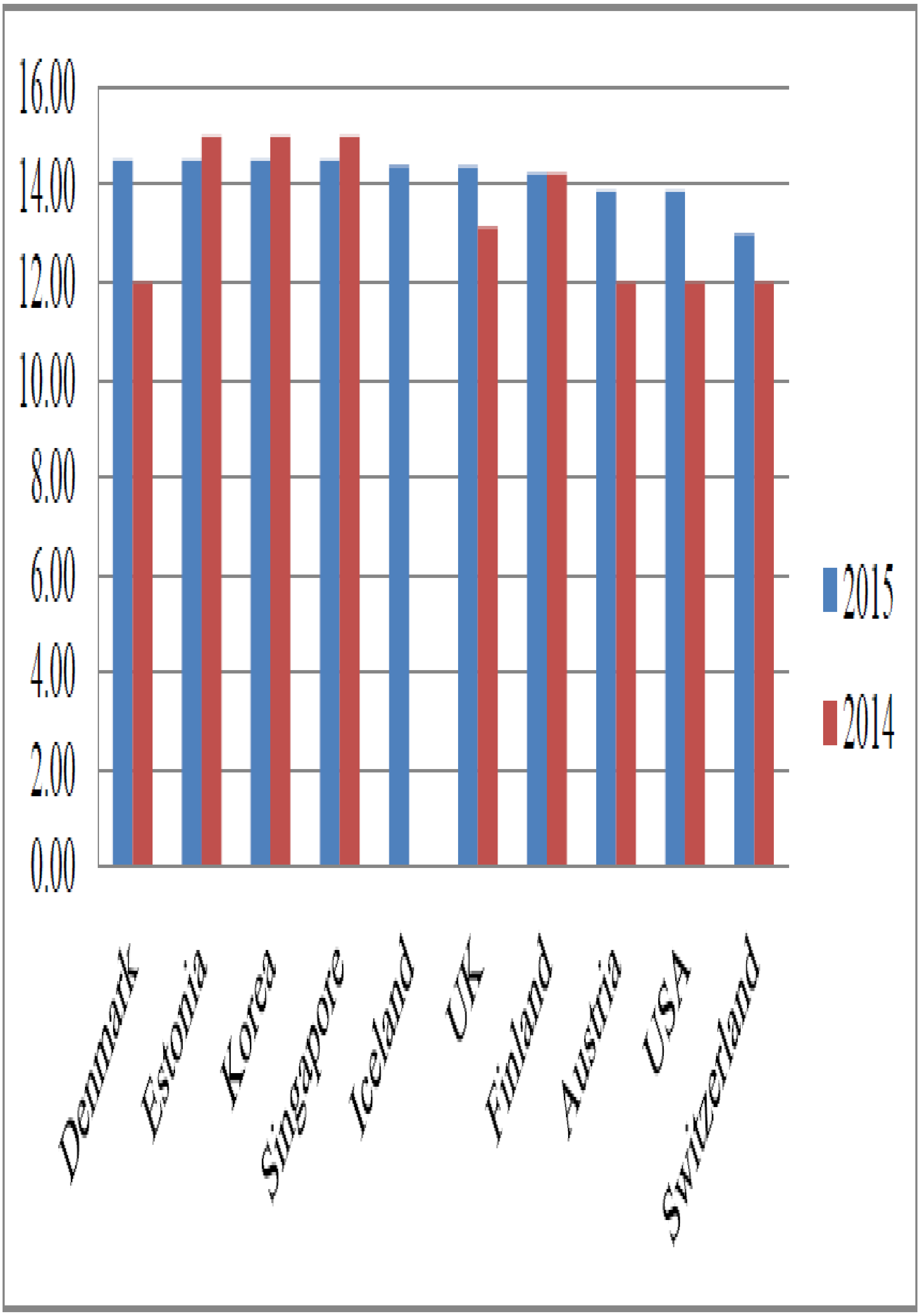


Figure 2.6: This figure shows the top 10 Online Service 2014-2015 [40]

2.6.2 Cyber Security

The security measures associated with individual e-government systems are relatively similar to many e-commerce solutions. However, the span of control of e-government and its unique impact on its user base requires a network that is greater than the sum of each individual system. E-government faces the same challenges as e-business in the private sector, but the stakes are often higher. [40]

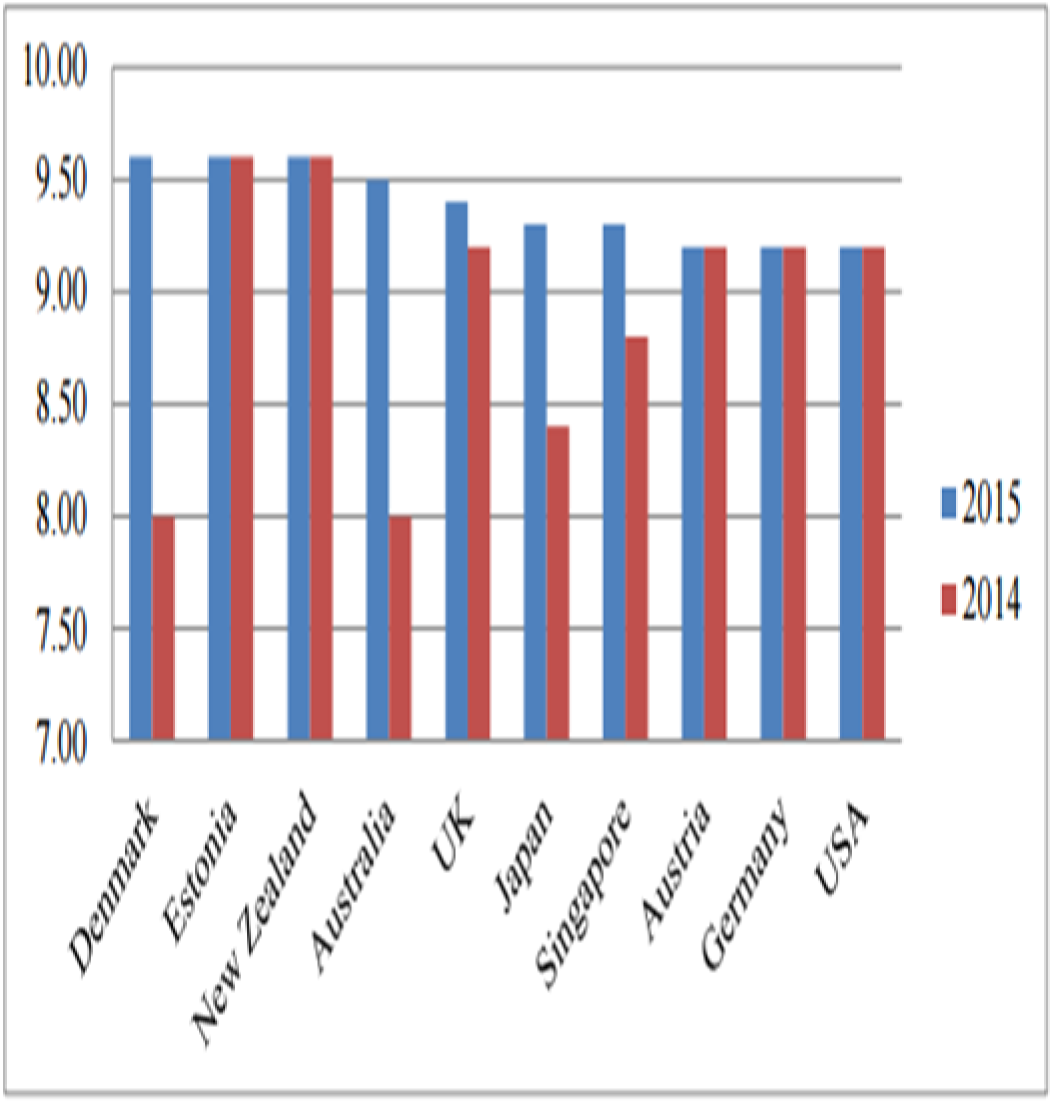
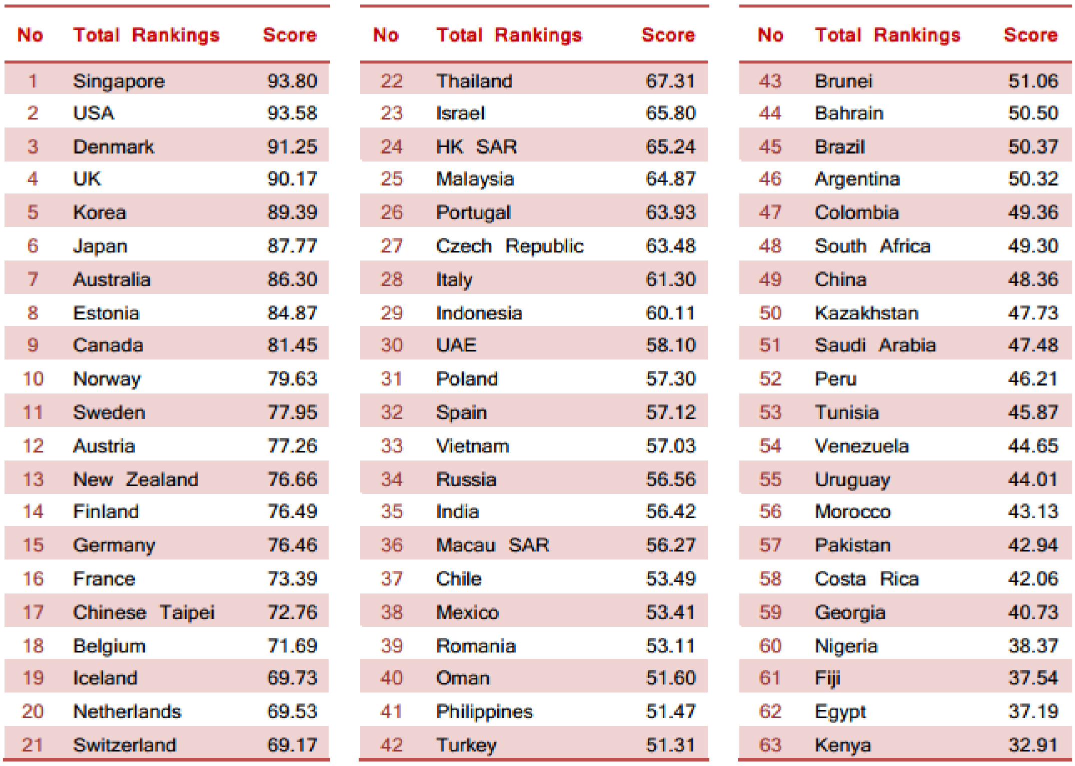


Figure 2.7: This figure shows Top 10 Cyber Security 2014 - 2015

2.6.3 Total ranking 2015

The below table 2.2 shows the ranking of all countries over the world:

Table 2.2 shows Waseda – IAC e-government Total Ranking 2015



No	Total Rankings	Score
1	Singapore	93.80
2	USA	93.58
3	Denmark	91.25
4	UK	90.17
5	Korea	89.39
6	Japan	87.77
7	Australia	86.30
8	Estonia	84.87
9	Canada	81.45
10	Norway	79.63
11	Sweden	77.95
12	Austria	77.26
13	New Zealand	76.66
14	Finland	76.49
15	Germany	76.46
16	France	73.39
17	Chinese Taipei	72.76
18	Belgium	71.69
19	Iceland	69.73
20	Netherlands	69.53
21	Switzerland	69.17
22	Thailand	67.31
23	Israel	65.80
24	HK SAR	65.24
25	Malaysia	64.87
26	Portugal	63.93
27	Czech Republic	63.48
28	Italy	61.30
29	Indonesia	60.11
30	UAE	58.10
31	Poland	57.30
32	Spain	57.12
33	Vietnam	57.03
34	Russia	56.56
35	India	56.42
36	Macau SAR	56.27
37	Chile	53.49
38	Mexico	53.41
39	Romania	53.11
40	Oman	51.60
41	Philippines	51.47
42	Turkey	51.31
43	Brunei	51.06
44	Bahrain	50.50
45	Brazil	50.37
46	Argentina	50.32
47	Colombia	49.36
48	South Africa	49.30
49	China	48.36
50	Kazakhstan	47.73
51	Saudi Arabia	47.48
52	Peru	46.21
53	Tunisia	45.87
54	Venezuela	44.65
55	Uruguay	44.01
56	Morocco	43.13
57	Pakistan	42.94
58	Costa Rica	42.06
59	Georgia	40.73
60	Nigeria	38.37
61	Fiji	37.54
62	Egypt	37.19
63	Kenya	32.91

2.7 E-government security challenges

The increase of the e-services raised a new challenge for governments in the countries that use e-services. The government information will need a strong protection programme in order to avoid any breach which might put at risk the government operation or reveal the citizens' private data. The trust relationship between the e-government authority and the other governmental departments must base on how confident the government departments would feel toward the security programme applied in the e-government infrastructure, the telecom service providers, and the other government departments. One of the main factors to increase the confidence and the trust relationship is to have a high level of security awareness. Being well informed about the security policies, architectures, competencies supporting the security functions and the operational procedures in the government departments will assist in raising the level of confidence and trust. The challenge of achieving the security awareness has been there for a while and since the inception of the e- government programme. Government departments took the responsibility of protecting their e-services but the security programmes implemented in each government department is different and varies from network security to application security levels. Their objectives were to encourage the public to use the government e-services offered through their individual portals or the common portal gateway. These services might be provided directly from the e-government authority or any of its affiliated government departments. “The milieu of citizens, agencies, and commercial corporations around the e-government authority shall raise the security concerns around inter and intra communication” [41], Many researchers presented different models to address the security concerns of the e-government and to measure confidentiality, integrity, and availability known as the C.I.A triad. “Security issues are conceived to comfort the public in using e-government services and government administration and agencies to access, share and exchange information security”, [42]. Information sharing was always considered a concern but need to exist between the governments departments. The requirement of having information sharing between government departments in order to complete an e-service process, for example, sharing the citizen profile, or authenticating an applicant, started to be stronger with the need of having single citizen profile and strong integration in the backend system. Despite the strong need of information sharing and the intensive communication between the government authority and its affiliates, the flow of information between different government departments always raises security concerns [41]. It is an inevitable challenge for the e-government and need to be addressed through the adoption of a security model or a change in the method of information sharing. Moreover, the type of information to be exchanged and the purpose of the information use determine the level of risk the government will need to consider. According to Conklin [41] the level of information sharing between the police department and the water department is different than the police department and the public. The change of information classification is a threat that needs to be addressed by the e-government authority. The process of information sharing is not performed through technology only. The operational procedures, human, policies and decision factors can have positive or negative impact on the process.

2.7.1 The threats impact on the e-government services

Like the e-business model, the government e-services depend on the reliability of the technological infrastructure and its security, the integrated processes and their security checks, and the integrity and skill of the supporting staff. The e-government uses ICT to make the interaction with citizens and businesses easier and seamless with the government. The threats of lacking any of the key elements required to run or launch an e-services hall always be a concern for the e-government. The government e-services have a larger population of users in comparison to e-business e-services which have specific users. The users of government e-services users are the citizens who are the people who live in the country, business corporations, visitors or tourists. Having a larger population will always increase the probability of having malicious attack on the online service. The lack of public confidence caused by the threats on the e-services will be noticed by the low level of use of any e-service offered by the e-government or any of its affiliates. The electronic governance of the e-services is a worldwide topic where many researches were conducted to address how possibly it can be supported. As mentioned by Mitra, “the serious needs of ensuring security on the website vis-à-vis protection of privacy and the prevention of abuse are overwhelming concerns that persuade the use of such models” [43]. It is a clear indication that the need of security has a direct link to the user ate of the e-service. The increase number of threats on authentication, authorization, confidentiality, and non-repudiation of any e-government e-service has negative impact on the proliferation of such service or any associated services [44].

2.7.2 Vulnerability, Security and Trusted Issues

According to Priyambodo, T.K., Prayudi, Y. [45], services provided by e-government to citizens, enterprise, a public officer, government administration and agencies via the Internet and mobile connections are vulnerable to a variety of threats. Meanwhile, [46] argues that vulnerability refers to flaws or weaknesses in system security procedures, design, implementation, and internal controls that could be exploited by threat-sources. Once exploited, it could result in a security breach, consequently causing harm to e-government information assets and services. The assets must be protected to ensure secure e-government include client computers, the messages traveling on the communication channel, and the Web and e-government servers—including any hardware attached to the servers.

In any system, including the system of e-government, it is known there are four main regions of threat in any given system: programs, peripherals, communications, input and output. According to Teo, T.S.H., Srivastava, S.C., Jiang, L. [47], there are many factors that trigger the occurrence of vulnerability. Among those factors are Technical and Technology, Human, Social, Political factors of the Countries, Economic, and Networking.

According to Moen, V., Klingsheim, N., Inge, K., Simonsen, F., Hole, K.J. [48], e-commerce is one example of the application of a good security system. However, the use of The Public Key Infrastructure (PKI) that is applies to e-commerce is not fully applicable within the scope of e-government without a thorough analysis of what the new trust model should be. The trust calculation for commerce is based on monetary issues, while government solutions involve important infrastructure, society, and privacy issues. Trust is part of humanity and social interaction. There are a lot of principles and definitions of trust. In this case [49] has made a list of definitions of trust from a number of sources. While according to Alsaghier, H., Ford, M. [50], trust is defined as an individual's belie for expectation that another party (e-government) will perform a particular action important to trust or in the absence of trustor's control over trustee's performance. Furthermore, Santos [51], adds that the solutions to improve trust is through two aspects, namely:

- Enforcing the security properties required by the users, that is to provide protection against data users, as well as security of the computing platforms used.
- Giving users guarantees that the desired security properties are being enforced.

Considering users are not directly involved in the control process of security and do not know how power computing platforms are used, the users need to be given guarantees that the infrastructure being run is completely safe. In this case, the guarantees that can be given are through trusted computing hardware and trusted certifier that is offline. Meanwhile according to Burmester, M., Mulholland, J. [52], a system is categorized as a trust if it meets three criteria, namely:

- Protected capabilities, the presence of a set of orders having exclusive permission to access a specific location where sensitive data are stored or a location where a particular activity can be run.
- Integrity measurement, the existence of metrics from the platform characteristics that contain things affecting the integrity of the platform.
- Integrity reporting serves as informing the specific storage location of integrity measurements as well as providing a legal authentication from the stored value based on trusted platform identities.

Trust in the government agency has a strong impact on the adoption of a technology. Colesca [49] reveals that a high level of trust in the government's ability, motivation and commitment to the e-government programs coupled with a high level of trust on enabling technologies leads to a synergy between the government and citizens. In addition, [47] mention that in an e-government system, trusting believes an e-government website will act responsibly when a citizen visitor transacts with it. The existence of threat and vulnerability especially malware would be a factor that can eliminate trust from the system.

2.7.3 Security and Trust Standard

Standard is the highest level of policy that shows transparency to the public that all the processes carried out in an institution have been in accordance with the provisions. Security standard features a high-level concept. According to Wada, K., King, P. [53], ideally every institution has a policy as the guideline to communicate their goal that contains a set of basic principles to be a reference for technical and operational levels. Policy will provide an overview of culture and value built into the institution. Although policy is solely a guideline, given the development of a more advanced technology as well as feedback from the operational experiences and practices on a daily basis, the policy must also be responsive to follow such developments. Security and trust standard that can be applied in e-government is using the approach of Information Security Governance, that is governance of organizations/institutions that provides a guiding strategy, ensures that the goal of the company is attained, manages risk, utilizes resources of the organization responsibly, and oversees the success or failure of security programs.

2.7.4 Security Policy, Model and Trust System

A secure environment is strongly influenced by the application of security policy, security model as well as trust management system.

- Security Policy. According to Gikas, C. [54], security policy is a statement that clearly specifies what should and what should not be in the field of security. In the lower level, security policy will contain a set of policies regarding authorization and secure states. In general, security policy is a set of statements and requirements of system behavior that will ensure the realization of a secure system. Meanwhile, [55] stated that in the coverage of law enforcement, security policy must also include policies about confidentiality of classified data. In this case, all classified data/information should be protected and only users with a certain level who have the right to access such data and information. In addition, there must be rules and obligations that bind users who utilize the classified data.

- Security Model is an abstraction that provides a conceptual language that will be used by the administrator to implement the security policy. Security model will define the hierarchy of access or modification of rights that can be owned by users from the institution.
- Trust Management System is a framework to determine whether the security policy expressed through logic and abstraction as well as implemented through programming or system setting has completely complied with the policy that should be followed. Trust management system is applied to policy language and compliance checker.

According to Sandhu, R. [56], for a simple environment, the use of several security models are adequate. For future development, [56] predicts that a security model will be increasingly complex, and the approaches that can be done as solutions are Application-Centric Access Control Models and Technology-Centric Access Control Models. Even according to Al Nagi, E., &Hamdan, M. [6], additionally the issue security and convenience will be more balanced, one of which is through applying the concept of a context-aware authentication.

2.8 Offered information security models and theories

Many journals and literature were reviewed to analyse the existing models and theories developed to evaluate the information security level in an organisation or between group of organisations interacting with each other through information sharing or transactional services. The focus was on the models and theories researchers and scientists came up with or adopted in developing security systems, or models. Reviewing the objectives of these models was also part of the literature review process of this research. The scope and the objective of the research were clear from the initial stage of the literature review. Journals addressing information security models, theories of systems and enterprises protection, human behavioral theories and the cybercrimes, decision factors in the information security, and security frameworks and standards were reviewed, analyzed, and categorized based on the area of the research they address. The review process focused on finding supporting arguments for the need of a new model. The strengths of the existing models were considered as good characteristics to have in the new model and the weaknesses been the supporting factors to justify the existence of some of the layer sand shape the structure during the development process. Some of the journals and proceeding articles were reviewed to get strong academic support on some of the views related to e-government or organisations' information security. The criteria of selection were based on the strength of the argument the journals was presenting, the popularity of the publisher in the information security field, and the clarity of the concept to reader. The CIA triad; confidentiality, integrity, and availability, are the concepts which act as the fundamental security objectives for data, information, and computing services [58].

2.8.1 Multilevel and multilateral models

Multilevel models were developed to protect the confidentiality and the integrity of information. These models look at the nature of information flow between entities and how security of the flow could be governed by rules. There are four models address the multilevel security:

A) Nondeducibility Model.

B) Non Interference Model.

C) Bell-Lapadula Model (Confidentiality Model)

D) Biba (Integrity Model)

2.8.1.1 Non-deducibility model

The Sutherland's non deducibility model developed in 1986. The model explicitly explains that information can flow from high-level objects to low-level objects if and only if some possible assignment of values to low-level objects in the state is inconsistent or conflicting with a possible assignment of values to the state's high level objects [59], see figure 2.8.

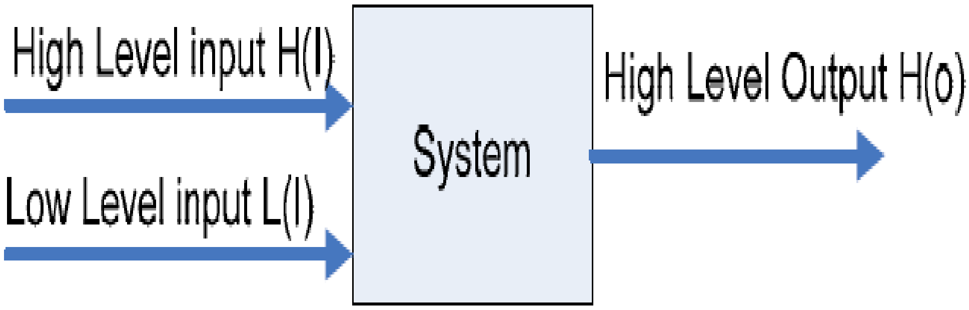


Figure 2.8: This figure shows High and low level inputs/non deducibility

The model can be expressed mathematically as the following:

Assignments H & L H for high level objects

L for low level objects

No flow of information from high (H) to low (L) unless

$P(H)>0 \;\&\; P(L)>0 \longrightarrow P(H|L)>0$

The non-deducibility model has been observed with a weakness as it is considered as a model for information sharing not information flow. As per the security definition of objects bidirectional. The non-deducibility model fails this definition and therefore, it was categorized as a good model for data compartmentation rather an information sharing.

The flow of information security can be presented in the following mathematical representation using Bayes' Theorem with the condition as follow:

$P(H|L)\,P(L) = P(L|H)\,P(H)$ condition (1)

It follows that:

$P(H)>0 \;\&\; P(L)>0 \longrightarrow P(H|L)>0$ if and only if $P(H)>0 \& P(L)>0 \longrightarrow P(L|H)>0$

Knowing that $P(H|L) = (P(H|L)P(H))/P(L)$ & $P(L|H) = (P(L|H)P(L))/P(H)$

Replacing P (H|L) and P (L|H) values, the author found that the above condition holds:

$((P(L|H)\,P(H))/P(L))P(L) = ((P(H|L)\,(PL))/P(H))\,P(H)$ this will lead $P(L|H)\,P(H) = P(H|L)\,P(L)$ which holding condition (1)

The mathematical expression represents the need of information flow to be bidirectional.

The bidirectional concept of information flow is maintained by limiting the objects when the system is secure with non-deducibility model.

If $P(H)>0 \;\&\; P(L)>0 \longrightarrow P(H|L)>0$ where H is the assignment sequence to the system's high level input port & L is an assignment sequence to system's low-level input and output.

Most of system's high level output can only be generated from low level input see figure 2.9.

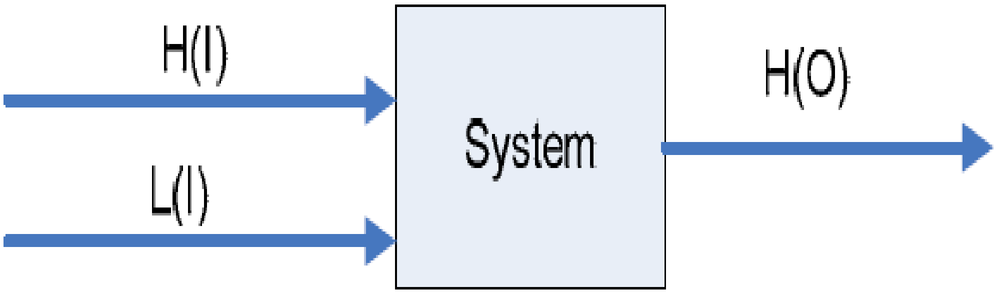


Figure 2.9: This figure shows high level output from low level input

Researchers and analysts think that non-deducibility is weak since there is nothing to stop low making deduction about high level input with 99% certainty.

2.8.1.2 Non-interference model

The non-interference model was developed by Goguen and Mesguer in 1982 [60]. The concept of the model is that high actions have no effect on what low can see. “A system is non-interfering if its low-level output was independent of its high-level input in the sense that for any system with output function out (U, I), value is the output generated by input history I to user U, out (U, I) = out (U, I*), where I* is I purged of all inputs from users with security levels > U’s” [59]. This is another model which is related to policies within a system which can represent as anode for the e-services.

2.8.1.3 Bell-Lapadula model

Bell-Lapadula or BLP is the most well-known model to address confidentiality of information. It was developed in 1973 by Bell and Lapadula and became a prominent model for the Mandatory Access Control (MAC) and a true implementation of themultilevel security policy concept [61]. The model is considered as a multilevel security model. The model was implemented in many systems which became known as multilevel secure systems [62].

The Bell-Lapadula model has two main properties [62]:

1) The property which sets the policy of the read control in the system. The rule of this property that a lower level object can’t read a higher level object or what’s known as No Read Up (NRU). This property blocks exposure of secured data handled by objects with high level of security.

2) The *property (Star property) which blocks objects with higher security level to write data to objects with lower security level.

In the BLP model, access to the system is classified as: A) The Mandatory Access Control (MAC) which is applied when the system enforces a security policy independently of users' actions. B) The Discretionary Access Control (DAC) which is applied when users can take their own access decision about their files**.**

Being the most popular model in data security, a lot of criticisms from researchers in the security field have posted critiques on the BLP model pointing out loop holes. The scientific argument raised by Mclean illustrated that BLP model rules were not in themselves sufficient to provide security. As supporting evidence Mc Lean introduced a system called systems "Z"[63] with BLP rules and policies embedded.

The system allowed the user to request the system admin to declassify any file from high to high file without breaking the BLP assumptions. The counter academic argument by Lapadula was based on the fact that the breach of security was due to changing labels which is not a valid operation in the BLP core model and any system which applies it. McLean's debate was based on his analysis on the BLP model and findings which indicated that checking the validation of any system operation is not part of the scope. The scientific argument led to an introduction to the tranquillity property; a property which defines two states of security; strong and weak. The strong security state has security labels that never change during the system operation. The weak security state has security labels that never change in such a way as to violate a defined security policy.

2.8.1.4 The Biba model

The Biba model or as known "Bell-Lapadula upside down" was developed by Ken Biba. The model addresses the integrity aspects only and does not address the other two aspects of C.I.A (confidentiality, Integrity, Availability) triad. The basic elements of the Biba have a similar structure as the BLP model [58], The Biba model addresses the Low Water Mark Principle which technically means that the integrity of an object is the lowest level of all the objects that contributed to its creation [62]. The low water mark concept was implemented in the industry as part of a system called LOMAC operating system; an extension to Linux Operating System [64]. The operation of LOMAC OS reflected the embedding of the low watermark.

The way LOMAC OS was applying the water mark concept is by classifying the file systems into network and system files. The operating system has network files and system files. The network and system files have different levels of security. The system files are set with the highest security level and always protected against low security levels objects. The security level of the file system gets downgraded to low integrity if an access from an object is required. The downgraded file will not be able to open or write to a system file. A system file can be a password file for instance [62].

2.8.2 Multilateral security

These set of models were developed in the field of the information security following a multilateral concept.

2.8.2.1 Compartmentation and lattice model

“The compartmentation model is used by the intelligence community. The term compartmented security is used in the U.S as a common terminology for the Multilateral security as it is called in England and the rest of the world”, [62]. A good compartmentation based model is the lattice model which is a variant of BLP. The Lattice model is a mathematical structure in which any two objects A&B can have dominance relation A>B or B>A. The model is defined by a tuple with five components (SS, OS, CS, *, →) where SS stands for set of subjects causing the information flow, OS stands for the set of objects capable of storing information, CS stands for set of security classes,

* is the combining operator and → is the flow relation (the legal flow) [69]. The relation between the different classifications and how a person can have an access to a certain classification but not to another is illustrated in see figure 2.10.

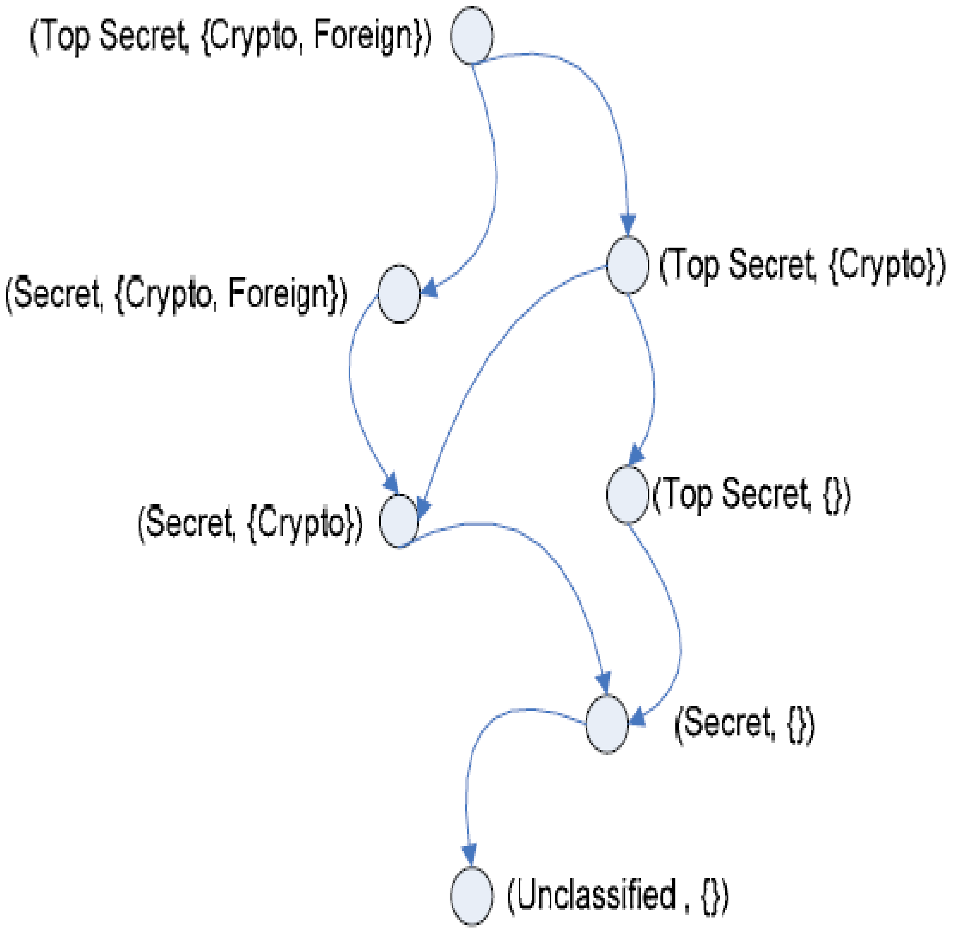


Figure 2.10: This figure shows Lattice labels

2.8.2.2 The Chinese wall

The Chinese wall model was developed by Brewer and Nash [65] to prevent any conflict of interest with an organisation or between an organisation and its clients. The model is shown below:

mathematically expressed as

Let C= client

Y(C) = C’s company

X(C) = C’s competitor

The Chinese wall model has two main properties which act as the main two rules of the model. Both properties have a mathematical representation as illustrated below:

1. The simple security property

"A subject s has access to C if and only if, for all C's that s can read, either Y(C) ¢ X (C') or Y(C) = Y (C')", [62].

2. The *property

"A subject s can write to C only if s can't read any C' with X (C') ≠ 0 & Y(C) = Y (C')" [62].

2.8.2.3 The British medical association (BMA)

The BMA is a model developed to describe the medical information flow while the medical ethics and standards [62]. The model assists the medical institutions to exchange information among them while maintaining the privacy of the patients' records. The content of using technology as a method of transferring patients' records and data securely was raised by many countries and medical organisations.

The BMA represents doctors in all branches of medicine all over the UK. The BMA is a voluntary association with over two-thirds of practicing UK doctors in membership and an independent trade union dedicated to protecting individual members and the collective interests of doctors.

The BMA also promotes the medical and allied sciences, seeks to maintain the honour and interests of the medical professions and promotes the achievements of high quality healthcare. The BMA policies cover public health issues, medical ethics, science, the state of the NHS, medical education and doctors' contracts. Policies are also decided by elected members, mainly practicing doctors and supported by a professional staff who work with other bodies to meet its objectives [68].

2.9 Application of secure systems (Multilevel)

Many products in the industry applied the multilevel security model. The purpose of studying these products was to indicate the possibility of building products (military use or commercial) which can reflect policies and models.

2.9.1 Secure Communications Processor (SCOMP)

SCOMP was one of the earliest products developed to reflect the multilevel concept and policies. The project was a collaboration between Honeywell and the US department of defense (DoD) [66].

The product has four rings of protection and the Operating System is using these rings to maintain up to 32 separate components and to allow one way information flows between them. The security kernel was kept to minimum in order to allow the computer to perform the day to day business operation. This product was used in the military applications such as Mail Guards which is a special firewall that allows mail to pass from low to high but not vice-versa (what's known as data diode). SCOMP was the only machine rated as A1in1984 which is the highest security rate a computer system can obtain. The kernel was represented in mathematical values in order to get the rating.

2.9.2 Blacker

"Blacker is an example for an encryption device designed to incorporate multi-level security (MLS) technology", [62]. The idea of blacker is to separate the encryption processors from the clear text processor by assigning colour codes. The enciphering processor (Encryption processor) has a colour of black while the clear text one has a colour of red. The device was rated as the highest in security rating. It was givenA1as the only communication security device with A1 evaluation. Motorola had tried to produce the second series or a successor but was not able to obtain the same rate. A rate of B2 was given to the new box.

2.9.3 Naval Research Laboratory (NRL) pump

The NRL Pump was developed by the Naval Research Laboratory. NRL Pump is one-way data transfer device (data diode) using buffering, while limiting the bandwidth of

Possible backward leakage by number of mechanisms such as timing randomization of acknowledgement messages. The way the pump works was described in an algorithm format by Lanotte and Tini[67]. The operation of the pump can be summarized as follows:

- A low agent sends a message to some high agent through the pump.
- The pump stores the message in a buffer and sends an acknowledgement to the low agent.
- The low agent can't send any new message until the acknowledgement of the previous message is received.
- The pump stores the message until the high agent is able to receive it.
- The high agent receives the message and then sends an acknowledgement to the pump.
- The high agent does not acknowledge some received message before a fixed timeout expires. The pump stops the communication.

The following algorithm represents the operation [67]:

LS: represents the low system

P: represents the pump

HS: represents the high system

A → B: msg represents the message msg sent from A to B

Ls→ P: reqL: the low system requests to the pump to start a communication with a high system.

P → LS: valid L: the pump checks if the low system is a valid process and, then it acknowledges its request.

P→ HS: reqH: the pump requests to the high system to start a communication with the low system.

HSP→ : valid H: the high system checks if the pump is a valid process, and then itacknowledges its request.

P→HS: grant H: the pump communicates to the high system that the communication can start.

PLS:→ grant L: the pump communicates to the low system that the communication can start.

The NRL pump is an implementation of a data transfer methodology based on an algorithm. The algorithm sets the rules on how a system can communicate or transfer data to another. It was found to be a strong mechanism for transferring data or exchanging information but yet has no comprehensive analysis on the other factors which might affect the security programme between two different organisations. Although the algorithm can be placed and enforced on systems designated for intra organisations communication, the policies on these systems and the competencies responsible for supporting these systems will have a direct impact.

2.10 E-government architecture framework

One of two types of architecture can be adopted by e-government systems: Centralized and De-Centralized. Centralized architecture standardizes the IT services across the government departments. It provides the services that span across various departments with a centralized resource allocation mechanism. Centralized model helps greater integration across various departments and the E-Governance Portal. De-centralized architecture is preferred when government agencies conduct separate implementations of different business processes across individual departments [70].

2.10.1 E-government portal

The diversity of e-government applications and functions can be presented to users through various types of websites and portals organized within a whole-of-government architecture and applying the principles of no-wrong-door and content easily discovered on basis of user requirements, rather than government structures and integrated channel management. That portals, sometimes called “gateways”, aggregate and organize content and services, often with links to websites of individual ministries or programs. The goal of a portal is to efficiently guide users to the information and services they seek. National web portals can represent the face of a country to the world and the face of government to the citizenry [71]. The benefits of a Portal are immense. Portals act as a one stop resource for information. Having a secure e-government portal will reduce the costs for the government in delivering timely information to its citizens [4]. E-Governance Portal is built based on Service Oriented Architecture (SOA). Service Oriented Architecture (SOA) may be defined as a group of services that communicate with each other through data-passing or two or more services coordinating some activity [70].

2.10.2 Identity management in e-government systems

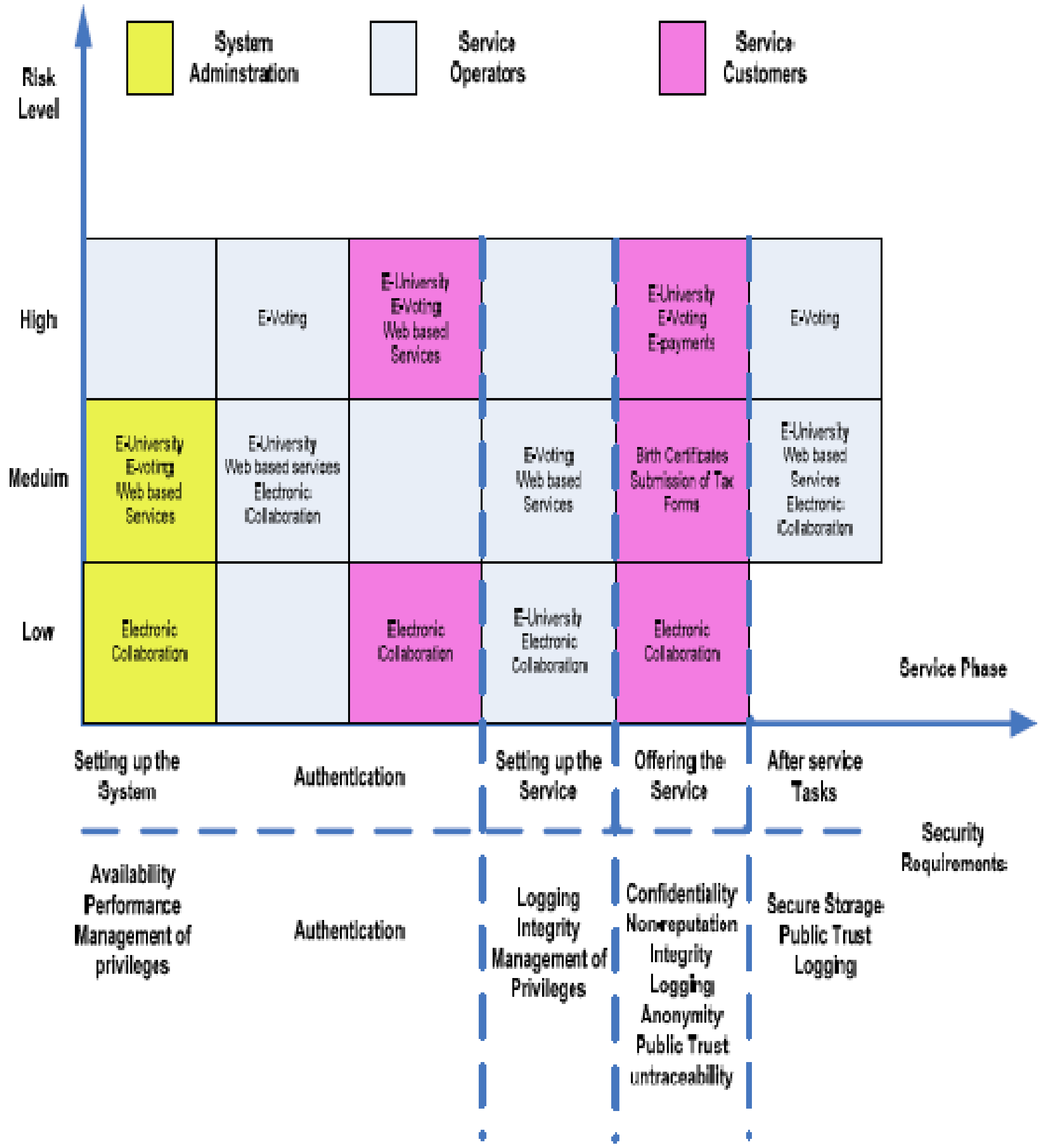
E-governments over the world need to develop digital identity management systems to provide services such as user identification, authentication, and authorization in an e-government environment. A digital identity management system is based on a schema for representing digital identities (a database subset, for example, that includes name, last name, date of birth, photo, certificate, serial number, etc.) and authentication mechanisms and protocols that entities use to demonstrate they are the owners of a given digital identity. Accordingly, the purpose of a digital identity is to tie a particular transaction or a set of data in an information system to an identifiable individual. With the help of a digital identity, a user can be identified and authorized to use a given resource or service [72]. Identities and identity management are of primary importance for governments as they encompass the identification of citizens and their interactions with public services and government. Trusted, secure and accountable identity management solutions are key e-government enablers [72]. Federated identity management plays a key role in this phase. Federated identity management (FIM) refers to an infrastructure that consists of technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. FIM enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Use of FIM can increase security, lower risks, and reduce cost by eliminating the need to deploy multiple identity management systems. It can also drastically improve the end-user experience by eliminating the need for account registration through automatic "federated provisioning", i.e. authenticate the user once and use the same identity information across multiple systems (also referred to as single sign-on) [72].

2.10.3 Lambrinoudakis security framework

There is no doubt that most of the government e-services are supported by solid technology infrastructure.

The Lambrinoudakis security framework was developed to identify and organize the security requirements for the information systems supporting the e-services offered by the e-government [73], (See figure 2.11). A risk analysis was conducted on the e-University which represents a suite of services and allows remote accessibility. Lambrinoudakis divided the cycle of the e-University service launch into 5 steps (setting up the supporting system, authentication, setting up the service, offering the service, and after service task).

The framework did not address the human aspects of the cycle, skills requirements, and the need of the enforcement of the security policy throughout the cycle. It only addressed the operational and management aspects such as logging and storage. The skills of security staff must be equivalent if not better than the attackers' capabilities and the policies must be developed to block internal and external threats. Ignoring these two key security aspects was found as a weakness in Lambrinoudakis framework.


Risk Level
System Adminstration
Service Operators
Service Customers
High
Meduim
Low
E-Voting
E-University E-Voting Web based Services
E-University E-Voting E-payments
E-Voting
E-University E-voting Web based Services
E-University Web based services Electronic Collaboration
E-Voting Web based Services
Birth Certificates Submission of Tax Forms
E-University Web based Services Electronic Collaboration
Electronic Collaboration
Electronic Collaboration
E-University Electronic Collaboration
Electronic Collaboration
Service Phase
Setting up the System
Authentication
Setting up the Service
Offering the Service
After service Tasks
Security Requirements
Availability Performance Management of privileges
Authentication
Logging Integrity Management of Privileges
Confidentiality Non-reputation Integrity Logging Anonymity Public Trust untraceability
Secure Storage Public Trust Logging

(Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G., 2003)

Figure 2.11: This figure shows the Lambrinoudakis Model

2.10.4 The analysis of networked systems security risks (ANSSR)

The Analysis of Networked Systems Security Risks (ANSSR) identified 5 types of deliberate attackers types:

- Users (including trusted users)
- Developers
- Maintainers
- Customers

- Outsiders

The (ANSSR) model follows the approach of analyzing threats from one source, the attackers. For this reason the model is week [74]. The (ANSSR) was effective but it doesn’t cover all aspects of the threats analysis, as the likelihood of initiation is only linked to attackers only.

2.10.5 Models for checking internet commerce

Many models were developed for enforcing checks for the Internet Commerce. Some of them were concentrating on equipment which will perform checks related to scheduling with fixed regular time period. Keller addressed the issue of optimal checking schedules using calculus of variation methods [76]. Different controls for monitoring the Internet were developed by many researchers. A mathematical model was developed by JV Hansen [75] for optimization and artificial intelligence methods for scheduling the monitoring of related controls of the Internet Commerce (IC).

The optimization model has the following key elements and assumptions:

1. Controls are to be checked at a fixed time interval t.
2. Number of controls remains constant and immediately after a control check, the cost of control failure (CCF) is L0.
3. The cost of monitoring is constant M.
4. The cost of control failure increases at a fixed rate r.
5. After a time t since last check, the CCF is L0+rt.

The control system is in existence for a total time T and the number of checking intervals is N=T/t, therefore; cost (total) (CT) over time is the sum of CCF and the cost of checking. The objective is to minimize C (T).

2.10.6 Heeks design-reality gap model

Heeks [27] built his model on the assumption that success and failure of e-government depends on the gap existing between the current situation (*reality*) and the (*design*) for e-government in the future. Heeks proposed seven dimensions in order to understand the design-reality gap, abbreviated in the acronym (ITPOSMO) Figure 2.12. Following is a brief description of the seven dimensions:

I*nformation:* the formal information held by the digital system and involves: data stores, data flows and data management. The informal information held by the people using the system.

T*echnology:* the components of digital IT.

P*rocesses:* the activities undertaken by stakeholders involving information-related processes and broader business processes. **O***bjectives and values***:** the key dimensions, through which factors such as culture and politics are made manifest.

S*taffing and skills:* both the quantitative and qualitative aspects of competencies including staff and other users.

M*anagement systems and structures:* the overall management systems and structures established to organize e-government system operations.

O*ther resources:* the required time and money to implement e-government.

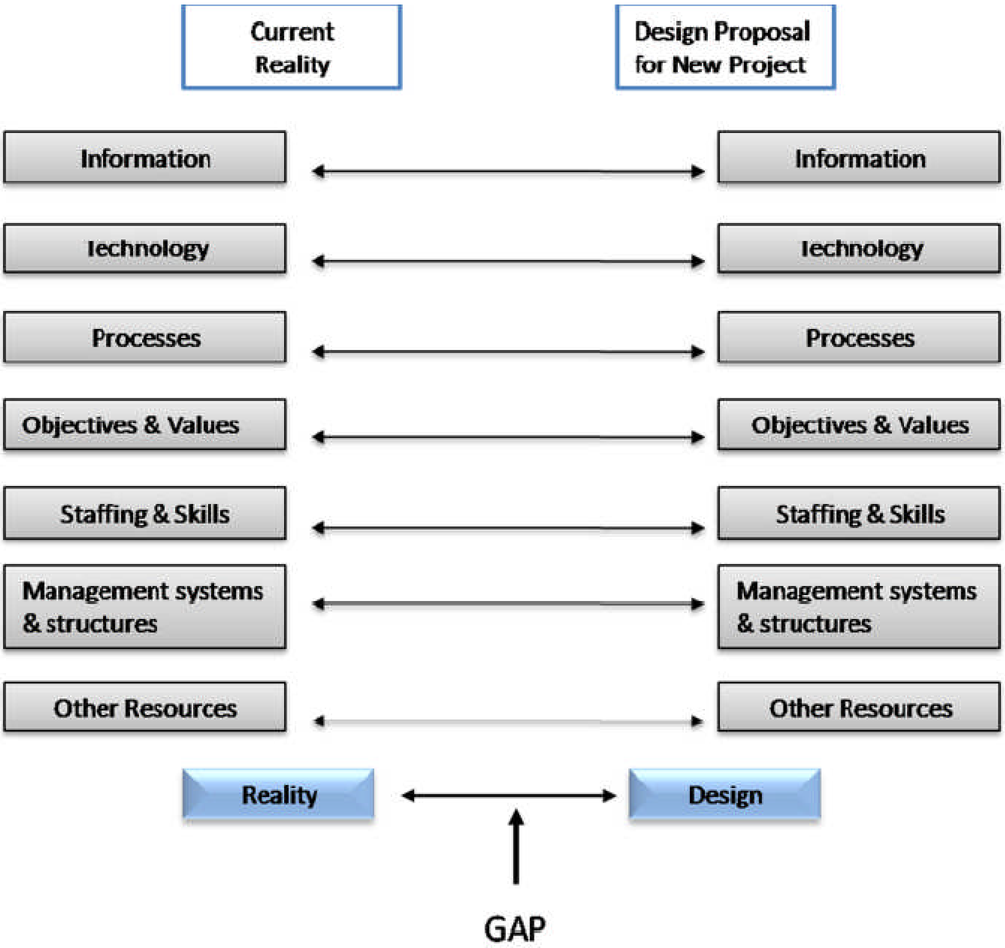


Figure 2.12: This figure shows design-reality gap in e-government projects Adopted, (Heeks, 2003)

2.10.7 Ebrahim and Irani e-government framework

Ebrahim and Irani [78], proposed a strategic e-government framework and five dimensions as barriers to e-government. Ebrahim and Irani believe that benefits and barriers associated with e-government should be considered as factors that influence the implementation process. See table 2.3.

Table 2.3: Dimensions of e-government adoption

Dimension	Examples
IT infrastructure	• Complex systems • Lack of reliable networks and low capacity • Lack of government systems integration • Lack of documentation
Security & privacy	• Threats from hackers or viruses • Absence of privacy of personal data • High cost of security applications • Unauthorised access to systems • Lack of security rules, policies and privacy laws • Lack of risk management security program
IT skills	• Lack of IT training • Lack of skilled and specialist IT staff in market • Lack of employees with integration skills • Unqualified project manager Shortage of
Organisational	• Lack of coordination and cooperation between departments • Unclear vision and management strategy Complex of • business processes • Politics and political impact
Operational cost	• Cultural issues • business process • Resistance to change

	• Time consuming for reengineering • Limited financial recourses • High cost of IT professionals and consultancies • High cost of IT in developing countries

2.10.8 Bakry STOPE model

Bakry [79] introduced the **STOPE** model, Figure 2.13, to provide a base for the development of an international standard policy concerned with e-readiness assessment. The framework follows a comprehensive approach and identifies five dimensions (strategy, technology, organisation, people and environment). The STOPE model can be useful in decision making at different stages. Countries and organisations need to consider these dimensions if they are willing to integrate with the networked world or are planning to achieve sustainable development. Each of the five dimensions integrates factors related to:

S*trategy:* the strategy of the country with regards to the future directions, commitments and plans toward ICT development and utilization.

T*echnology:* the technology concerns with ICT facilities, infrastructure, support, and ICT strategy.

O*rganizations:* the organizations management, regulation, and cooperation.

P*eople:* people’s ICT skills, training, education, and awareness.

E*nvironment:* the environment surrounding the economy, resources, general regulations and environment.

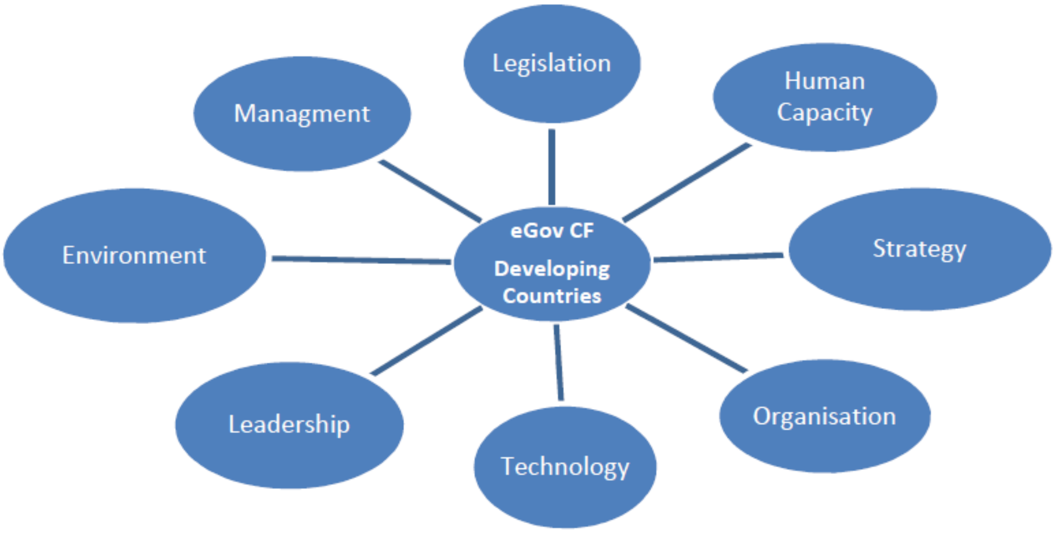


Figure 2.13: This figure shows e-government critical factors

2.10.9 Model for e-government security

The framework document is a high-level expression of security requirements and expands upon the security statements in the e-government strategy ["e-citizen e-business e-government"]. It also sets out the process for determining the security requirements and assuring the presence and proper operation of the security countermeasures put in place to meet the security requirements. Other related and more detailed security requirements and process statements address specific topic areas. Figure 2.14 below depicts the relationships [87].

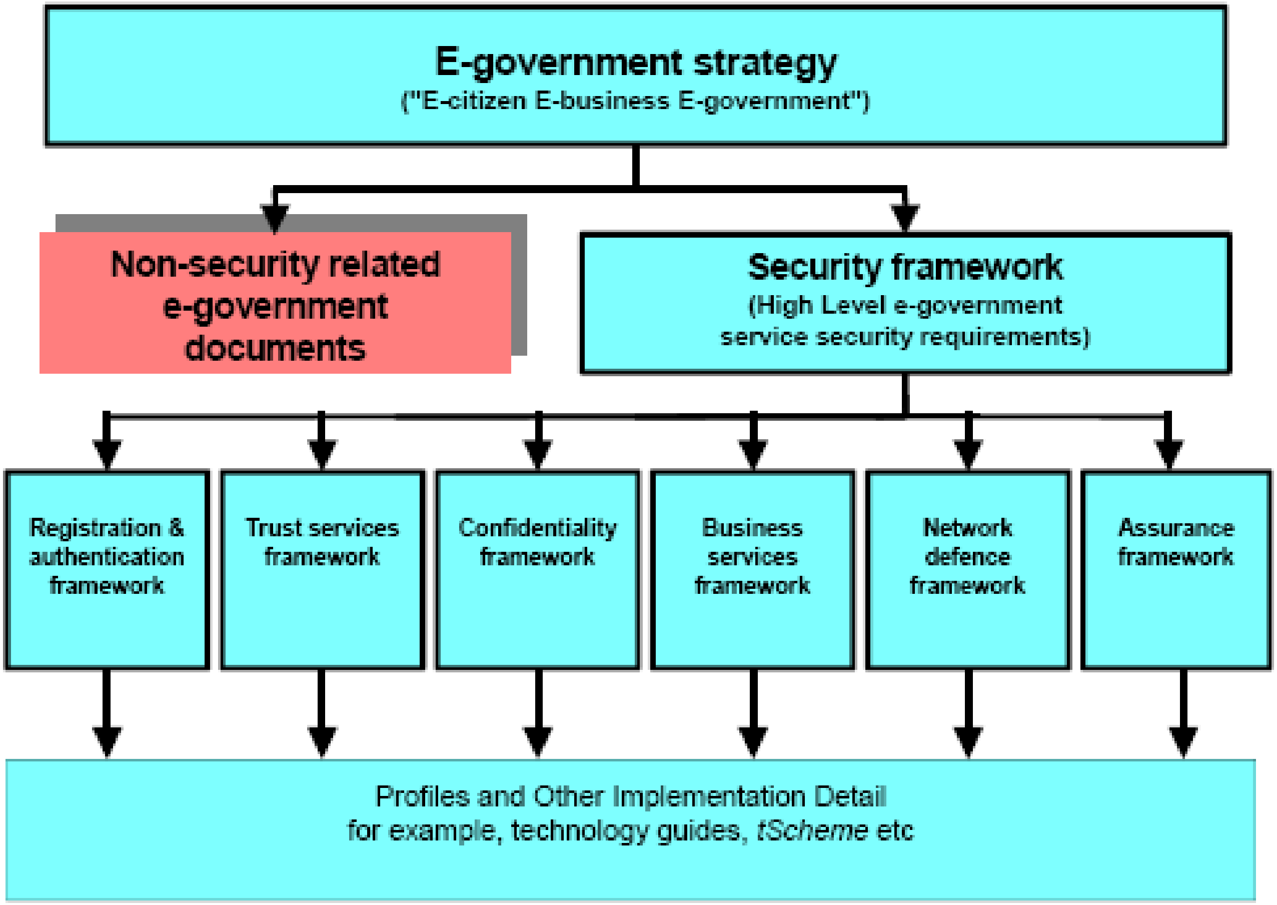

E-government strategy
("E-citizen E-business E-government")
Non-security related e-government documents
Security framework
(High Level e-government service security requirements)
Registration & authentication framework
Trust services framework
Confidentiality framework
Business services framework
Network defence framework
Assurance framework
Profiles and Other Implementation Detail
for example, technology guides, *tScheme* etc

Figure 2.14: This figure shows security frame work [Office of the e-Envoy]

This high level security framework is supported by more detailed framework statements for the specific topic areas below:

a. The registration and authentication framework covers the security services required to ensure that all users are uniquely and unambiguously identified and granted access only within the authorizations made. All systems security ultimately rests upon the capability to identify and appropriately authenticate and enforce clients and all other users' privileges in respect of the system assets.

b. The trust services framework covers the security services required to ensure that transactions are properly traceable and accountable to authenticated clients or other users and cannot subsequently be disavowed.

c. The confidentiality framework covers the security services required to ensure that information is stored securely and not disclosed to persons or processes unauthorized to see it.

d. The business services framework covers the security services required to ensure that the e- Government service applications themselves are designed, developed, configured and operated in a secure and robust manner and their information assetsproperly protected. This includes disaster recovery and business continuity.

e. The network defense framework covers the security services required to ensure that the plant, stored data and other assets of the e-government service are properly protected against malicious or inadvertent electronic attack.

f. The assurance framework addresses the means by which trust in the implementation of security elements can be assured.

2.10.10 EGIT Framework

The Electronic Government Information Technology Framework (EGIT) provides a standard reference point for addressing various basic information technologies.[88] See Figure 2.15.

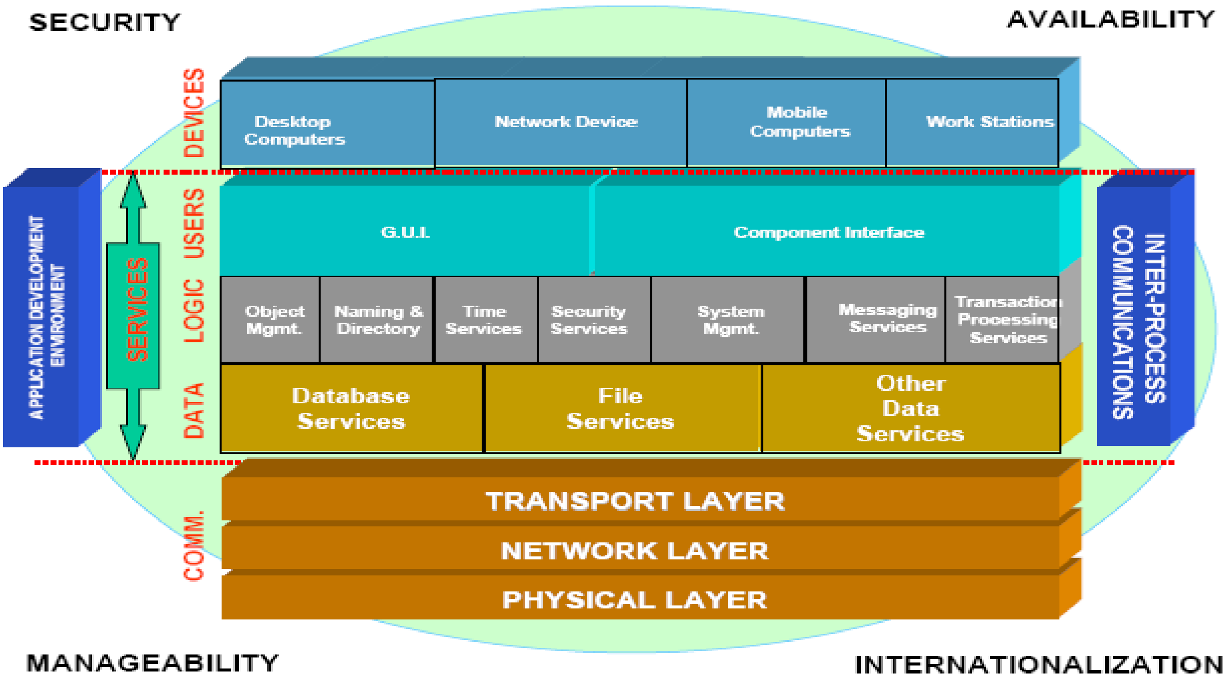


Figure 2.15: This figure illustrates EGIT framework

This Framework has five major areas:

·Devices

·User Services

·Logic Services

·Data Services

·Communication

The Inter Process Communications provide the communication vehicle among the User, Logic and Data Services layers, while the Application Development Environment creates an overall application development platform for the EGIT Framework.

Each layer is divided into components. EGIT definitions focus on the interface for requesting to and receiving services from each component.

Qualities that are applicable to all layers and components are:

- Security
- Availability
- Manageability
- Internationalization

2.10.11 Integrated security system (ISS)

This is an integrated security system of various individual security systems, which are often used as separate systems. The components of this system include a registration system, a certification system, a smart cards system, and an authorization system as shown in figure 2.16. This system is supported by a security platform which has different security mechanisms, which can be updated or changed whenever necessary. The main functions of this system are to provide identification of users, users' authentication, non-repudiation, confidentiality, delegation, information integrity and authorization. Authentication is provided through public key certificates. Authorization and delegation are provided using attribute certificates. An attribute certificate is a certificate that carries authorization and delegation information. It contains a reference to the authentication tokens for validation purposes. Non-repudiation is provided using smart card systems and signature schemes. Users in need of registration services, a smart card, a public key certificate, and authorization attributes usually identify themselves multiple times and perform registration procedure at four different administration stations in non- integrated security systems. In this system identification of users, verification of users' identities and registration of users is done once per user and all relevant security data are shared among the four security sub-systems. The same administrator registers the client, issues a digital certificate, issues an attribute certificate and a smart card to the client. The administrator can visualize all the data and can perform updates and other management operations from the same interface. The system offers functional integration of data and security administration procedures and also visual integration through a common security administration interface [89].

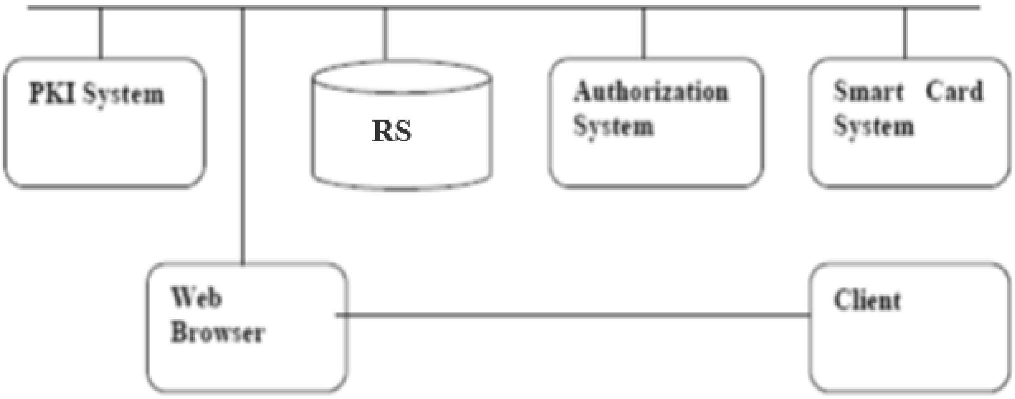
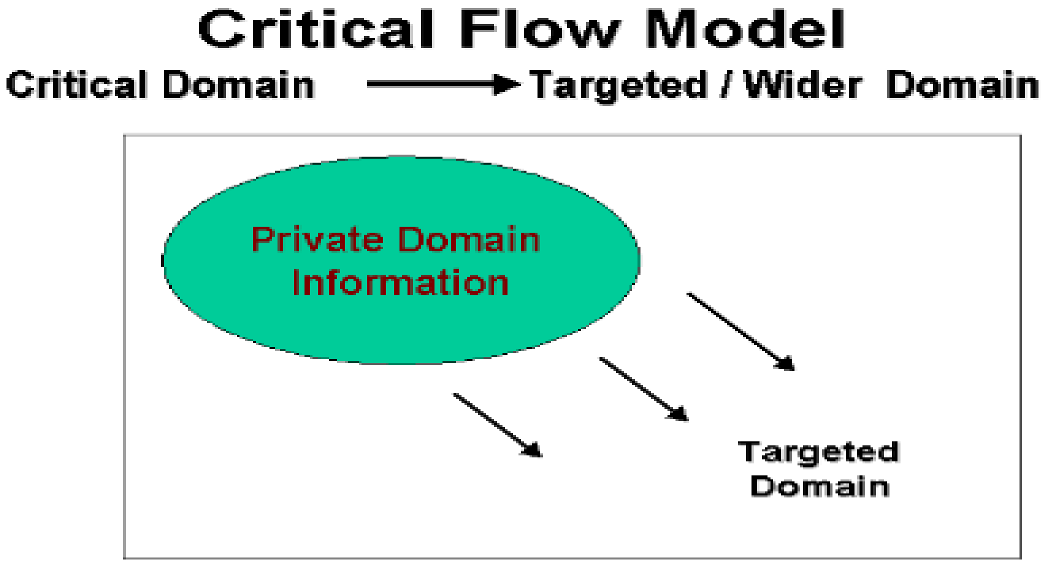


Figure 2.16: This figure illustrates the architecture of ISS

2.10.12 Critical Flow Model

The model is based on broadcasting information of 'critical' value (which by its very nature will not be disclosed by those involved with bad governance practices) to targeted audience using ICTs and other tools. Targeted audience may include media, affected parties, opposition parties, judicial bench, independent investigators or the general public. Those who would divulge such information could include upright officials and workers, whistleblowers, affected parties and those who were themselves involved in bad governance practices but have now changed their minds or may wish to trade such information for lenient punishments [90]. See figure 2.17.



Critical Flow Model
Critical Domain → Targeted / Wider Domain
Private Domain Information
Targeted Domain

Figure 2.17: This figure shows the Critical Flow Model

The use of this model requires a foresight of:

- Understanding the "critical and use value" of a particular information set
- How or from where this information could be obtained
- How could the information be used strategically
- Who are the best target group for such information- the users for whom the availability of this information will make a huge difference

This model could be applied in the following possible ways:

- Making available corruption related data about a particular Ministry / Division/ Officials online to its electoral constituency or to the concerned regulatory body.
- Making available Research studies, Enquiry reports, Impact studies commissioned by the Government or Independent commissions to the affected parties.
- Making Human Rights Violations cases violations freely available to Judiciary, NGOs and concerned citizens.
- Making available information that is usually suppressed, for instance, Environmental Information on radioactivity spills, effluents discharge, information on green ratings of the company to concerned community.

This model may not work in cases where the governance mechanism does not allow public debates and opinions, and censures all information of critical nature.

2.10.13 Comparative Analysis Model

Comparative Knowledge Model is one of the least-used but a highly significant model for developing country which is now gradually gaining acceptance. The model can be used for empowering people by matching cases of bad governance with those of good governance, and then analyzing the different aspects of bad governance and its impact on the people [91].

2.10.14 E-Advocacy/ Lobbying and Pressure Group Model

E-Advocacy / Mobilization and Lobbying Model is one of the most frequently used Digital Governance model and has often come to the aid of the global civil society to impact on global decision-making processes. The strength of this model is in its diversity of the virtual community, and the ideas, expertise and resources accumulated through this virtual form of networking [92].

2.11 Electronic governance model

There are four dimensions of the e- Governance model as follows:

LEVEL: Level describes on the one hand the area (local, national, trans-national) in which State transformation is taking place. On the other hand, Level describes the extent to which State transformation is taking place: e.g. are there only procedural changes or do the implemented e- Governance measures reengineer the organization as a whole.

ACTOR: On each level, actors built up their areas of influence. There are key actors having taken care of policy and decision making, while the regulatory dimension is disregarded.

FUNCTION: This model sharply separates three functions: service-delivery, policy-making and regulation. Each function can be found on each level and can be fulfilled by each actor.

TECHNOLOGY: ICT so far has had and in the future will have a huge impact on the fabrication of a State’s functions. ICT will be one of the major drivers for State transformation [93]. See figure 2.18.

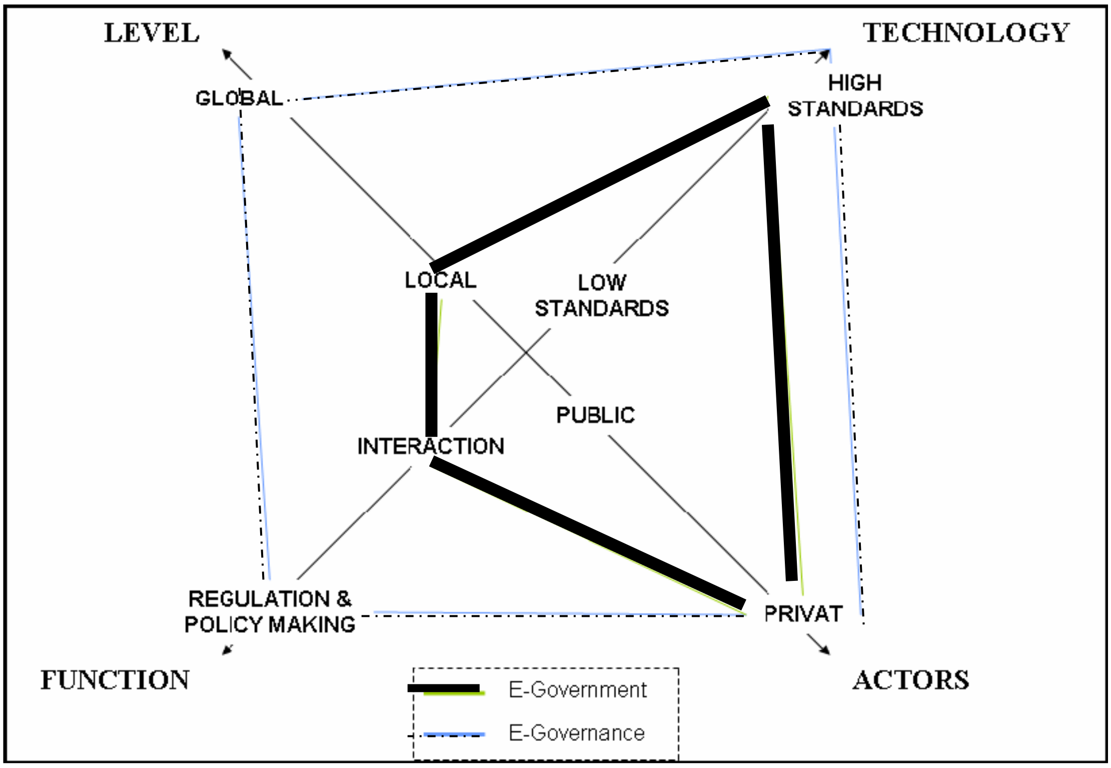


Figure 2.18: This figure illustrates the governance model

2.12 Electronic government systems

E-government systems have become wide spread in more and more countries. However, e-government development systems are too complex to design. E-government is “utilizing the internet and the word-wide-web for delivering government information and services to citizens” [80].

2.12.1 Strengthening Software System Security

Software system itself inherent defect, the local government of the electronic government affairs information security threat was great. In view of this situation, the use of advanced reliable safety technology is the maintenance e-government information safe powerful guarantee. Computer software system of the security administration basically has the following four aspects:

1. Ensure complete software system security. Prevent software the plug in lost, damaged, modify, forge, the specific contents of the management system software about choice and development program, software security testing, system vulnerability

scanning, testing and maintenance, system software users encryption, dynamic tracking, etc.

2. Ensure that the software storage secure. It main have confidentiality storage, compression storage, important data information backup, computer operating system recovery in such aspects as security.

3. Ensure the software network communication security. It main have software transmission, encryption software transmission, software security software users to download, identification, audit and tracking aspects of content.

4. Ensure the normal use security of software. Main have legitimate reasonable use, the user of the safety management, scientific whether grant access, system into the limit, prevention software abuse, stop stealing data, unauthorized copying, etc. [81].

2.12.2 Strengthening Software System Security Emergency Management System

Emergency response refers to when the computer or network system security make the emergency judgment and rapid relief and recovery service. So, the urgent task is to establish the local emergency treatment system, and make corresponding control measures. The local government can set up information safety emergency response center, the establishment of early warning and emergency treatment technology platform, and to further improve the security incident found and analysis ability. By inhibiting strategy, to limit the potential loss and damage From technological gradually realize the early warning, disposal, found, various links and different about the network, system, and department of linkage system between the emergency treatment. Fully mobilize all positive factors, to establish and perfect the local e-government information security emergency management system [82].

2.13 Information security

The terms network security and information security are often used interchangeably, however network security is generally taken as providing protection at the boundaries of an organization, keeping the intruders out [83].

2.14 Passwords

Passwords still pose a significant threat to an information system’s security. This threat is mostly attributed to the human factor, as users tend to select passwords that are easy to remember, but are not resilient to brute force or dictionary attacks.

The password system must be able not only to prevent any access to the system by unauthorized users (i.e., prevent them from logging in at all), but it must also prevent users who are already logged in from doing things that they are not authorized to doing in at all), but it must also prevent users who are already logged in from doing things that they are not authorized to do. Password security is of course only one component of overall System security, but it is an essential component [159].

To counter exhaustive attacks, educated guessing and deriving password of the passwords, there are common advice to improve password management includes monitoring failed login attempts, changing pass words regularly, and avoiding easily guessed passwords [160].

The first weakness can be eliminated by using a one-way function to encode the password. And the second can be eliminated by one must use a sequence of passwords one must use a sequence of passwords xl, x2 . . ... xl0oo, where xi is the password by which the user identifies himself for the ith time [161].

A 2010 paper by Dinei Florencio and Cormac Herley, two researchers at Microsoft Research, presented an analysis of password policies of 75 different websites. They found that, almost counterintuitively, “[s]ome of the largest, highest value, and most attacked sites on the Internet such as Paypal, Amazon, and Fidelity Investments allow relatively weak passwords,” primarily because these websites earn revenue by having people login [162].

2.14.1 Securing User Password

Anne Adams and Martina Angela Sasse say a lot of sensible things in their article about password selection, “Users Are Not the Enemy” (Dec. 1999, p. 41). “Without feedback from security experts, users [create] their own rules on password design that [are] often anything but secure.” The combinatorics of using simple variations on dictionary words would appear to be sufficient to defeat almost any guessing program, and many users rely on such variations**.** Security departments need to partner with users, rather than view them as the enemy within, and users need to better understand the threats to a company in a competitive environment [163].

Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. The U.S. Federal Information Processing Standards suggest several criteria for assuring different levels of password security.

Password composition

Short password lifetime

Finally, password ownership, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations. There are four major factors influencing effective password usage were identified within the framework:
- Multiple passwords;
- Password content;
- Perceived compatibility with work practices; and
- Users' perceptions of organizational security and information sensitivity. One clear finding from this study is that inadequate knowledge of password procedures, content, and cracking lies at the root of users' "insecure" behaviors [164].

2.14.2 Threats against Passwords

The threats against passwords are divided into four groups: threats that directly capture passwords, such as installing keyloggers; threats that take advantage of weak passwords and password hashes, such as password guessing and cracking; threats that replace passwords; and threats that involve attackers reusing compromised passwords.

1- Password Capturing: is getting a password from storage, transmission, or user knowledge and behavior by the attackers.

2- Password Guessing and Cracking: is attempting to determine password by attackers through two types of techniques: guessing and cracking.

3- Password Replacing: An attacker can successfully authenticate to an account by replacing the account's existing password with another password that is known by the attacker.

Using Compromised Passwords: If an attacker has compromised a password through guessing, cracking, or capture, then the attacker will be able to use that password until it is changed by the user. To reduce the potential impact of such unauthorized password use, many organizations have implemented password expiration mechanisms that force a user to select a new password after a certain number of days [165].

2.14.3 Password Guideline

Passwords are vulnerable to compromise because of five essential aspects of the password system:

1. A password must be initially assigned to a user when enrolled on the ADP system.
2. A user’s password must be changed periodically.
3. The ADP system must maintain a password database.
4. Users must remember their passwords.
5. Users must enter their passwords into the ADP system at authentication time.
6. Don’t use the same password on multiple services.
7. Don’t write your passwords down [166].

2.14.4 Attacks on Passwords

♦ In-band

– Attacker repeatedly tries passwords until he authenticates/gets access (guessing, dictionary, or brute force exhaustion)

– Can’t entirely prevent these attacks (can ensure they don’t succeed very often)

♦ Out of band – everything else

– Eavesdropper

– Man-in-the-middle

– Shoulder surfing

– Social engineering [167].

2.14.5 Estimating Password Strength

Password Strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability [167].

2.14.6 Alternative Security Schemes

There are numerous alternatives to password security systems. Among the considerations are the cost to implement, the time required to use, any special considerations regarding place of use, ability to change the scheme if it is compromised, physical limitations, health considerations, non-transferability, time stamped, and so on. In public-key encryption (PKE) the user is authenticated by the private key used to encrypt a message to the server. Public-key infrastructure (PKI) uses PKE to authenticate users across a number of different applications or systems. A PKI can be set up by an organization to be used across its various systems or it can be set up by a third-party vendor to provide authentication services to many vendors. PKI can allow a user to have a single private key that can be used across some or all of the user’s needs, simplifying key management for the user [168].

2.14.6.1 Biometric avenues for human identification

Knowledge-based security (passwords) and token-based security (ID cards) have been used to restrict access to systems. However, security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. Biometric systems make use of fingerprints, hand geometry, iris, retina, face, facial thermograms, signature, gait, palm print and voiceprint to establish a person’s identity. Biometric systems installed in real-world applications must contend with a variety of problems:

- Noise in sensed data
- Intra-class variations
- Distinctiveness
- Non-universality.
- Spoof attacks [169]

2.14.6.2 Visual Passwords

Visual passwords use pictures instead of words or numbers. The idea is driven by the assumption that pictures are more secure and easier to remember than words. Humans have a vast, almost limitless memory for pictures which they remember far better and for longer than words. Pictures have been used in a variety of ways to support authentication, and can be classified into three distinct groups:

Searchmetric systems that require searching a number of images in a challenge set. The target images are then selected by a variety of input techniques, ranging from direct touch to indirect operation of other interface devices.

Locimetric systems that require identification of a series of positions within an image. *Drawmetric* systems that require the user to sketch a drawing [170].

2.14.6.3 Authentication System Using Implicit Learning

The Serial Interception Sequence Learning (SISL) task is a task in which human participants learn a sequence of letters without being aware of what they have learned. It is a method for storing a secret key within the human brain that can be detected during authentication, but cannot be explicitly described by the user. It is a new approach to protecting against coercion attacks using the concept of *implicit learning* from cognitive psychology. The identification system operates in two steps: training followed by authentication [172].

2.15 Social Engineering Attack

Social engineering can be defined as a breach of organizational security via interaction with people to trick them into breaking normal security procedures [173].See figure 2.19.

2.15.1 Classification of Various Social Engineering Attacks

2.15.1.1 Psychological Attacks

1-Phone Social Engineering/Pretexting: Pretexting is the act of creating and using an invented situation in order to grant access to sensitive materials. See figure 2.5

2- Phishing: the most common phishing type completion of a fake online form. [175]

4- Spear Phishing: is any high targeted email or telephone scam, usually employed in business environment [175].

5- Watering Holes: this is a type of social engineering attack in which cybercriminals will identify key web sites that are frequented by individuals or groups they would like to attack, such as mobile app developers.

6- Spoofing: is a process of falsifying ones identity and masquerading as someone else [175].

7- Trojan Horse: Some social engineers exploit people’s curiosity or greed to deliver malware” [175].

2.15.1.2 Physical attacks

1- Dumpster Diving is looking for information that could be used to carry out an attack on a computer network in someone else's trash (passwords written down on sticky notes, phone list, calendar, or organizational chart [174].

2- Shoulder Surfing involves using direct observation techniques, such as looking over someone's shoulder at public places to get his login and password [176].

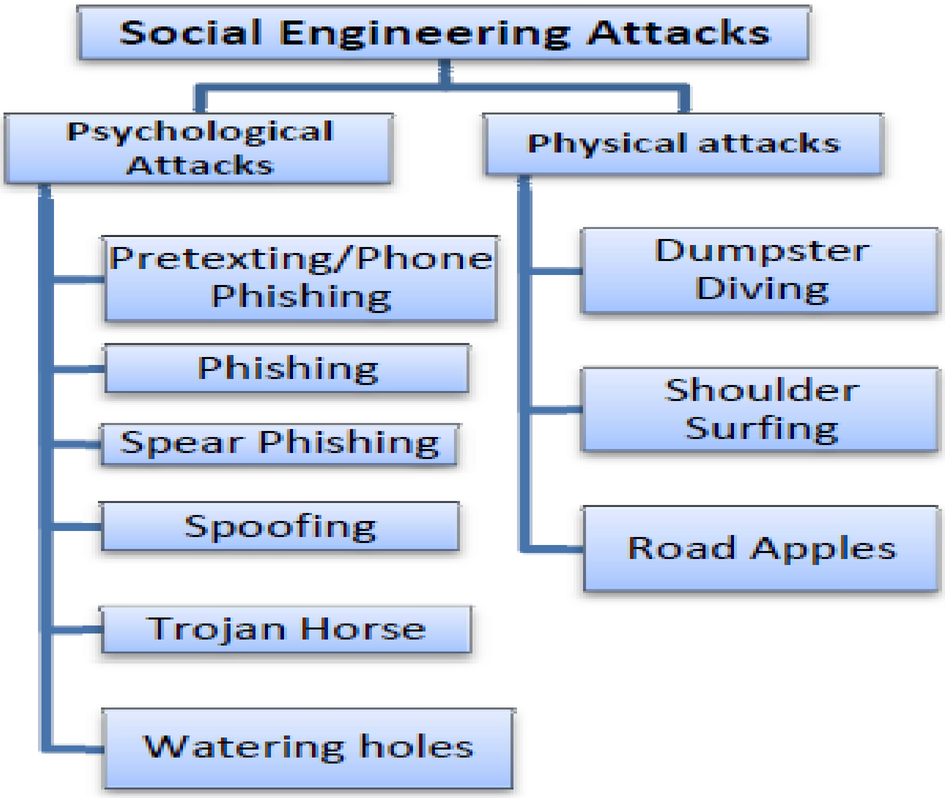


Figure 2.19: This figure shows the classification of social engineering attacks

2.16 Network security

Network security systems today are mostly effective, so the focus has shifted to protecting resources from attack or simple mistakes by people inside the organization, e.g. with Data Loss Prevention (DLP). One response to this insider threat in network security is to compartmentalize large networks, so that an employee would have to cross an internal boundary and be authenticated when they try to access privileged information. Information security is explicitly concerned with all aspects of protecting information resources, including network security and DLP [84].

Network security starts from authenticating any user, commonly (one factor authentication) with a username and a password (something you know). With two factor authentication something you have is also used (e.g. a security token or 'dongle', an ATM card, or your mobile phone), or with three factor authentication something you are is also used (e.g. a fingerprint or retinal scan). Once authenticated, a stateful firewall enforces access policies such as what services are allowed to be accessed by the network users.

2.17 Database security

Database security is a very broad area that addresses many issues, including the following:

- Legal and ethical issue regarding to access certain information.
- Policy issue at the governmental, institutional, or corporate level as to what kinds of information should not be available.
- System related issues such as system levels at which various security function should be enforced.
- The need in some organizations to identify multiple security levels and to categorize the data and users on these classifications for example, top secret, secret, confidential, and unclassified.

In multi-users database system, the Database management system (DBMS) must provide techniques to enable certain users or user groups to access selected portions of database without gaining access to the rest of the database. A DBMS typically includes a database security and authorization subsystems that is responsible for ensuring the security of portions of a database against unauthorized access. It is now customary to refer to two types of database security mechanisms:

- Discretionary security mechanism: These are used to grant privilege to users, including the capability to access specific data files, records, or fields in specified mode (such as read, insert, delete, or update).
- Mandatory security mechanism: these are used to enforce multilevel security by classifying the data and users into various security classes (or levels) and then implementing the appropriate security policy of the organization.

A second security problem common to all computer systems is preventing unauthorized persons from accessing the system itself either to obtain information or to make malicious changes in apportion of the database. The security mechanism of a DBMS must include provisions for restricting access to the database system as the whole. This function is called access control and is handled by creating user accounts and passwords to control the log-in process by the DBMS.

A third security problem associated with databases is that of controlling the access to a statistical database, which is used to provide statistical information or summaries of values based on various criteria.

A fourth security issue is data encryption, which is used to protect sensitive data such as credit card number that is being transmitted via some type of communications network [85].

2.18 Web security

Web security policy defines a framework for allowing web services to express their constraints and requirements. Such constraints and requirements are expressed as policy assertions [86].

2.18.1 Web Application Security

As with any new class of technology, web applications have brought with them a new range of security vulnerabilities. The set of most commonly encountered defects has evolved somewhat over time. The most serious attacks against web applications are those that expose sensitive data or gain unrestricted access to the back-end systems on which the application is running. Web application security is today the most significant battleground between attackers and those with computer resources and data to defend, and it is likely to remain so for the foreseeable future [86].

2.19 Physical protection

An important asset of government departments is the information they store and process on a daily basis. This information must be protected against threats to confidentiality, availability and integrity.

This type of threats are no less important than the technological one it consist of factors that affect the security issues of E-government in Sudan.

Physical security has three important components: access control, surveillance and testing [177].

Physical security can be defined as the measures taken to ensure the safety and material existence of something or someone against theft, espionage, sabotage, or harm. In the context of information security, this means about information, products, and people. Physical security is the oldest form of protection. Physical protection is the first step in the layered approach of information security. If it is nonexistent, weak, or exercised in malpractice, information security will fail. For ages, people have been protecting themselves from harm and their valuables from theft or destruction. In the past, physical security was all the protection someone needed to have safety [178].

2.20 Examples of e-government security models

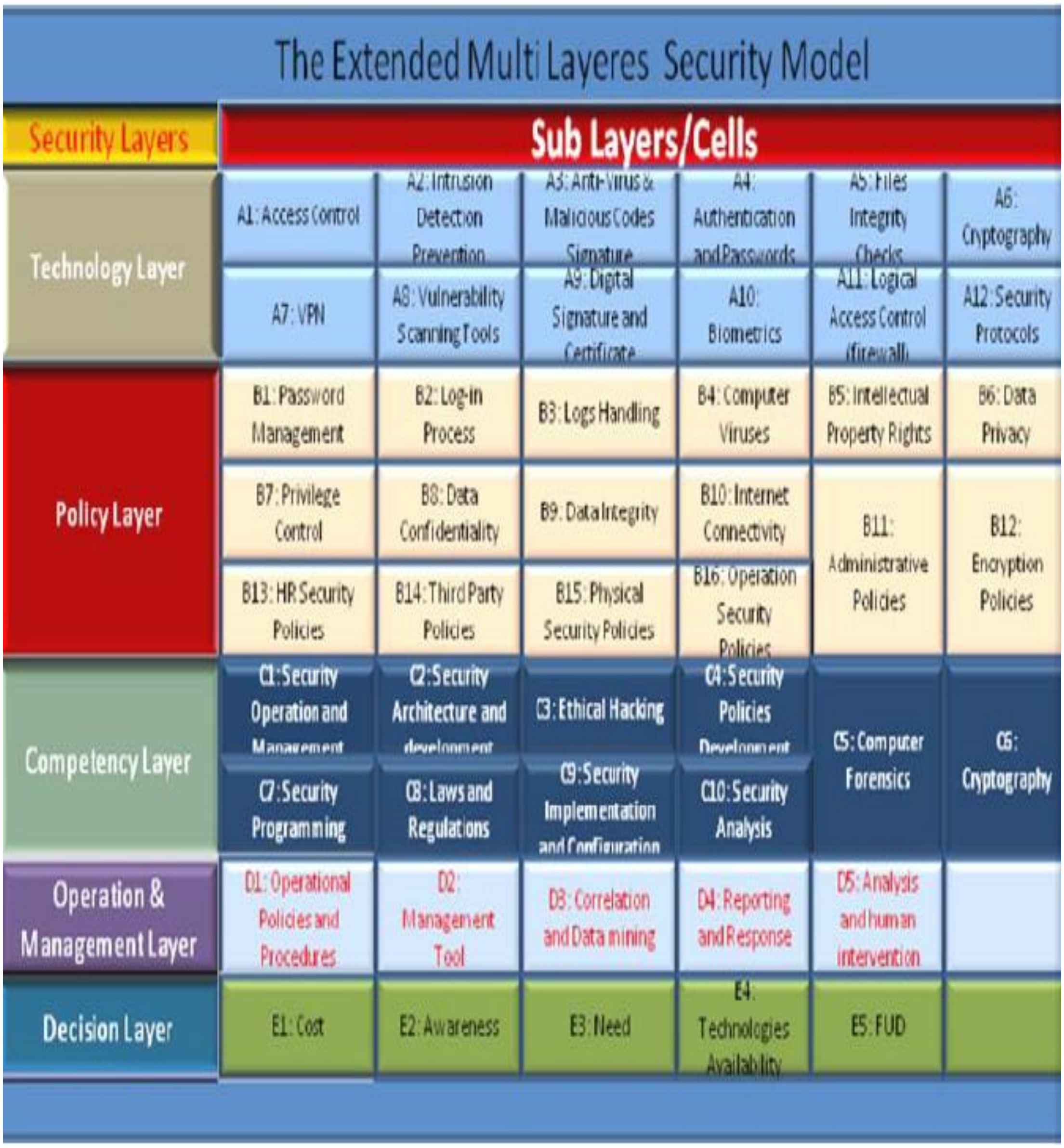
E-Government security models are widely used in the implementation and development of e-government systems. Due to the deference situation of the countries over the world there are various security models applied in each country.

2.20.1 The Five Security Layered-Model in Dubai

In this model there are five layers. Each layer will mitigate group of threats related to an e-services. The model is composed of technology layer, policy layer, competency layer, operational and management layer, and decision layer.

The technology layer for example will address all the technological threats while the policy and competency layers will address the threats on an e-service related to the human aspect. Each layer is composed of detailed layer which is called the sub-layer of the main layer [142]. See figure 2.20 shown the e-government security model in Dubai.

This is a description for some important security threats that faced the Sudanese e-government and not found in Dubai. These threats will be used in the proposed security model for the Sudan. The treats are: IT infrastructure, the managerial treats and law and legislation treats.



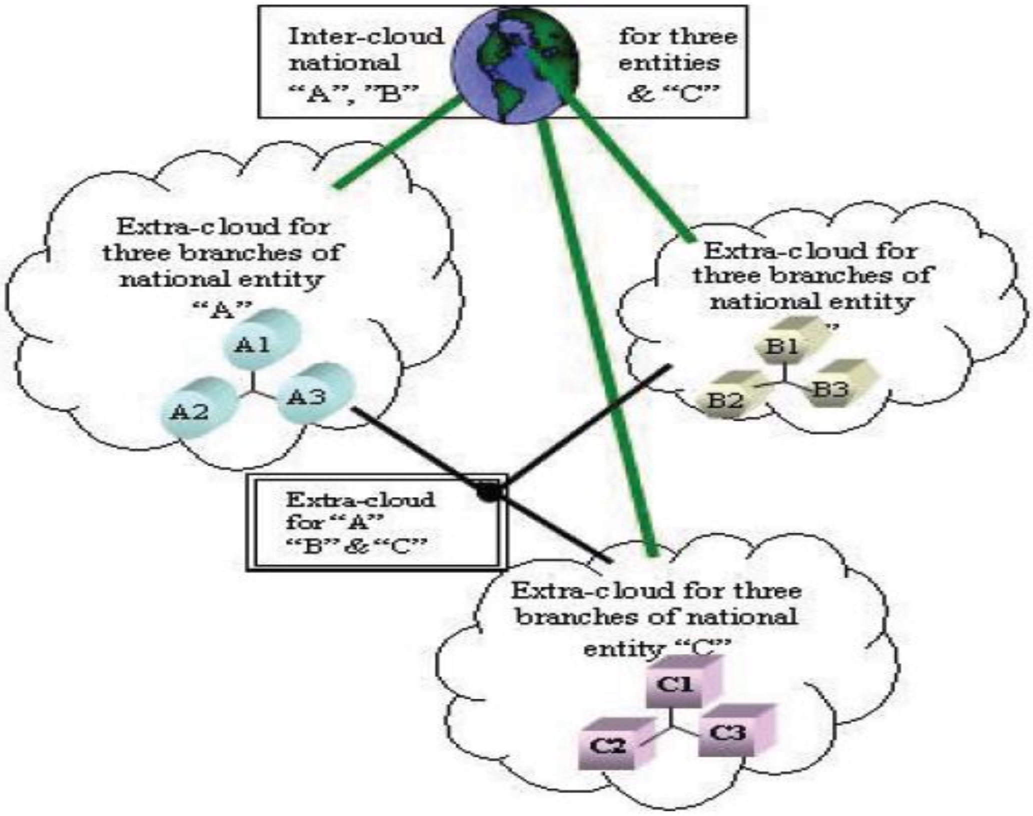
The Extended Multi Layeres Security Model

Security Layers	Sub Layers/Cells					
Technology Layer	A1: Access Control	A2: Intrusion Detection Prevention	A3: Anti-Virus & Malicious Codes Signature	A4: Authentication and Passwords	A5: Files Integrity Checks	A6: Cryptography
	A7: VPN	A8: Vulnerability Scanning Tools	A9: Digital Signature and Certificate	A10: Biometrics	A11: Logical Access Control (firewall)	A12: Security Protocols
Policy Layer	B1: Password Management	B2: Log-in Process	B3: Logs Handling	B4: Computer Viruses	B5: Intellectual Property Rights	B6: Data Privacy
	B7: Privilege Control	B8: Data Confidentiality	B9: Data Integrity	B10: Internet Connectivity	B11: Administrative Policies	B12: Encryption Policies
	B13: HR Security Policies	B14: Third Party Policies	B15: Physical Security Policies	B16: Operation Security Policies		
Competency Layer	C1: Security Operation and Management	C2: Security Architecture and development	C3: Ethical Hacking	C4: Security Policies Development	C5: Computer Forensics	C6: Cryptography
	C7: Security Programming	C8: Laws and Regulations	C9: Security Implementation and Configuration	C10: Security Analysis		
Operation & Management Layer	D1: Operational Policies and Procedures	D2: Management Tool	D3: Correlation and Data mining	D4: Reporting and Response	D5: Analysis and human intervention	
Decision Layer	E1: Cost	E2: Awareness	E3: Need	E4: Technologies Availability	E5: FUD	

Figure 2.20: This figure shows e-government security model in Dubai

2.20.2 E-Government Cloud Computing Proposed Model: Egyptian E-Government Cloud Computing

The proposed hybrid model for Egyptian E-Government Cloud Computing consists of three computing clouds; Inter-Cloud computing, Intra- Cloud computing and Extra-Cloud computing, Figure 2.19[144]. The three cloud models are analogs to the terms Internet, Intranet and extranet in their functionality, operation and management. Intra-Cloud computing "I**A**CC" is a private cloud which is dedicated to a single national entity cluster, Figure 2.20 Members of that cluster are the only legitimate users. Extra-Cloud computing "E**X**CC" is a community cloud that enables entities from different clusters to integrate and to aggregate their work as required. There are two types of E**X**CC. The first type connects multiple I**A**CC of a specific national entity cluster, Figure 2.21. The second type connects different national entity clusters that differ in their functions and services, Figure 2.22 Inter-Cloud computing "I**E**CC" is a public cloud that enables any user (citizen, guest, organizations) to require specific requests and receives their responses or outcomes, Figure 2.20 In I**E**CC, it is expected to store the least sensitive data and to run the related application software.



Inter-cloud national “A”, ”B”
for three entities & “C”
Extra-cloud for three branches of national entity “A”
A1
A2
A3
Extra-cloud for three branches of national entity ”
B1
B2
B3
Extra-cloud for “A” “B” & “C”
Extra-cloud for three branches of national entity “C”
C1
C2
C3

Figure 2.21: This figure shows a proposed model for Egyptian E-Government Cloud Computing

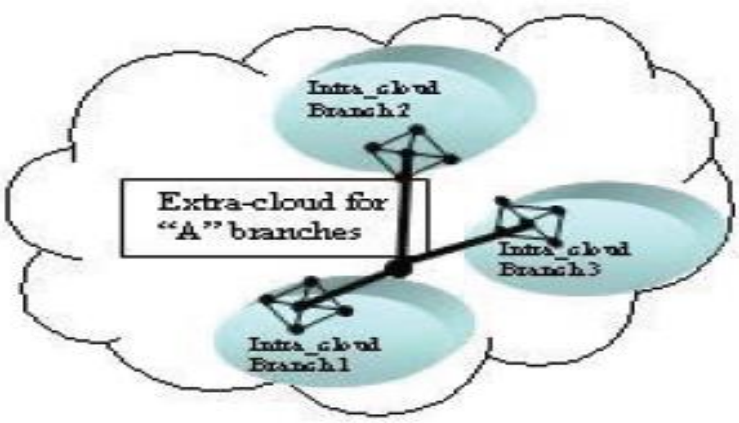


Figure 2.20: This figure shows IACC and EXCC for National entity A.

2.20.3 A Secure Maturity Model for protecting e-government Services: A Case of Tanzania

The proposed secured e- Government maturity model consists of four layers, namely: (1) secured digital presence, (2) secured interaction, (3) secured transaction, and (4) secured transformation. The implementation of the proposed model is neither based on a specific technology/protocol nor a certain security system/product, but rather an approach towards a structured and efficient implementation of those technologies. The security layers include technical and non-technical security control elements. The proposed security layers are further described in the following paragraphs [145].

a. Secured Digital Presence

This stage involves simple provision of government information through website (static) with basic information that the citizen can access [146]. This is a one-way communication between governments, businesses and citizens. Generally, the information provided by organizations at this stage are public and normally with zero security. At this stage, the security layer should have the ability to verify e-Government services identity in order to build trust between government agencies and users. The users would like to be sure that they are connected to the e-government service belonging to the administration in question [147].

b. Secured Interaction

At this stage the interaction between government and the public (Government-to-Citizens and Government-to- Businesses) is stimulated by various applications. Citizens can ask questions via e-mail, use search engines and download forms and documents [147]. The communication is performed in two ways, but the interactions are relatively simple and generally revolve around information provision. At this stage, the security layer should have the ability to authenticate a user/ citizen asking for a service. The most important security aspects at this stage are identity authentication, availability and integrity.

c. Secured Transaction

At this stage public organizations provide electronic initiatives and services with capabilities and features that facilitate clients to complete their transactions in full without the necessity of visiting government offices [148]. The public can carry out their financial transactions with the government such services also allow the government to function in a 24/7 mode. The most important security aspects at this stage are personal information confidentiality, identity authentication, availability, non-repudiation, accountability and integrity.

d. Secured Transformation

This stage allows users of e-government services to interact with government as one entity instead of Information systems are integrated, and the citizens individual government organizations can get services at one virtual counter [149]. The integration of information systems can result in situations where the privacy of individual citizens is in danger. The most important security aspects of this stage are personal information confidentiality, identity authentication, availability, nonrepudiation, accountability and integrity. At this stage, the security layer should restrict the utilization of personal information, and secure such information from access by unintended parties. A government agency should be able to authenticate another government agency that requires a service on behalf of the users.

2.20.4 A Security e-government Model Based on Service-oriented Architecture

Service-oriented architecture is an IT architectural style that supports integrating business as linked services which users can combine and reuse them in the production of business applications [150]. It provides an effective way for constructing loose coupled web services. It relies on services exposing their functionality via interfaces that other services can understand how to utilize those services. SOA logical architecture is shown in figure 2.23 [151].

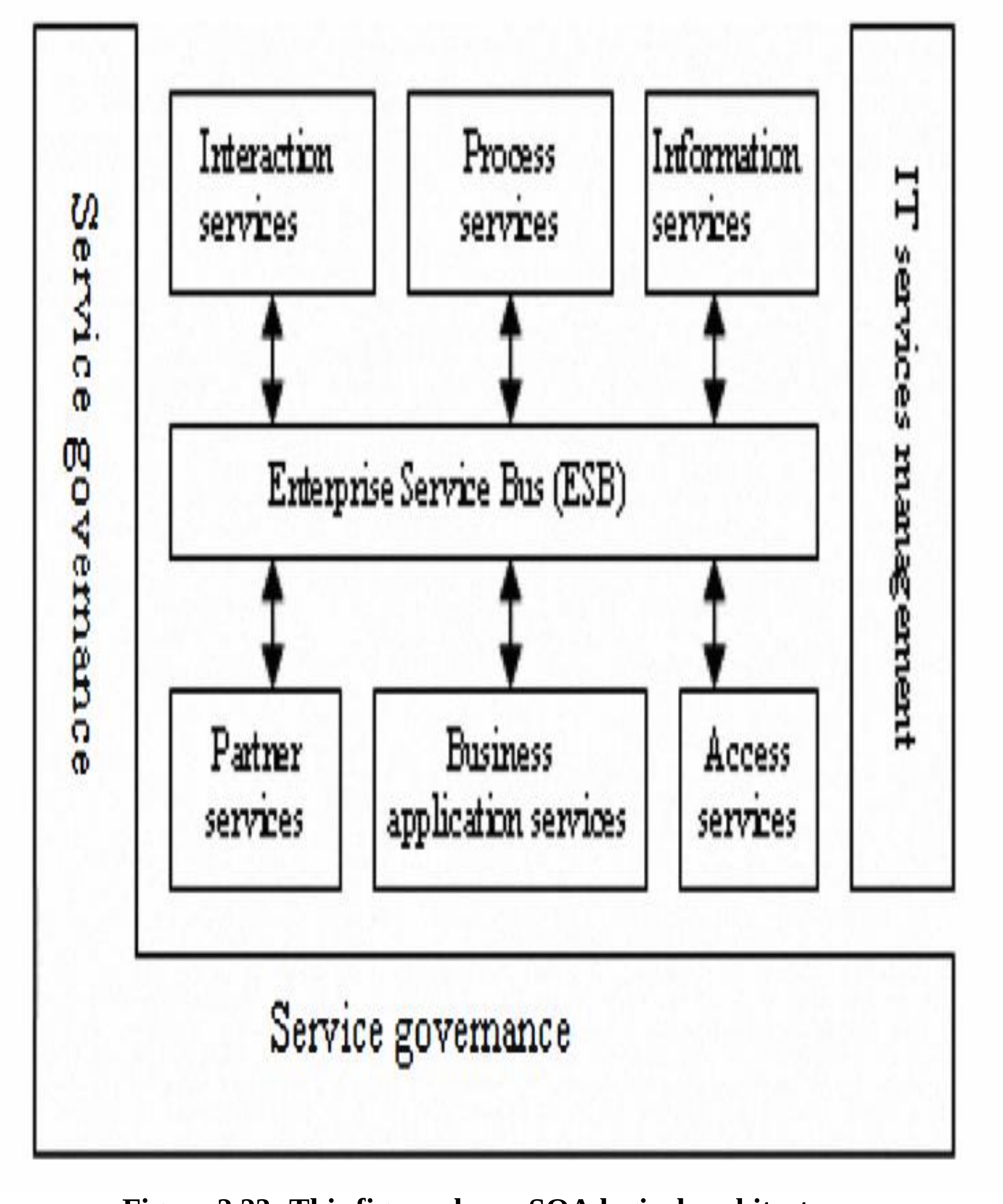


Figure 2.23: This figure shows SOA logical architecture.

The SOA technology framework to integrate e-government: using BEPL implement work process; realizing seamless integration between services by ESB. Taking the case of online application processing, a scheme of integration e-government system based on SOA is shown as figure 2.24 [151].

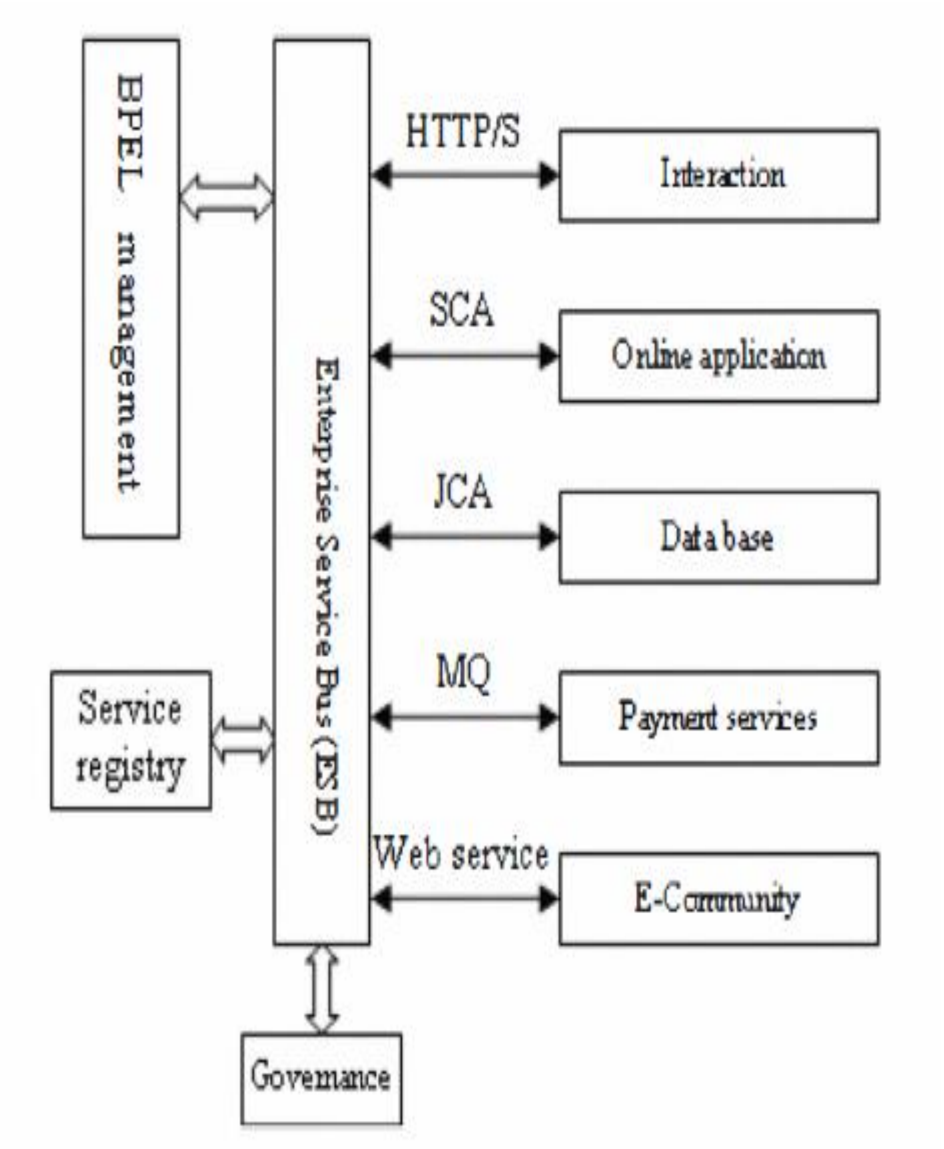


Figure 2.24: This figure shows a scheme of integration e-government system based on SOA.

2.20.5 E- Research on Role-Based Access Control Policy of e-government

The access control system includes subjects, objects and access control policy, and their relationship is shown in figure 2.25 [152].

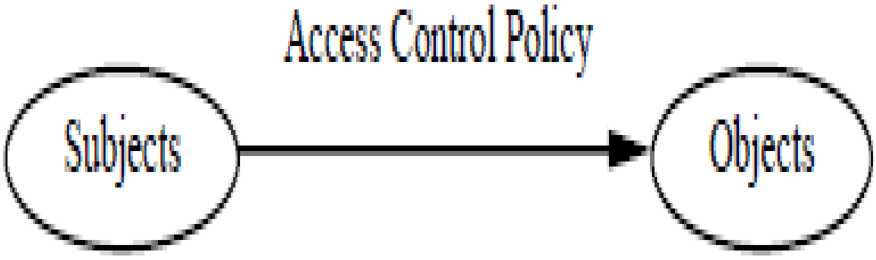


Figure 2.25: This figure shows access control system model

The RBAC is a new access control technique and notion. It is the development and amelioration of DAC and MAC, and it has been regarded as an effective measure to resolve resource unified access control of large information systems by the public.

The RBAC contains five kinds of entities, such as users, roles, constraints, permissions, and sessions. In the RBAC model, it injects the idea of roles between users and access permissions, and a user connects with one or more specific roles, and a role connects with one or more permissions, and roles can be created or canceled according to actual working requirements. The sessions show the relationship between users and roles. The users should activate roles by creating sessions every time and get the specific resource access authorities as shown in Figure 2. 26 [153,154].

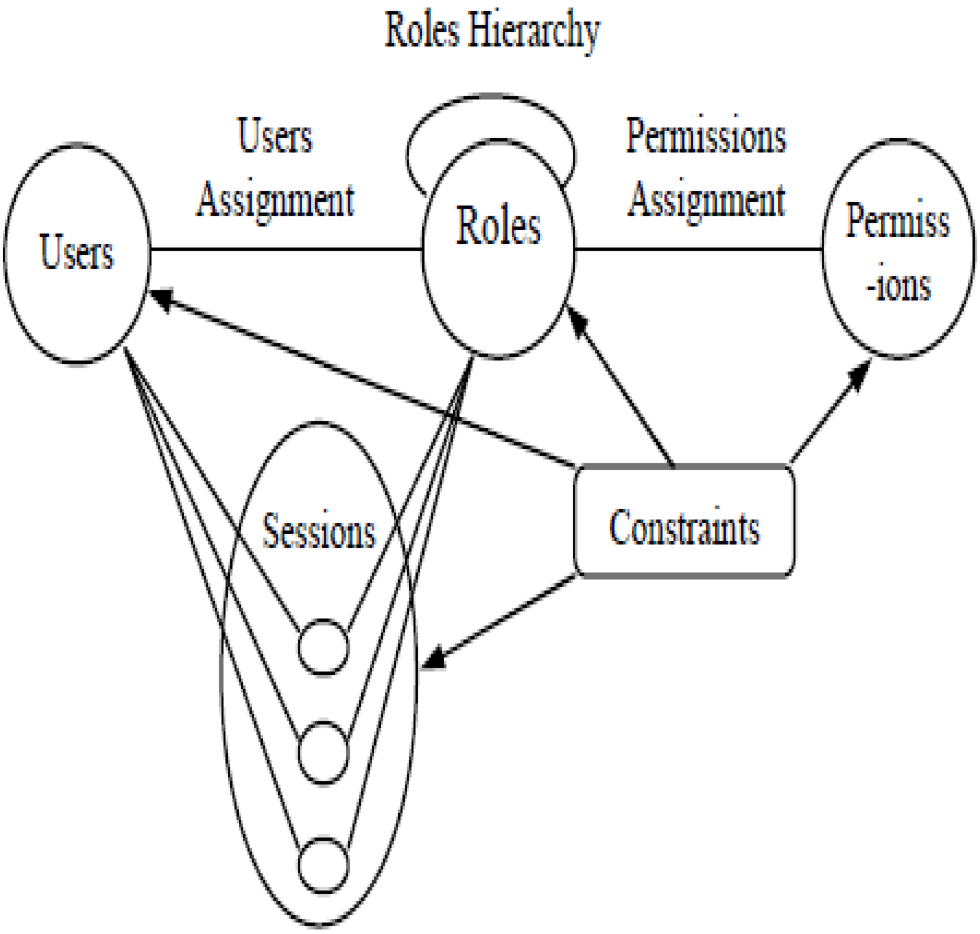


Figure 2.26: This figure shows basic RBAC model

2.20.6 Security System based on Information Security Model

The system is designed through modularization and it is mainly divided into initialization module, management module and various application modules. In which, the initialization module is used to manage the original data of the initial management module and various application modules, the management module is used to manage the content which has effect in the overall system, such as the users, privileges and a series of rules in the system. Various application modules work together by using the initialized data and through the transmission media to complete the overall function of the system. The secure e-government system structure is shown in figure 2.27.

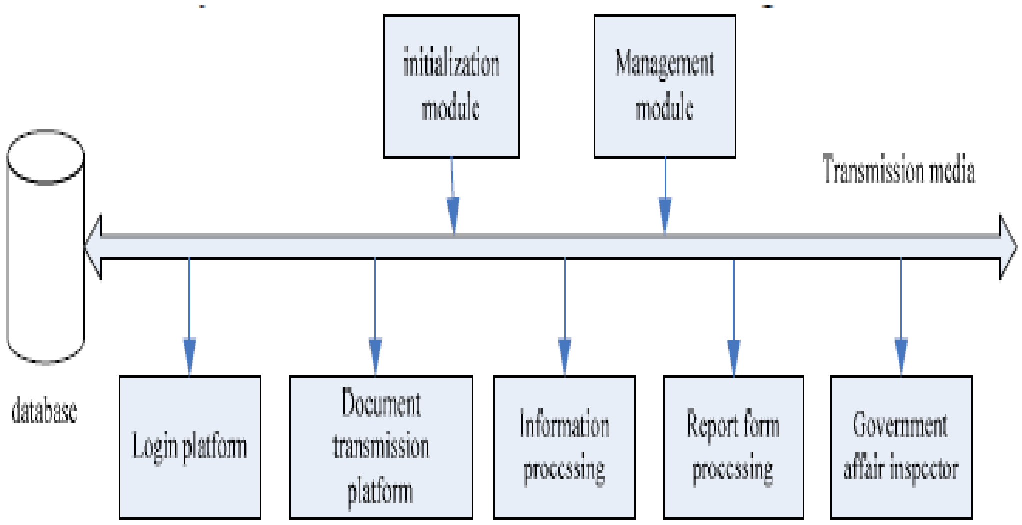


Figure 12.27: This figure shows secure e-government system

2.21 Summary

This chapter starts with general information about the e-government over the world and focuses on the state of the e-government over the world and reviews the key issues related to concepts, definitions, and perceptions. These issues are explained by identifying the main characteristics and various perspectives, and their interaction necessary when embracing e-government. The interdisciplinary nature, multiple definitions and meanings reflect the challenges existing in e-government applications. The literature reviewed in this chapter has helped to develop a better understanding of the challenges impeding successful e-government implementation, as well as addressing the many opportunities provided to improve government efficiency and effectiveness.

CHAPTER III

METHODOGY

3.1 Introduction

This chapter describes Sudan, highlights its background and main characteristics, history, governance, demography, economy, and background description of ICT, e-government in Sudan as a part of research methodology, and specifies the research methods that applied in the work, and detail how the research process was carried out.

3.2 Sudan History, Location and Area

Sudan was a British colony that achieved independence on 1st January 1956, being one of the first countries in sub-Saharan Africa to gain independence from the colonialism that occurred in Africa in the 1860s. Throughout its history, Sudan has been divided because of the Arab heritage, associated with northern Sudan; and its African heritage in the south [94].

The civil war between the North and South lasted for more than two decades, being the longest civil war in the twentieth century. The violence, famine, and disease during the war killed more than 2 million people, forced an estimated 600,000 people to seek refuge in neighboring countries, and displaced approximately 4 million others within Sudan [95].

In 2005 the Comprehensive Peace Agreement (CPA) was signed; and in 2011 a referendum took place to determine whether the south region should remain part of Sudan or become independent. Southern Sudan voted in favour of independence and on the 9th of July 2011, the country was split into two separate states. The UN estimates that approximately 2 million displaced people have returned to South Sudan. The division affected the politics of the whole country and led to dramatic changes in terms of demography and economy [96].

Since 2003 Sudan has been beset by another conflict in the western region of Darfur. According to the UN this has driven two million people from their homes and resulted in more than 200,000 deaths. The Darfur problem has led to one of the most serious humanitarian crises in resent world history, badly affecting the economic development of the entire country [97].

Sudan is located in the north-eastern part of Africa (Figure 4.1), and occupies the central region between Africa and the Arab World. The location results in Sudan's unique characteristics, as it is the main passage between north and south of Africa [97]. Sudan was also the main route for the pilgrim and trade convoys that crossed from the west of Africa to the Holy Lands in Makah, until the middle of the current century [98].

3.3 Government System

Decentralization, as per the following government levels: - National government level; exercising powers with a view to safeguarding Sudan national sovereignty, conserving its territories and enhancing the people prosperity. -State government level; exercising powers at states level across Sudan, with provision of public services via the closest level to the citizen. - Local government level; applicable throughout the country which is made up of 18 states [99].

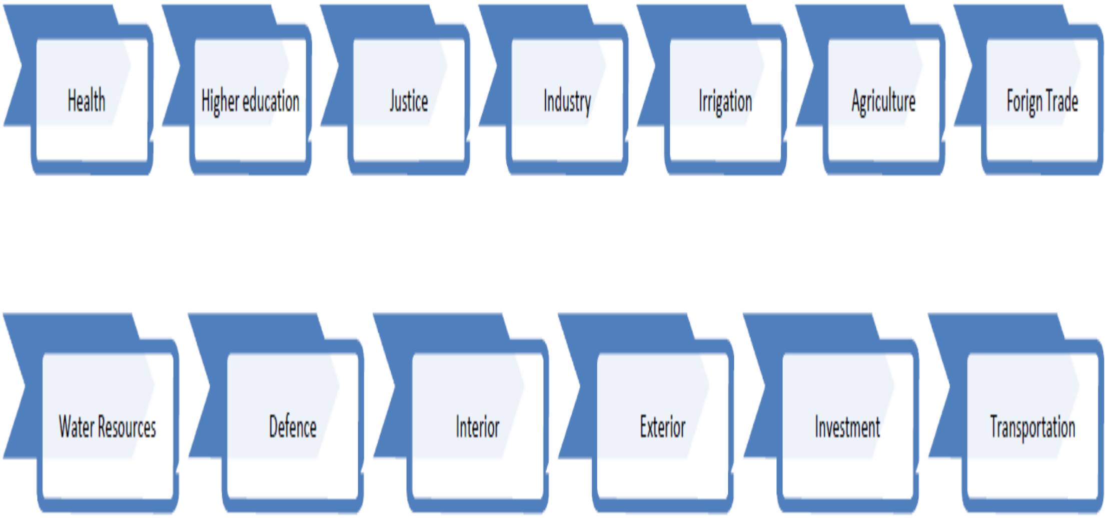


Figure 3.1: Government areas of responsibilities

3.4 Sudan Demography and Economy

Sudan, officially the Republic of Sudan but sometimes referred to as North Sudan, sits along the Red Sea south of Egypt and has a population consisting mostly of descendants of migrants from the nearby Arabian Peninsula. Sudan has a total area of 1,886,068 square kilometers (728,215 square miles) and has an estimated 2014 population of 39,105,664, a significant increase from the 34,847,910 estimated in 2013 [100]. The economy depends largely on the agriculture and oil sectors [101].

Sudan is an extremely poor country that has had to deal with social conflict, civil war, and the July 2011 secession of South Sudan - the region of the country that had been responsible for about three-fourths of the former Sudan's total oil production. The oil sector had driven much of Sudan's GDP growth since it began exporting oil in 1999. For nearly a decade, the economy boomed on the back of increases in oil production, high oil prices, and significant inflows of foreign direct investment. Following South Sudan''s secession, Sudan has struggled to maintain economic stability, because oil earnings now provide a far lower share of the country''s need for hard currency and for budget revenues. Sudan is attempting to generate new sources of revenues, such as from gold mining, while carrying out an austerity program to reduce expenditures. Agricultural production continues to employ 80% of the work force. Sudan introduced a new currency, still called the Sudanese pound, following South Sudan''s secession, but the value of the currency has fallen since its introduction. Khartoum formally devalued the currency in June 2012, when it passed austerity measures that included gradually repealing fuel subsidies. Sudan also faces rising inflation, which reached 47% on an annual basis in November 2012. Ongoing conflicts in Southern Kordofan, Darfur, and the Blue Nile states, lack of basic infrastructure in large areas, and reliance by much of the population on subsistence agriculture ensure that much of the population will remain at or below the poverty line for years to come [102].

3.5 Sudan National Fibre Network

Sudan has an extensive fibre network rollout by incumbent Sudatel. It has a direct link to international fibre through Port Sudan figure 3.3.

Internet access has substantially improved in the country and access to high bandwidth is common place where fibre is available. Sudatel contribute 13% in the submarine cable to east Africa extending from Port Sudan to cape Town linking 13 countries in the eastern coast of Africa and owns 50% of SAS1 and SAS2, which are huge projects for transmission linkage between Port Sudan and Jeddah, in addition to Sudatel Contribution at the continental cable ACE with 9% that links the western coast countries extending from Cape Town to France. Sudatel is also linked with Ethiopia and Egypt via the fiber optic [103].

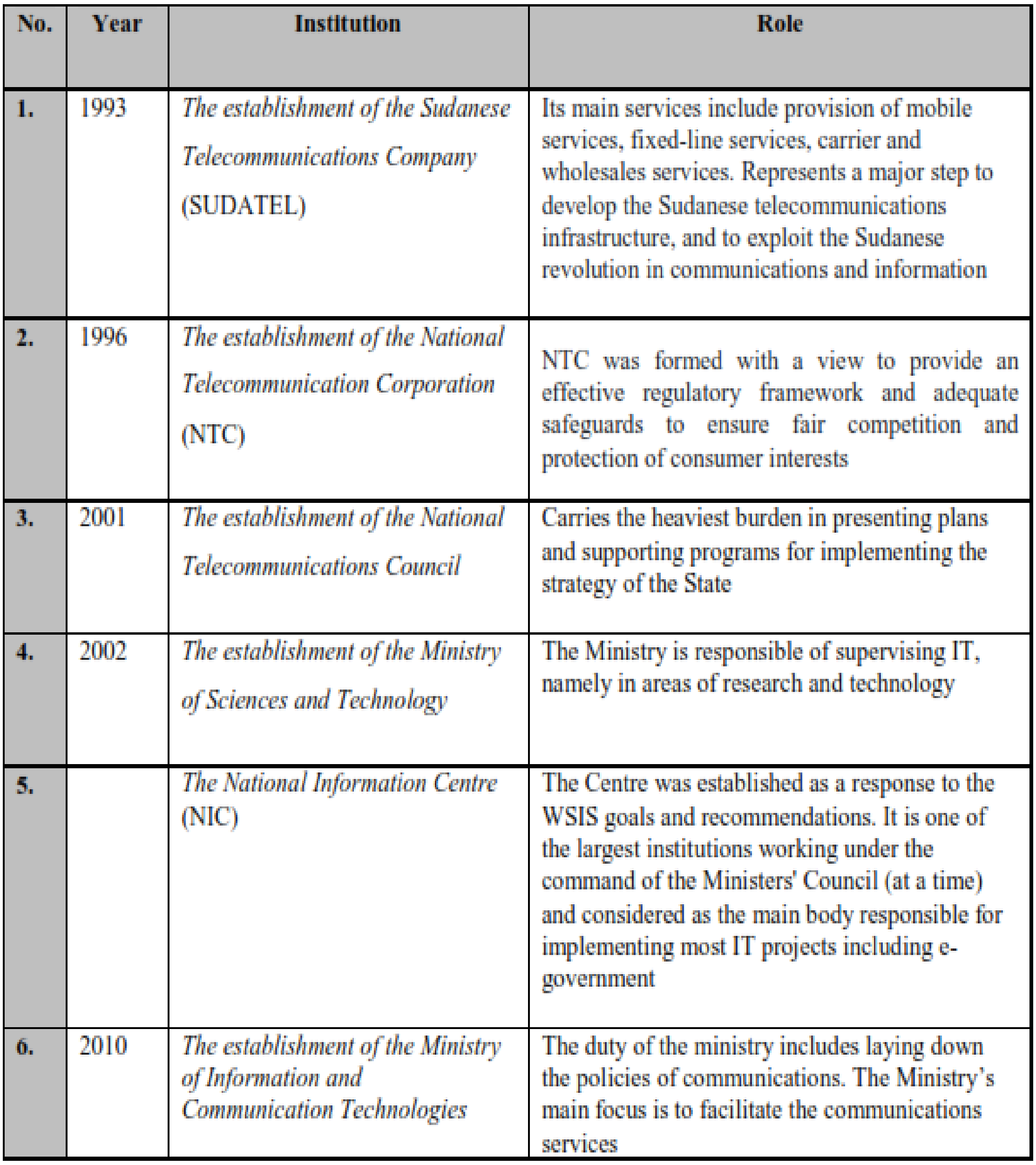
3.6 ICT in Sudan

Sudan’s experience during the last two decades in both building and capitalising on ICT as a gateway for sustainable development is a landmark in the country’s history [104]. Sudan is deploying ICT technologies as an enabler (or instrument) of development. To this end, the government drafted a 25 year National Strategy for the period 2007-2031, to promote the ICT industry. In the year 2001 the government approved the national strategy for building the information industry in Sudan. The strategy is embodied in: “the firm foundation of information industry ... leading to the widest dissemination and utilisation of information, ... which shall contribute to achieve economic growth, job opportunities ... and eradication of poverty”[105].

The Sudanese government is committed to the objectives determined by the WSIS held in Geneva in 2003 and in Tunisia in 2005, as well as the internationally agreed development goals; including those contained in the Millennium Development Goals

[106]. Sudan has made considerable efforts to accelerate the implementation of WSIS action plans; the most important of which was the establishment of several ICT institutional bodies to play the role of regulating, planning, training and executing ICT projects and initiatives. Table 3-1 presents most official ICT institutions formulated by the government.

Table 3.1: ICT institution bodies



No.	Year	Institution	Role
1.	1993	*The establishment of the Sudanese Telecommunications Company* (SUDATEL)	Its main services include provision of mobile services, fixed-line services, carrier and wholesales services. Represents a major step to develop the Sudanese telecommunications infrastructure, and to exploit the Sudanese revolution in communications and information
2.	1996	*The establishment of the National Telecommunication Corporation* (NTC)	NTC was formed with a view to provide an effective regulatory framework and adequate safeguards to ensure fair competition and protection of consumer interests
3.	2001	*The establishment of the National Telecommunications Council*	Carries the heaviest burden in presenting plans and supporting programs for implementing the strategy of the State
4.	2002	*The establishment of the Ministry of Sciences and Technology*	The Ministry is responsible of supervising IT, namely in areas of research and technology
5.		*The National Information Centre* (NIC)	The Centre was established as a response to the WSIS goals and recommendations. It is one of the largest institutions working under the command of the Ministers' Council (at a time) and considered as the main body responsible for implementing most IT projects including e-government
6.	2010	*The establishment of the Ministry of Information and Communication Technologies*	The duty of the ministry includes laying down the policies of communications. The Ministry's main focus is to facilitate the communications services

The strategy called for the adoption of financial, economic, commercial, educational, Industrial and information policies that encourage and support the targeted objectives [106].

The main objectives articulated were:

- Developing national human capital in knowledge technologies
- Achieving e-readiness and bridging the digital divide
- Facilitating individuals to enrich the national content and political involvement of citizens through virtual organizations and e-voting

- Building an electronic government and civil society organizations

An important outcome from these themes was promoting the role of the private sector and encouraging private investment. Privatisation in the telecommunications sector, which took place in 2005, had a major impact in: decreasing telecommunication costs; increasing the rate of development in the field of information technology; and narrowing the digital divide between the rural and urban areas [107].

As a result, by the year 2010 there were four mobile and fixed lines telecoms companies with more than 21,000 km fibre optic, 18 million subscribers (45% of the population) and 4.2 million Internet users. The income in 2009 reached US $3 billion, making the Sudan telecommunications sector one of the fastest growing markets in Africa [108].

The Sudanese government also recognised the importance of developing policies and procedures that guarantee a well-developed ICT infrastructure through legislation; vital to increase citizens' confidence and trust. In this regard, the government managed to enact new legislation, including the Computer Crime Act 2007 and the Electronic Transaction

Law. In addition, it introduced standards for ICT hard technology and software. An important achievement was establishing the Computer Career Council. Sudanese people from various backgrounds and with different qualifications all showed interest in adopting ICT, and the government gave support. The ICT community established Sudanese IT and Internet societies and most Sudanese newspapers are now published online. In 2010 the ICT community started producing the first weekly ICT magazine. Public and private TV channels broadcast ICT programs (ESCWA, 2009), aiming to raise awareness among citizens. This led to pressure on the government from the citizens and the "aware community" requesting more access to information and a greater role in decision making. Despite the progress achieved in ICT in Sudan, it is still immature compared to other developed or rapidly developing countries. The complex issues surrounding Sudan politically, economically and socially have hindered many initiatives. There are obvious difficulties facing ICT initiatives in such a developing country, with comparatively few resources and low levels of funding from state and local governments. Some citizens may be looking forward to being part of the information society and even be demanding electronic service delivery, but this is a small percentage of the society. More than 40% of people in Sudan are below the poverty line [109] and their priority is a better quality of life. This meant that the attention of policy and decision-making leaders drifted towards other problems of peace, security and citizens' basic needs. The difficulties facing ICT in Sudan can be generalised in the following challenges [110]:

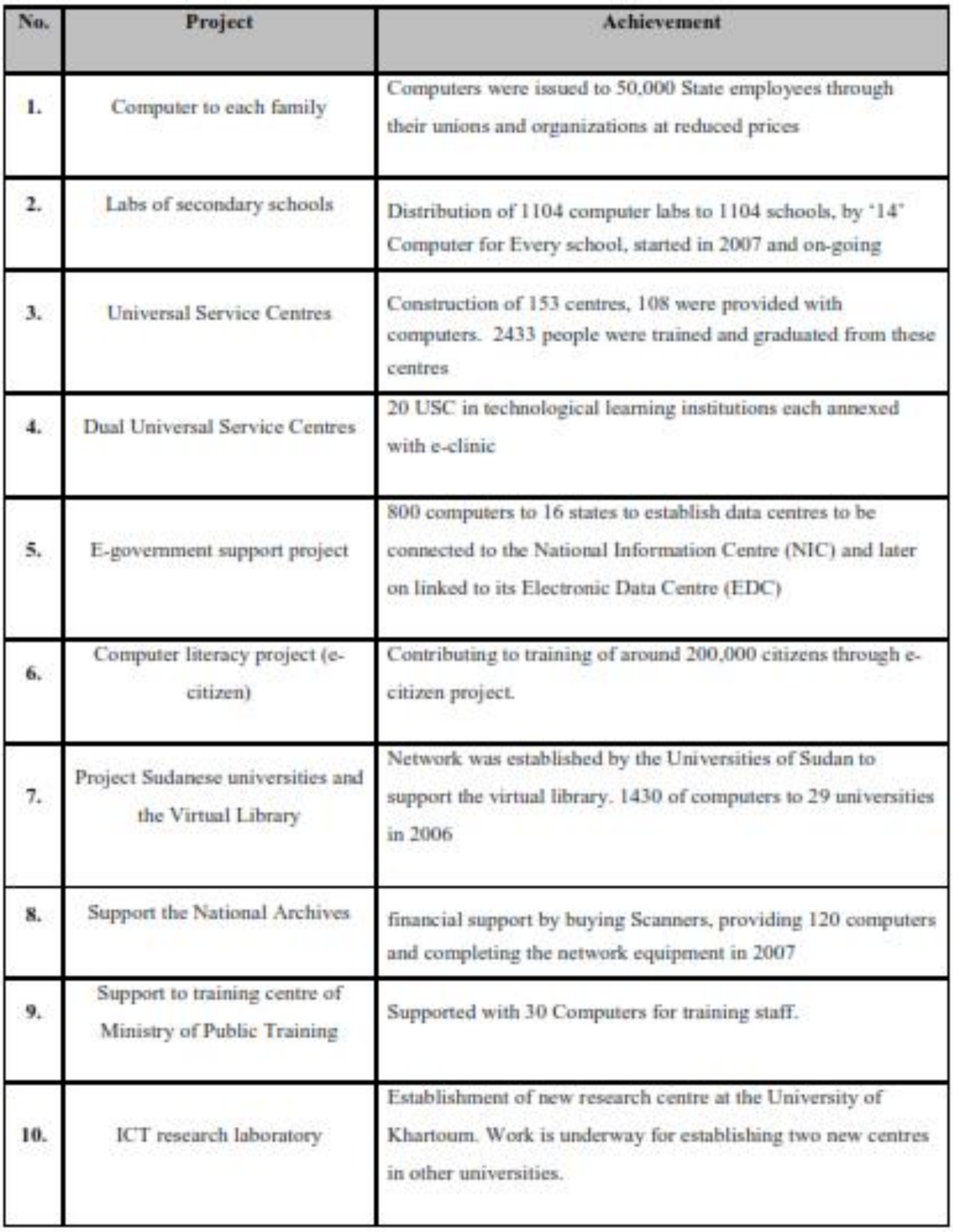
- The vast and wide geographical area of Sudan
- Bureaucracy
- Organizational structure
- Education and training system
- Public awareness
- Legal framework
- Institutional framework
- International and regional partnership
- Allocation of funds

As funding is a major obstacle for ICT projects, which are expensive by nature, the government established the Informatics Support Fund in 2003, with a remit to fund informatics development projects in Sudan [106]. This Fund provides support for the development of the communications infrastructure. It also seeks to provide services in different areas in Sudan, attempting to bridge the gap between urban and rural areas in the country.

Internet services started in Sudan in 1998, but it was only in the early 2000s that the government began to give real attention to ICT and involve IT at a large scale in government operations and processes. The number of applications and projects are still limited and are yet to mature. As is the case in many countries, the first utilization of ICT was through the private sector. E-business in the private sector prompted the government to adopt its own e-business, but it is still limited when compared with government economic activity in general.

Table 3-2 lists some ICT projects and applications. They are at different levels in their progress, but all projects played a significant role in the development and adoption of ICT in the government.

Table 3.2: Selected ICT projects in Sudan



No.	Project	Achievement
1.	Computer to each family	Computers were issued to 50,000 State employees through their unions and organizations at reduced prices
2.	Labs of secondary schools	Distribution of 1104 computer labs to 1104 schools, by '14' Computer for Every school, started in 2007 and on-going
3.	Universal Service Centres	Construction of 153 centres, 108 were provided with computers. 2433 people were trained and graduated from these centres
4.	Dual Universal Service Centres	20 USC in technological learning institutions each annexed with e-clinic
5.	E-government support project	800 computers to 16 states to establish data centres to be connected to the National Information Centre (NIC) and later on linked to its Electronic Data Centre (EDC)
6.	Computer literacy project (e-citizen)	Contributing to training of around 200,000 citizens through e-citizen project.
7.	Project Sudanese universities and the Virtual Library	Network was established by the Universities of Sudan to support the virtual library. 1430 of computers to 29 universities in 2006
8.	Support the National Archives	financial support by buying Scanners, providing 120 computers and completing the network equipment in 2007
9.	Support to training centre of Ministry of Public Training	Supported with 30 Computers for training staff.
10.	ICT research laboratory	Establishment of new research centre at the University of Khartoum. Work is underway for establishing two new centres in other universities.

3.7 The Internet in Sudan

The Internet in Sudan started in 1996 as a joint venture between Sudan Telecommunications Company (SUDATEL) and the Sudan Corporation of

Broadcasting and Television as a dial-up service. A private company was licensed to provide a broadband wireless service beside the existing one. As from 1998 internet service was introduced by 2.5G technology through the licensed mobile service operators. In 2007 the internet service began to be provided by the 3G technologies (CDMA-EVxDO, UMTS) which facilitated a vast and dense ubiquity all over the country. That was sustained by the higher capacities made available from the submarine optic cables connected to global systems (FLAG). The provision of the Internet service by the licensed public service operators with high speed and assorted packages led the working ISP's to shrink considerably, in addition to the decline of the telephone fixed service and the increase of the mobile. This matter is being studied intensively by the NTC to remedy the situation particularly in the Telecom Act Update. As the coverage, penetration and access to the internet service is still lower than expected despite the wide use of the web network in the country, NTC is managing to remedy the situation by formulating effective rules that can lead to increase the coverage and access facilities beside improving the affordability. Those goals are expected to be effective through universal service programs and the support of consultations with service providers and stakeholders [106].

3.7.1 The internet backbone in Sudan

It is known that Sudatel is a largest telecommunications and Internet service provider in Sudan. The company is responsible for the construction and maintenance of Sudan's telecom infrastructure. The IP Backbone Topology view shows links between routers, and network locations. See figure 3.2.

In case of Sudatael in Sudan there are plane A and B that composed of Huawei routers that connect network location (Sudanese cities) with each other's by 10 gigabit Ethernet or Gigabit Ethernet or STM-1 (Synchronous Transport Module level-1). NE80E core routers (NE80E for short) are applied as core routers in IP backbone networks, IP metropolitan area networks (MANs), and other large-scale IP networks.

NE80E core routers (NE80E for short) are applied as core routers in IP backbone networks, IP metropolitan area networks (MANs), and other large-scale IP networks.

The NetEngine40E series universal service router (NE40E) is a high-end network product provided by Huawei Technologies Co., Ltd. NE40Es are usually deployed at the edges of Internet Protocol (IP) backbone networks, IP Metropolitan Area Networks (MANs), and other large-scale IP networks. The NE40E can provide a complete, layered IP network solution. The NE40E can be flexibly deployed at the edge or core of IP or MPLS networks, simplifying network structure. With its ability to provide an extensive range of services and reliable service quality, the NE40E is driving IP and MPLS bearer networks to develop greater broadband capacity and to become more intelligent and more service-oriented.

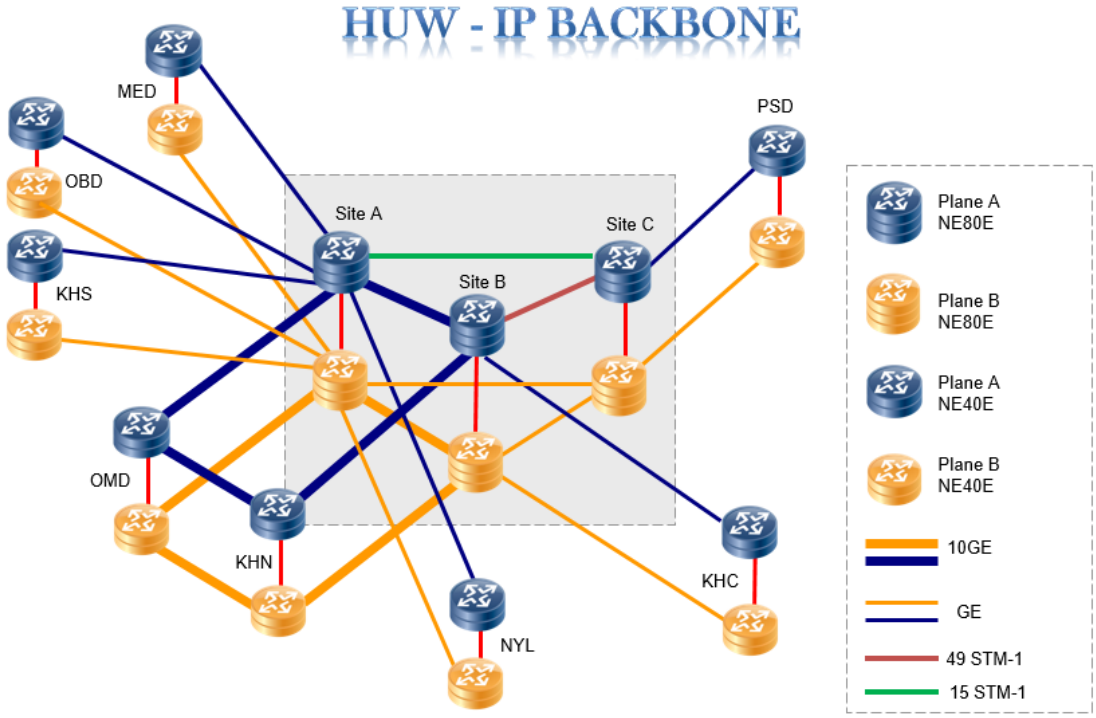


Figure 3.2: illustrates the HUW IP backbone used by SUDATEL

The STM-1 (Synchronous Transport Module level-1) is the SDH ITU-T fiber optic network transmission standard. It has a bit rate of 155.52 Mbit/s. Higher levels go up by a factor of 4 at a time: the other currently supported levels are STM-4, STM-16, STM-64 and STM-256. Beyond this we have wavelength-division multiplexing (WDM) commonly used in submarine cabling.

10-gigabit Ethernet (10GE, 10GbE, or 10 GigE) is a group of computer networking technologies for transmitting Ethernet frames at a rate of 10 gigabits per second (10×10^{9} or 10 billion bits per second). It was first defined by the IEEE 802.3ae-2002 standard. Unlike previous Ethernet standards, 10-gigabit Ethernet defines only full duplex point-to-point links which are generally connected by network switches; shared-medium

CSMA/CD operation has not been carried over from the previous generations Ethernet standards. Half duplex operation and hubs do not exist in 10GbE.

10 gigabit Ethernet is a telecommunication technology that offers data speeds up to 10 billion bits per second. It differs from traditional Ethernet in that it is a full-duplex protocol and does not require Carrier Sense Multiple Access/Collision Detection (CSMA/CD). Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently being used as the backbone in many enterprise networks. Gigabit Ethernet is carried primarily on optical fiber (with very short distances possible on copper media). Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone. An alternative technology that competes with Gigabit Ethernet is ATM. A newer standard, 10-Gigabit Ethernet, is also becoming available.

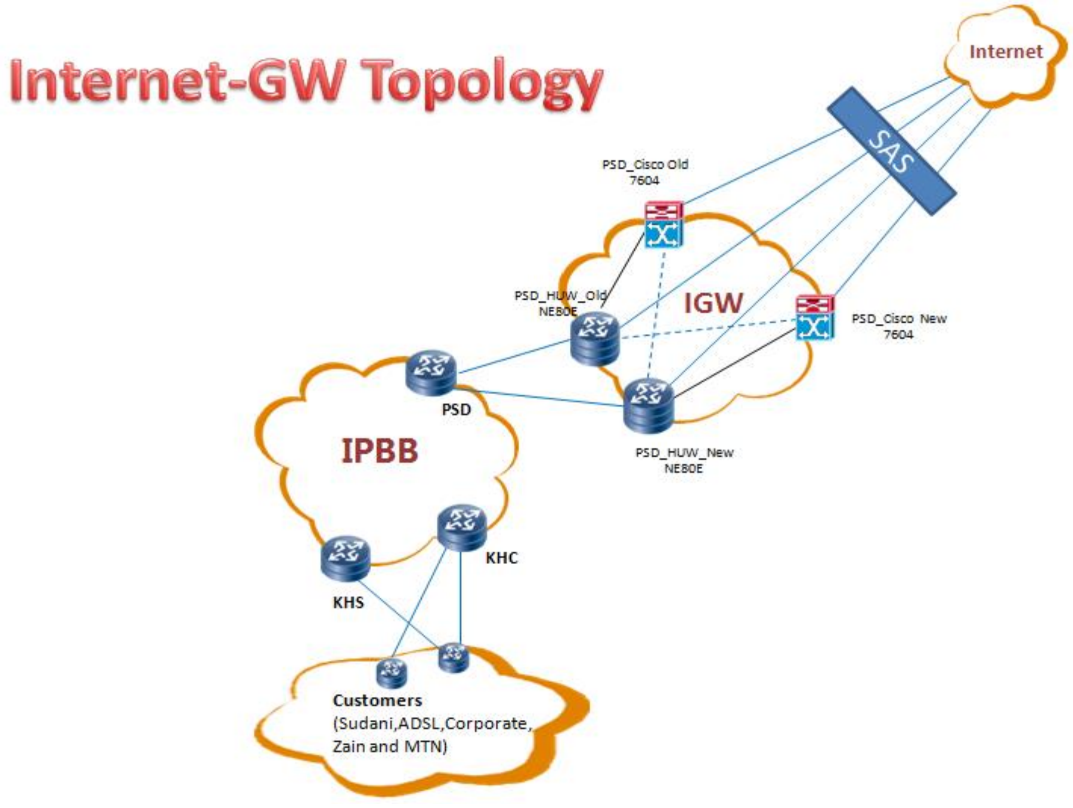


Figure 3.3: illustrates the internet GW topology used by SUDATEL

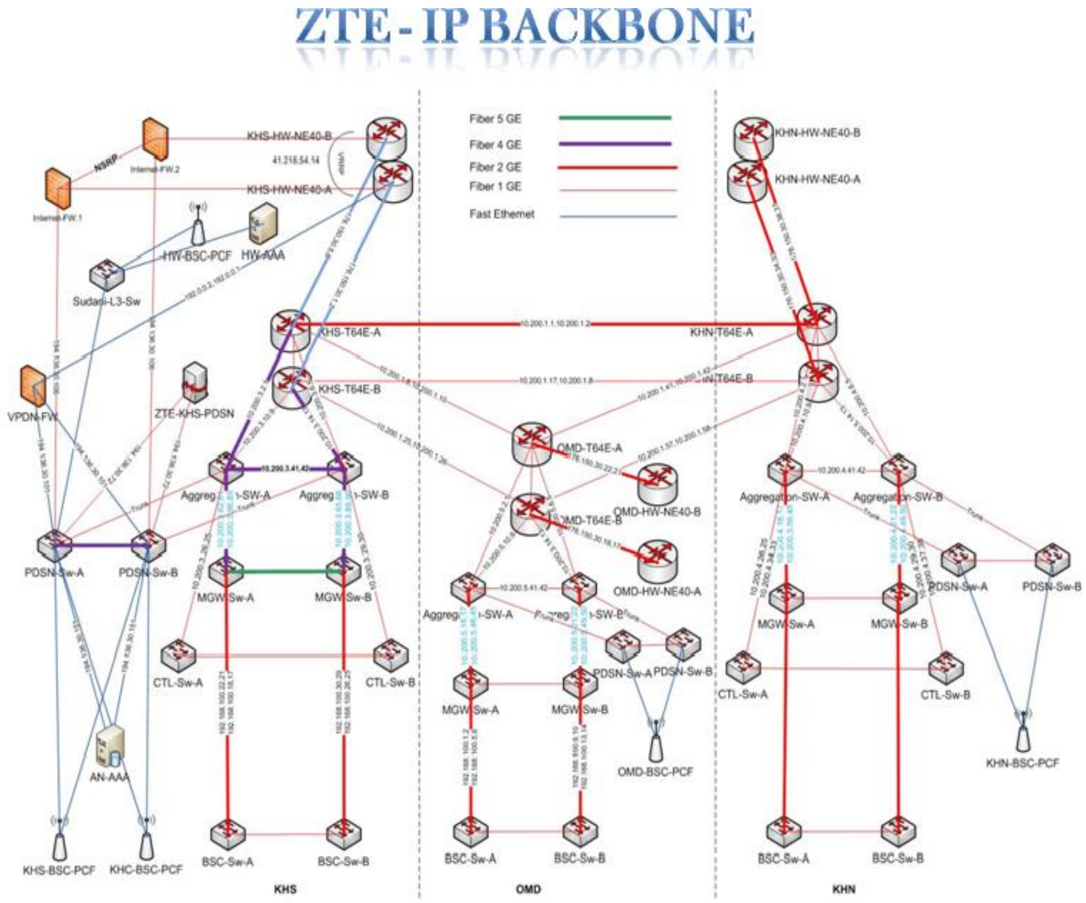


Figure 3.4: illustrates the ZTE IP backbone used by SUDATEL

3.8 Civil Registration System (CRS) in Sudan

CRS presented by the Ministry of Interior in Aug 2011, first describe the strategy a political commitments of developing civil registration and vital statistics system, then talk about the system in detail, followed by associated challenges and conclusion.

The functional scope of the CRS covers the following:

- Registration processing for the citizens and families
- Capture all incidents and events: Birth, Marriage, Divorce and Death.
- Development & maintenance of secured centralized consolidated database/ data warehouse.
- Generation and issuance of National Identification Number and issuance of Citizenship Certificate to all Sudanese nationals, including those holding the old Nationalization Certificates

- Production and issuance of Citizen ID Cards

Civil Registration System (CRS) in Sudan is the Heart of the e-government Systems adopted in Sudan.

3.9 Sudanese in difference with the passwords

Data are collected from freshman students (for the academic year 2014/2015 in Sudan) as a citizen's sample who are use online admission to universities as an e-government services, question was asked them the following question "Do you give passwords to one you trust? Their answers were illustrated as the figure below. The findings revealed that more than 60% do not give their passwords to those who trust them. More than 35% their answers were yes, sometimes. More than 1% said yes. See Figure: 3.5 [171].

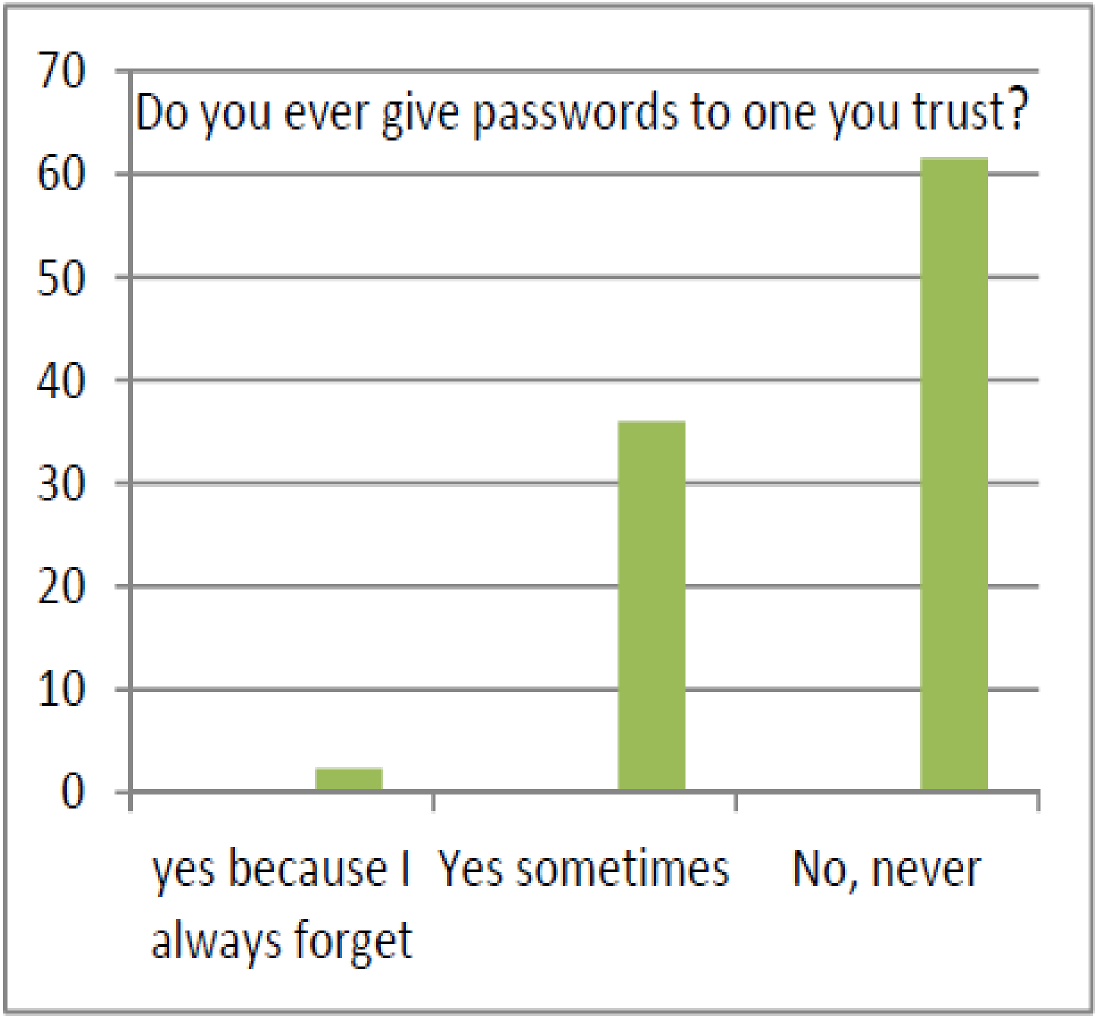


Figure 3.5: illustrates the Sudanese people with passwords

3.10 E-government in Sudan

E-government is a significant objective, if not the most, in the nationally approved strategy for ICT in Sudan. The government recognized the important role that e-government can play in terms of economic and social development and in 2001, the President of the Sudan announced the decision to embark upon e-government. The announcement indicated that the country was ready at the national and organizational level to move forward and make the transformation to the new government paradigm. The mission of e-government in Sudan is to achieve citizens' satisfaction through providing information and services with distinction, transparency and quality; and to contribute in reaching sustainable development. This mission was adopted in the e-government vision which focused mainly on: good governance, social and economic development and ICT utilization [110].

The government was also committed to the e-government aims and objectives highlighted by forums in the African region. Sudan is one of the 19 countries belonging to the foundation, Common Market for Eastern and Southern Africa (COMESA). In December 2007, COMESA developed an e-government framework under the Regional ICT Support Programme (RICTSP). The strategic aim of the project was in targeting effective use of ICT in order to reduce the costs of trade and investment; thereby to stimulate economic growth, reduce poverty, reduce the digital divide and contribute to the regional integration agenda [111].

The e-government project in Sudan is the responsibility of the National Information Centre (NIC). This centre was formed in 2004, and it is in charge of all ICT related projects within government [112]. Initially the centre worked under the command of the Council of Ministers. After the creation of the Telecommunications and Information Technology Ministry, the NIC became one of its administrations.

3.10.1 Stages of e-government in Sudan

Many different stages can be considered in the development of e-government in Sudan. Prior research and our point of view yielded that there are three stages of e-government in Sudan.

Stage one: Getting started stage

This stage started when Sudan developed its National Strategy in 1990s. The strategy is strongly linked to the ICT revolution in Sudan, which led to the dramatic change that took place later in the public sector. This stage faced many barriers due to the lack of understanding of the concepts and potential of e-government. Formal bodies and institutes responsible for e-government implementation were ill equipped and lacked the know-how.

Stage two: Adoption stage

This is the stage where more understanding and commitment were realised. The issues and challenges facing the adoption process started to be discussed at the highest levels of the National Assembly and Council of Ministers. Leaders and policy makers understood the need to approve new legislation and rules in order to organise the implementation of e-government. The vision of moving towards an information-based society was very clear by this time and policy decisions pointed to the necessity of involving ICT curricula (and programmes) in education. Also, ICT training had been provided for all government (including high ranking and senior) personnel.

Stage three: Current stage

The main feature of the current stage for e-government in Sudan is a total change in the mind set of top leaders and policy makers which reflected in the national focus on the development of basic infrastructure, including: the building of schools, universities, hospitals, electricity national grid, high ways, and water dams; in addition to the concern of developing regulatory frameworks and a stable economy and political system. This led to improvement in many area, and particularly in the increase of ICT applications applied in government operations. There are two main decisions that can be considered a turning point in the e- government at this stage:

- The establishment of the Technology and Information Ministry, which helped in raising e-government issues and ICT in general to the highest authorities in government.
- Empowering the NIC through approving its new Act. This act gave the NIC authorization to play the role of supervising, monitoring and coordinating e-government implementation at the national and organisational level. This helped in dealing with the project as a one entity and addressing all relevant issues. The NIC was able to make a balance in the progress of the adoption process by

considering all government institutes and also by focusing on the political, cultural and organisational context in parallel with the technological elements.

3.10.2 Description of e-government current stages in Sudan

According to UN report on e-government development index and world e-government development ranking in the years 2012 and 2014 Sudan index in the year of 2012 was 0.2610 and the world ranking 165. In the year of 2014 the index was 0.2606 and world ranking 154 .According to these figures it seem clear that Sudan has move ahead slowly while most countries in the same region has increased their E-Government value such as Tunisia Algeria and Morocco [39].

3.9.2.1 The projects of e-government in Sudan

There are some public sectors institutes initiated to adopt and implement web services to provide, deliver and disseminate services and information to the public such as the following institutions:

A. Ministry of High Education and Scientific Research e-government project

Ministry of High Education established National Universities Network project with aim of facilitating access to information and delivering services electronically. Therefore, there are two main projects under the National Universities Network project:

- The Sudanese universities information network
- The Sudanese universities virtual library

The goal of these projects is to provide connectivity among educational institutions, increase sharing of knowledge, guide the universities and the institutes to build their information infrastructure and enable digital libraries. This project has serves a large number of students and staff members.

B. Electronic Bank System E- Government project

CBOS (Central Bank of Sudan) in 1999 established EBS (Electronic Bank System) the company introducing technological banking solutions with aim of linking the banks electronically through the country and provide electronic payment services in and out of the country. EBS started its activity in mid 2000 and began project implementation in early 2001. This project results in changing the old bank system to modern fast and efficient bank systems, due to EBS adopted several services such as National Electronic Cheque Clearance, Card Personalization Services and Banking Information Network Services etc.

C. National Electricity Corporation E- Government project

The NEC (National Electricity Corporation) developed prepaid electricity services to eliminate the bills loses due to the old system implementation. With the adoption of the new system the NEC provide every customer with identification card and number to make the services easy and fast, so even the customer can order the electricity through his mobile device. NEC carried out its project and the process of change and use of ICT was introduced in the all departments of NEC.

D. Ministry of Interior e-government project

Ministry of Interior established a company in 2006 in order to introduce e-government initiatives in its work. The Ministry of Interior is concerned with computerizing the police work to gain the technologies advances. The company has two projects which are E-passport and the Civil Registration Record (National ID). As the result of the use of technology in Ministry of Interior daily official work the services delivery to citizens has improved.

Also the Ministry of Higher Education and Scientific Research in academic year 2014 – 2015 decided to computerize the application to higher education institutions.

E. HASSA service

Bank of Khartoum brings the first Mobile Money service in Sudan called “HASSA” that will really revolutionize the way you handle your daily financial needs. Whether its depositing cash, making withdrawals, money transfer, bill payments, mobile air time purchase etc. all of these can be done by either visiting any of the Hassa shops or using your own Hassa Mobile Account. Any person with a valid mobile phone connection can register for this service.

F. GROSHI service

Faisal Islamic Bank (Sudan) published Groshi service that is a service available to the public to make some financial transactions via mobile without downloading an application or open a bank account, where the service works on all segments of Sudanese Telecom regardless of the type of mobile device.

3.11 Research design

This type of research that deals with e-government security is classified within Information Systems (IS) domain. The nature of this type of researches is involve many areas, including technology and management science. The multidisciplinary nature of this type of research made it difficult to select appropriate strategy and research approach.

There are many problems faced during the research process:

- Lack of transparency this type of problems faced when the interview with some government respondents were conducted. They were either not answered or answered with reservations. The information has extracted through indirect ways of addressing the questions over the interviews conducted with some of the security practitioners or IT managers in person or through phone interviews. This indeed increased the time and effort in the data collection phase in the research process
- Lack of the holistic view of the subject matter this type of problem faced during some of the interviews conducted with some of the technology heads of the government departments to explain the purpose of the research it was noticed that the holistic view the security concept was lacking. The importance of information security to the government departments and to the e-government in Sudan is not strongly believed in many government departments.
- Not enough references there are no good references or documents about the evolution of e-services in Sudan.

Research is a systematic process of inquiry to explore and discover knowledge about something happening or existing in society, science or nature [113]. The research methodology as identified by [114], is the procedural framework within which the research is conducted. Some see the research methodology as the approach taken to research. However, the choice of an appropriate research methodology is a basic requirement in order to achieve a final result of high quality [115]. There is no single ideal solution; there are a series of compromises [116], and each research design will have its advantages and disadvantages.

To select the research methodology there are many factors to be considered, as [117], states: “the characteristics of the research inquiry will greatly influence the selection of an appropriate research strategy”. These characteristics include the research topic, the objectives, research questions and nature of the research problem.

The research methodologies may be quantitative or qualitative and also me be mixed type [118]. The choice between the three types takes into account the research goal and objectives to be achieved. According to Cresswell [119] there are three main elements which will needed to reach well designed research. The knowledge claim, the research strategy, and method of the data collection are the main pillars of a good research. As mentioned in Creswell's book that "researchers make claims about what is knowledge (ontology), how we know it (epistemology), what values go into it (axiology), how we write about it (rhetoric), and the processes for studying it (methodology)".

In this research, the knowledge is information security and the need of building a new security model for the e-government in Sudan. The knowledge is obtained from the data collection process during the research study. The value of this research will be reflected through the design security model for Sudanese electronic government. The thesis reflects the overall research process and all the relevant research steps taken. The methodological approach was adopted to reach the final security model.

Researchers who follow the quantitative approach use the post-positivism knowledge Claim. The qualitative approach will reflect the constructivism knowledge claim and it uses narrative, phenomenologies, ethnographies, grounded theories and case studies as strategies of inquires [118].

3.11.1 Qualitative research methodology

The qualitative research methodology was developed in social science to enable researchers to study social and cultural phenomena. It is a method that represents data as narration and is conducted through intense contact with the field or life situation. The qualitative method comprises many attributes; most importantly is that the qualitative data focus is on naturally occurring, ordinary events, in natural settings. Well-collected qualitative data will be rich and holistic, with strong potential for revealing complexity. The qualitative method provides explanations to extend our understanding of the phenomena, or promotes opportunities of informed decisions for social action. It also contributes to theory, policy making and social consciousness [120]. These features help to achieve the goal of understanding rather than prediction of dependent variables [121]. In addition, qualitative research is conducted through an intensive prolonged contact with the field [122], which makes it a powerful method for studying processes. The qualitative method does however, have its weaknesses. The complexity and richness of data can obscure the analysis process. More significantly it leaves the data open to interpretation; both interviewee and researcher bias become a real threat. Finally, the overall situation is dynamic and the case's circumstances can keep changing, which may affect the research validity and verification [123]. Table 3.3 illustrates both strengths and weaknesses of applying the qualitative research method

Table 3.3: Qualitative approach - Strengths and weaknesses

Strengths	Weaknesses
The qualitative analysis allows a complete rich and detailed description.	Qualitative difficult to analyse and needs high level of interpretative skills
An attempt to take account differences between People.	Great chance of bias
Does not reduce complex human experiences to numerical form and allows a good insight into the person's experiences and behaviour.	Hard to draw brief conclusions from qualitative data
Results are said to be rich, deep and meaningful	Qualitative faces difficulties in terms of comparisons
Ambiguities which are inherent in human language, can be recognised in the analysis	Low level of accuracy in terms of statistics

3.11.2 Quantitative Approach

The quantitative method can be described as an extreme of empiricism, which relies on control and explanation of the phenomenon [124]. It is a method that

Tends to measure "how much" or "how often" [125]. Creswell [119] argues that the quantitative approach is most appropriate when the problem is to identify factors that influence an outcome; understand the best predictors of outcomes; or the utility of an intervention. Moreover, in order to perform tests in the quantitative approach, the method has to be expressed in terms of "operation"; such as, surveys, laboratory experiment and mathematical modeling. The analysis of data will depend on statistical principles. Qualitative research is preferred when there is little previous research the phenomenon to be investigated and it needs to be more understood. Table 3.4 illustrates the differences between the two methods in terms of concepts, processes and analysis.

Table 3.4: Qualitative approach vs. Quantitative approach.

Qualitative	Quantitative
It is often an inductive process and the language is informal	It is a deductive process and the language is formal
Can be faster and cheaper compared with quantitative	Can be relatively slow and more costly compared with qualitative
Concepts are in the form of themes, motifs and taxonomies	Concepts are in the form of distinct variables
Analysis proceeds by extracting themes or generalisations from evidence and organising data to present a coherent picture	Analysis proceeds by using statistics, tables or charts
Procedures are particular and replication is difficult	Procedures are standard and replication is assumed

3.12 Research Methods

This section deals with the description of tools and resources used for data collection, and the tools and techniques applied for data analysis.

3.12.1 Data collection

According to Yin and Benbasat [126] there are many deferent methods and tools for collecting data that known as "source of evidence". See table 3.5.

Table 3.5: source of evidence

Source of Evidence	Strengths	Weaknesses
Documents	- Stable can be reviewed repeatedly - Unobtrusive not created as a result of the case study - Exact - Broad coverage	- Retrievability can be low - Biased selectivity - Reporting bias - Access may be blocked
Archival Records	- Same as for documents - Precise and quantitative	- Same as for documents - Accessibility due to privacy reasons
Interviews	- Targeted - Insightful	- Biased due to poor constructed questions - Response bias - Inaccuracy - Reflexivity
Direct Observations	- Reality - Contextual	- Time consuming - Selectivity - Reflexivity - Cost hours
Physical artefacts	- Insightful into cultural feature - Insightful into technical operations	- Selectivity - Availability

The interviews, document reviews and direct observations methods were used to collect data in this research.

3.12.1.1 Interviews

Interviews were conducted with people involved in e-government in Sudan; specialist in National Information Centre (NIC), private sector, academic and professionals. The aim of this interviews were to reveal the security threats that faced the Sudanese e-government. The analysis of these interviews resulted in a significant revision of the conceptual framework, which led to the identification of a list of security threats. See table 3.6 to show the conducted interviews and its information.

Table 3.6: shows the conducted interviews

	Interview	Duration	Type
National Information Centre (NIC)	General Director/ (NIC)	4 Hours	Face-to-face
	Head/ E-government Master Planning Committee	4 Hours	Face-to-face
	Head/ Training Department	4 Hours	Face-to-face
	CEO/ (NIC)	4 Hours	Face-to-face
National Telecommunication Corporation	Director General	4 Hours	Face-to-face
	IT and Information stuff	4 Hours	Face-to-face
The National Committee for e-authentication	Chairman of the Committee	4 Hours	Face-to-face
	Chairman of the Group Executive	4 Hours	Face-to-face
Academic	Staff/ Faculty of Computer Studies/International University of Africa	2 Hours	Face-to-face

Professionals		2 Hours	Face-to-face
SUDATEL	Development projects staff	5 Hours	Face-to-face
Civil Registration	Developer staff	4 Hours	Face-to-face
Governmental companies	General Manager	1 Hour	Face-to-face
Ministry of the Interior	director of computing	1/2 Hour	Telephone
Ministry of Higher Education and Scientific Research (MHESR)	Head/ Consultancy Committee.	½ Hour	Face-to-face
	CEO/ Consultancy Committee	2 Hours	Face-to-face
National Electricity Corporation (NEC)	General Director/ (NEC)	1/2 Hour	Face-to-face
	Director/ Statistics & Information Department	3 Hours	Face-to-face
	Director/ Communication Department	4 Hours	Face-to-face

3.12.1.2 Documents

The advantage of using documents is that they are stable and can be reviewed repeatedly. The documents included: white papers, studies, minutes of meetings, policies and strategies, presentations, reports, project plans and reference materials available on the internet. See table 3.7 shows the documents used in this theses.

Table 3.7 shows the documents used in this research.

White paper			
No.	**Document Name**	**Year**	**Source**
1	Five-Year Plan for the strategy of the knowledge society (2007 – 2011)	2007	National Council for Strategic Planning
2	E-government master plan	2007	National Telecommunication Corporation
3	National strategy	2001	National Council for Strategic Planning
4	Quarter national strategy for ICT industry	2001	National Council for Strategic Planning
5	The directing plan for e-government	2009	National Telecommunication Corporation
6	The NIC Act	2010	National Telecommunication Corporation
7	The NIC in brief	2010	National Telecommunication Corporation
Studies and Presentation			
No.	**Document Name**	**Year**	**Source**
1	Towards e-government in Sudan	2007	Council of Ministry
2	NIC governmental websites evaluation	2007	National Information Centre
3	Sudan digital magazine	2011	National Information Centre
4	Developing internet services in Sudan	2007	Sudan Internet Society
5	Internet issues	2007	National Telecommunication Corporation
6	The national ICT report	2011	Ministry of ICT
Websites			

	• National information centre • Council of ministries • ICT ministry • National telecommunication Corporation • Sudatel • National digital certification		

3.12.1.3 Observations

Observations were recorded using notebooks. Notes are useful to bridge any gaps existing in the other tools of data collection. Observations are a rich source of data about the research problem, the participants, the location, and so on [137]. Observation becomes a scientific tool and the method of data collection for the researcher, when it serves a formulated research purpose, is systematically planned and recorded and is subjected to checks and controls on validity and reliability. Under the observation method, the information is sought by way of investigator’s own direct observation without asking from the respondent [138].

3.12.2 Data Analysis

According to Yin [117] there are many ways to analyse data in the quantitative approach, but fewer in the qualitative approach, which are also less well formulated. However, the literature describes approaches of analysis such as: content analysis, thematic, comparative and narrative. Thematic and comparative are often used for analysis in the same project. The former identifies emergent themes from data and the latter contrasts and compares themes between different people or groups. Content analysis has been recognized for over 50 years [127] and is widely used as an analysis tool in qualitative research [127] Krippendorff [128] defines content analysis as: "the use of replicable and valid method for making specific inferences from text to other states or properties of its source". Some suggest that content analysis allows closeness to the text, which can provide valuable cultural visions and/or understanding of human thought over time.

3.13 The implemented research methodology

Implemented the research methodology consists of series of actions or steps necessary to effectively carry out research and the desired sequencing of these steps. The chart shown in Figure 3.1 well illustrates the implemented the research methodology. The following section describes each step.

3.13.1 Step 1: Conducting the preliminary study, SWOT analysis and identifying the research problem to achieve the research objectives

After establishing the research background, a pilot study was conducted with state e-government authorities and IT professionals; academics. The findings from preliminary study directly contributed to building the initial conceptual framework. Additional data was gathered through informal dialogue, government agency websites, publications and articles highlighted issues and challenges related to a variety of aspects; IT infrastructure, managerial, legal and technical. This was then collated with the interview data and analyzed using the SWOT tool of analysis.

3.13.1.1 Preliminary study

The purpose of the preliminary study is to collect information prior to the full research study. The information may be limited, but it is usually valuable and sufficient to help to identify the research problem. This preliminary study conducted with the goal of finding out how e-government security model in Sudan started; why designing of security model for Sudanese e-government is important; and what is expecting security model of Sudanese e-government. The preliminary study found that government transformation and adoption of the new technology was shaped by the IT infrastructure issues, managerial issues, technical issues and low and legislations issues. The aim of the research was refined to provide guidelines and direction, to help in the decision making process, through developing conceptual framework and then final security model. The findings from preliminary study directly contributed to building the initial security model. The study took place in Sudan on August 2010, during which time more than 20 open-ended interviews were conducted. As the interviews were aiming to understand perceptions and views in order to build the big picture.

The preliminary study found that there are four types of threats (challenges) that faced the e-government security in Sudan, and each type of the threats composed of many factors that affected to it. The information about security of e-government in Sudan was gained from the interviews with experts & consultants, officials, IT professional, and academic.

3.13.1.2 SWOT Analysis

SWOT Analysis is a useful technique for understanding the Strengths and Weaknesses which is represent the internal factors, and Opportunities and threats which is represent the external factors.

The main purpose of SWOT analysis achieve the aim of the preliminary study. The SWOT provides the necessary outlines to identify the research problem and research aim.

Strengths

- The government has granted licenses to several Internet Service Providers (ISP). The country's new policy aimed at encouraging the private sector by means of providing ICT investment in different areas.
- The formulation of the 25 year national strategy. The strategy had a clear vision for achieving an informatics society, strongly supporting the development of ICT and designating that it should be involved in all segments of the economy.
- This ICT strategy represents the starting point of the telecommunications revolution in Sudan. A modern telecommunications infrastructure was established and expanded all over the country, creating communication networks in most parts of Sudan.
- Establishing the National Information Centre (NIC) as a consultative body in the State in the field of IT, and electronic government projects.
- Establishing National Committee for electronic authentication
- Establishing the civil Registry that represents the number of individuals, common institutions, common symbol of economic, social activities, and project works in one system underlying the rest of the systems. E-government security basically depends on the civil Registry.

Weaknesses

- The poor economy is considered as the number one obstacle to ICT projects. The country lacks basic infrastructure and the general budget is unable to cover the basic needs of citizens.
- The long wars and many conflicts in different parts of Sudan, the national disputes causing major social and economic problems, in addition to the great number of refugees and displaced persons, have all distracted the attention of politicians and senior leaders. Moreover, the embargo and sanctions against Sudan led to the isolation of the country and weak relations with the international community. This prevented Sudan from having any role in the global network economy.
- Lack of resources exists in many areas, but the lack of ICT skills and well trained staff had created a lot of resistance. On the other side the public sector keeps losing the well trained and professionals in the IT field, due to low income.
- Despite the huge efforts and progress in the telecommunications infrastructure, it is still lacking essential components and it is far from satisfying the needs of the ICT market in the country. Many aspects of ICT technology are still very weak and the digital divide is huge across the country, being much worse in the rural areas and civil war zones.

Opportunities

- The e-government initiatives in education and banks, and e-payments services that published by Khartoum bank and Kink Faisal bank.
- The economic conference held in Sudan in 1999 that recommended privatizing the communications and information sector in Sudan, provided the opportunity to the private sector to launch initiatives, revive the telecommunications sector and modernize it. Moreover, it is creating a competitive market for ICT components and lifting standards in the sector.
- The open nature of e-government provides a golden opportunity for Sudan to make itself known to the outside world and remove some of its isolation. If the new environment of e-government is well utilized it can help in building new channels for relations and networks, in addition to facilitating information and knowledge exchange and transfer.

Threats

- The embargo and sanction on Sudan since 1996 that reflected on the information security in Sudan which leads to the use of open access software's in the websites design and development which leads to unreliability in the infrastructure.
- Lack of Software houses
- Lack of budget
- The continuous and rapid growth of ICT technology can be challenging for Sudanese institutes and public organizations to cope with in terms of training, adoption and implementation. Ultimately this will lead to a wider digital divide.
- Lack of Policies and find mechanisms to enforce it.
- Willingness to change in top management and administration.
- Conflict of interest.
- Lack of Low and legislation
- The consequences of political instability in the Middle East and neighboring countries could always be a threat for the economy and political situation in Sudan. In addition there is uncertainty in relations between Sudan and the international community, which may lead to more sanctions and continued isolation.

3.13.1.3 Research problem

The research problem was specified in the early stage of the research study. The main objective of this research was to find a security model for Sudan e-government which allows any e-organisation or entity to exchange information with other entities smoothly considering all the elements or factors which will hinder this communication or lower the trust of information sharing between these entities.

3.13.1.4 Research objectives

The main objective of this research is to design suitable security model for Sudan e-government.

3.13.2 Step 2: Reviewing the literature

The literature review explaining the existing security models addressing policies and the security triad (confidentiality, integrity, availability) which act as the high level objectives of any security architecture or model. Different types of models were analyzed. Models addressing confidentiality or integrity only were such as BLP or Biba were analyzed. Social and human behavioral model and theories were searched to build the concept of the human aspect in the information security field. In addition, e-government assessment and stages of growth, models and frameworks developed in e-government and other disciplines (IT and IS) were thoroughly reviewed. The review of the literature led to different ideas on how to pursue constructing the new model. More significantly, was the deep review of the key issues that impact upon the adoption of new technology in general, and e-government innovation in particular; such as, organizational and environmental issues. The majority of the literature was addressing technological security solutions or approaches to solve issues related to data integrity or confidentiality. These technological solutions were presented as architectures required or programmes to be installed in the IT infrastructure.

3.13.3 Step 3: Developing a conceptual framework

After identifying the research problem and reviewing the related literature the initial framework was provided. The framework is based on the IT infrastructure, managerial, legal and technical. The framework and its critical factors according to the initial findings from the SWOT analysis of the preliminary study, combined with the identified factors and key elements from the literature review were constructed. The development of the conceptual framework step is a major step in theory building and it is considered a type of intermediate theory (Carroll and Swatman, 2000), that attempts to connect all aspects of inquiry (problem definition, purpose, literature review methodology, data collection and analysis). The development of the initial conceptual framework will help develop understanding of the research problem and lead to the developing the final model.

3.13.4 Step 4: Developing the final model

In this step of research the details of each category of challenges and barriers to e-government in Sudan were specified according to its source. The information which was collected from interviewees, observations and documents were formulated into layers, and then these layers were focused studied to provide sub-layers into each category of the layer.

3.13.5 Step 5: Validation

In this step three actions been implemented in the same time.

Action 1: According to specialists, literal review, and documents the security layers and sub-layers that mentioned in this research were specified.

Action 2: The criterias that extrapolated from Wood's book [129] for the success of the model were set and the guidelines of modeling presented by Lankhorst [130] were followed.

Action 3: Evaluation some academic and specialists. See the evaluation form appendix B.

3.13.6 Step 6: Drawing conclusion

This is the final step of the implemented research methodology. See figure 3.6.

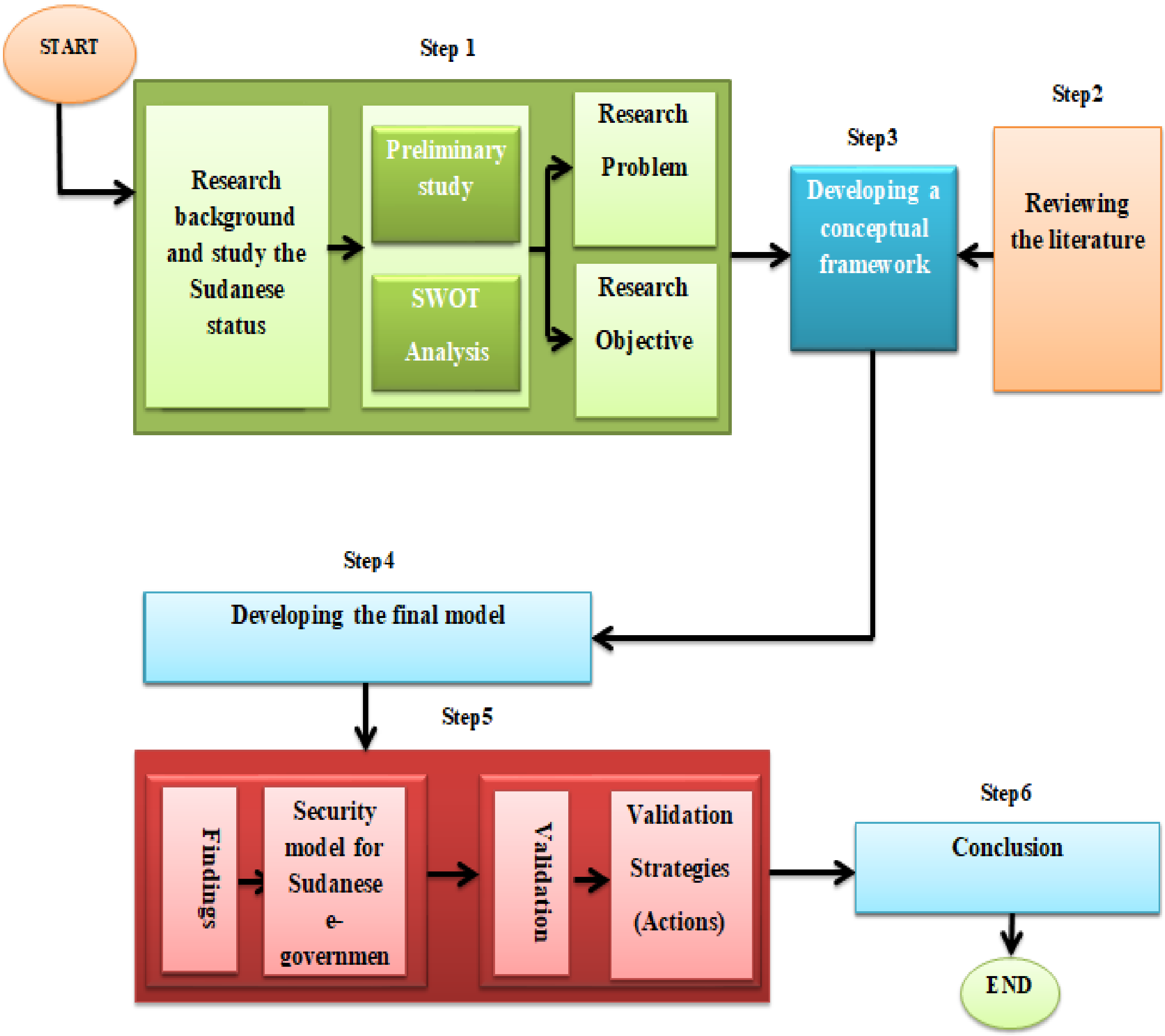

START
Step 1
Research background and study the Sudanese status
Preliminary study
SWOT Analysis
Research Problem
Research Objective
Step3
Developing a conceptual framework
Step2
Reviewing the literature
Step4
Developing the final model
Step5
Findings
Security model for Sudanese e-governmen
Validation
Validation Strategies (Actions)
Step6
Conclusion
END

Figure 3.6: shows the implemented research methodology

3.14 Preliminary study findings

The main findings of this study are summarised in Table 3.8. The description of each element of the SWOT analysis is presented as follows:

S	**W**
• Clear vision and objectives of national ICT strategy • Founding of modern Telecommunications infrastructure • Competitive local IT companies • Investing of private sector in the telecommunications sector • Political supporting	• Digital divide • Low awareness among citizens & political leaders • Lack of budget • Lack of IT management • Computer illiteracy • No security control • Weak effect of legislation & policy • No clear measurements and evaluation • No priorities in implementation • Wide multi-culture and multi-language society • Resistance to change • Slump of the economic in Sudan
O	**T**
• Improving quality of life through building an information-based society • Information and research opportunities • Regional influence, especially in Arab and African countries • Linking local and government departments with the centre • Increase in investment • Exchange of information • Role for business and private sector • Creating a knowledge-based economy	• Cannot cope with IT development • Cannot satisfy market demand • No guarantee for sustainable financial banking • Losing key staff • Unstable political conditions

3.15 Before starting to create the model

When about to create any model there are questions should be answered. Here in this section the questions and their answers were listed. [141] The validity of the model was started from here. See table 3.9.

Table 3.9: The questions and answers before creating the model

Questions	**Answers**
Is there a clear stakeholder?	Yes, all Sudanese peoples.
Is the objective explicit?	Yes, the objective to design security model for Sudanese e-government.
Will creating an enterprise architecture model (here e-government security model for Sudanese e-government) help to reach this objective?	Yes, because there are various types of threats and there countermeasures.
Are the boundaries clear of what you should model?	Yes.
Is it clear whether the situation ‘as is’ or the situation ‘to be’ should be modelled?	Yes, the situation should be modeled.
Can you obtain the information needed to create the model?	Yes, from its sources.
Are there realistic expectations regarding your role as an enterprise architect in the process?	Yes.

3.16 Summary

This chapter gave a general overview of Sudan and revealed the complexity of the cultural mix and unstable political conditions. It also demonstrated that the economy is turning from poor to fast growing, with the telecommunications sector playing a pivotal role. The chapter also highlighted the history of introducing ICT, the main projects and achievements, and explained the status of e-government Sudan. The information obtained from this chapter is carried on to the next phase of the research, as a guideline towards the proposed security model, the implemented research methodology, the methods of data collection, and the validation process followed during the construction of the thesis for the new security model.

CHAPTER IV

RISK ANALYSIS

4.1 Introduction

As is well known, e-government represents a fundamental change in the whole public sector structure, values, culture and the ways of conducting business by utilizing the potential of ICT as a tool in the government agency. Government in Sudan must make a serious efforts to complete the construction of e- government project. According to the interviews with specialists in National Information Centre that is responsible for e-government projects in Sudan, observation, and documents there are several types of challenges and barriers or risks that may impede the development of e-government adoption in Sudan. In order to provide a clear view of these threats that form the risks facing e-government in Sudan, threats were categorized according to their sources to four types and divided into technical and non-technical threats see figure 4.1. The aim of this chapter is to review the threats of implementation of e-government in Sudan.

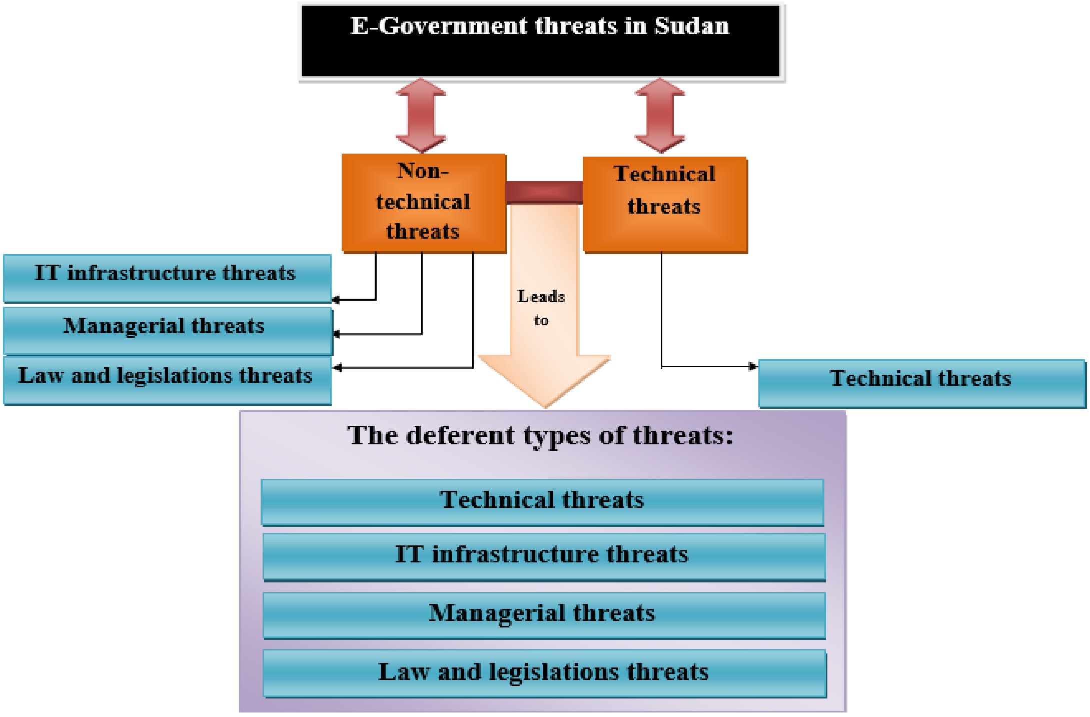

E-Government threats in Sudan
Non-technical threats
Technical threats
IT infrastructure threats
Managerial threats
Law and legislations threats
Leads to
Technical threats
The deferent types of threats:
Technical threats
IT infrastructure threats
Managerial threats
Law and legislations threats

Figure 4.1: shows the classification of the e-government threats in Sudan

4.2 Risks, assets, threats and vulnerabilities

To implement the necessary security measures it is necessary to identify and evaluate the system assets, the associated threats and vulnerabilities, as well as to assess the consequences from a potential security incident [131]. Before setting security measures within e- government services, an analysis must be performed to determine [131]:

- The assets that require protection.
- The corresponding types of threats and their probability of occurrence.
- The potential sources of threats.
- The cost from damaging the assets.
- The set of system vulnerabilities.

Risk can be described as the potential of a threat to exploit a vulnerability found in an asset [132]. A risk exists when there is a possibility of a threat to exploit the vulnerability of a valuable asset. That is, three elements of a risk are *asset, vulnerability* and *threat*. The value of an asset makes it a target for an attacker. The vulnerability of an asset presents the opportunity of a possible asset damage or loss. A threat is a potential attack which can exploit a vulnerability to attack an asset [131]. The measure of risk can be determined as a product of threat, vulnerability and asset values as shown in the formula below:

$$Risk = Asset \times Threat \times Vulnerability \quad \ldots\ldots\ldots. (4.1)$$

The risk elements and their corresponding countermeasures can best be visualized with a figure (4.2) [133].

Risk Management this refers to the process of identifying, assessing and controlling risks that may result in financial loss or organizational impact in the outsourcing process [133].

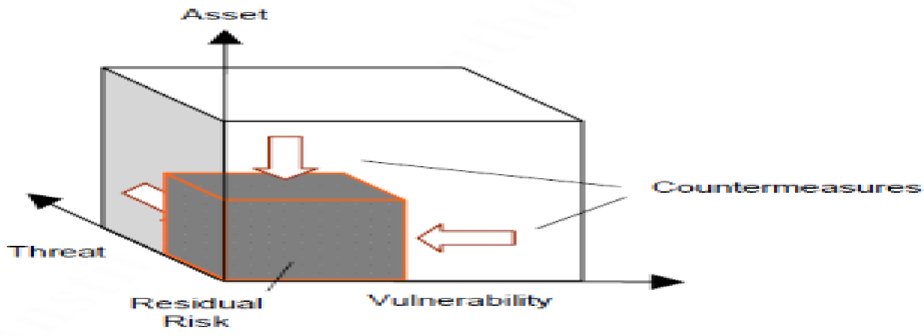


Figure 4.2: Risk as a function of asset value, threat and vulnerability

4.2.1 Estimate level of risk

The standard method of calculating the level of risk is multiplying the threat level by vulnerability weight, divided by the level of countermeasures available to protect the infrastructure and multiplied by the impact (equation 4.2). This method depends highly on knowing vulnerabilities and impacts on an asset. The two equations below reflect the standard method of calculating risk [133].

$$\textit{Level of Risk} = ((\textit{Threat} \times \textit{Vulnerability})/\textit{Countermeasures}) \times \textit{Impact} \ldots\ldots \quad (4.2)$$

$$\textit{Total Risk} = \textit{Vulnerability} + \textit{Threats} + \textit{Asset Value} \ldots\ldots\ldots\ldots\ldots\ldots \quad (4.3)$$

Without a threat agent, vulnerability, or an impact, there is no risk [132].The risk calculation can be described as follows:

$$\textit{Risk} = R(A,T,V\,) = R(L(T,V), F(Ia,Va)) \ldots\ldots\ldots\ldots\ldots\ldots \quad (4.4)$$

Where *R* is the function (a complex function, not a linearity relation.) of risk of security evaluation, *A* is asset, *T* is threat, *V* is vulnerability, *Ia* is the value of asset occurring security events, *Va* is the degrees of the vulnerability, *L* is the possibility of risk event caused by a threat agent according to the vulnerability of the information system, F is the damage caused by the risk event [132].

4.3 Challenges and Obstacles (Threats) in e-government in Sudan

There are several challenges or risks that can delay progress towards realizing the promise of e-government in Sudan. The variety and complexity of e-government initiatives implies the existence of a wide range of challenges and barriers to its implementation and management. This section, will categorize the challenges and barriers to e-government in Sudan according to its source to four categories: IT infrastructure, managerial, legal and technical category and each category contains a group of points. See figure 4.4 below. According to the questionnaire conducted in appendix (A) the threats affecting Sudanese e-government security and it’s percentage was specified. See figure 4.3.

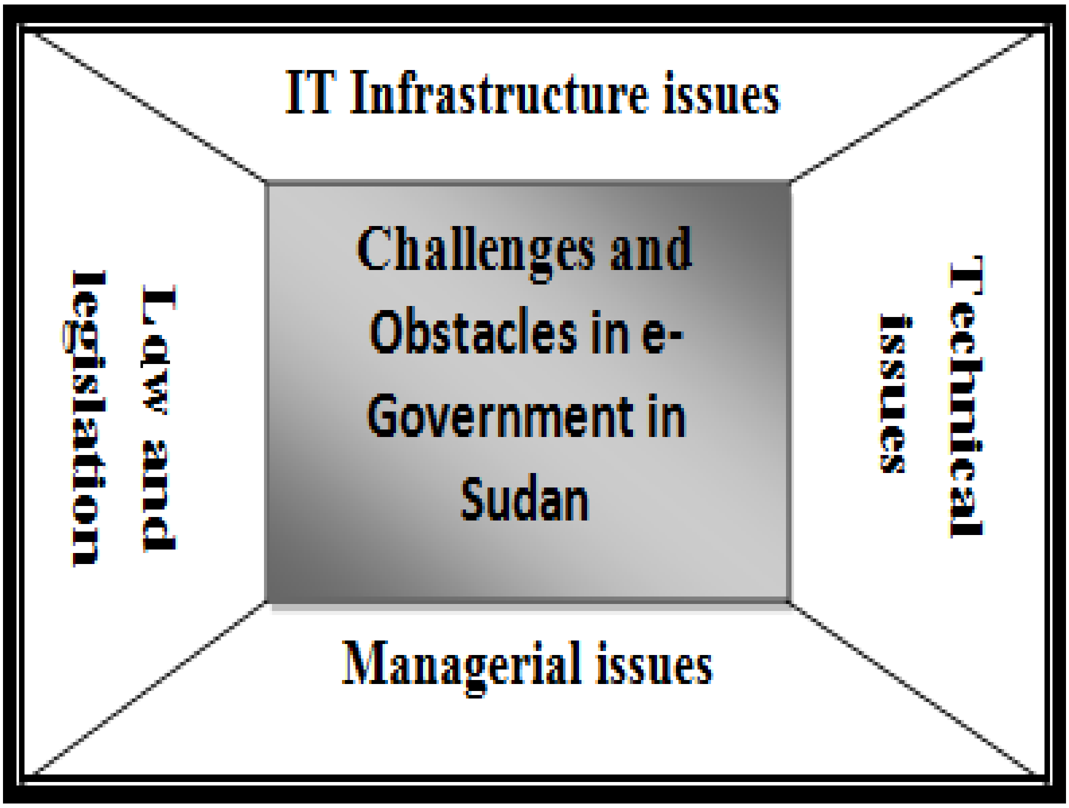
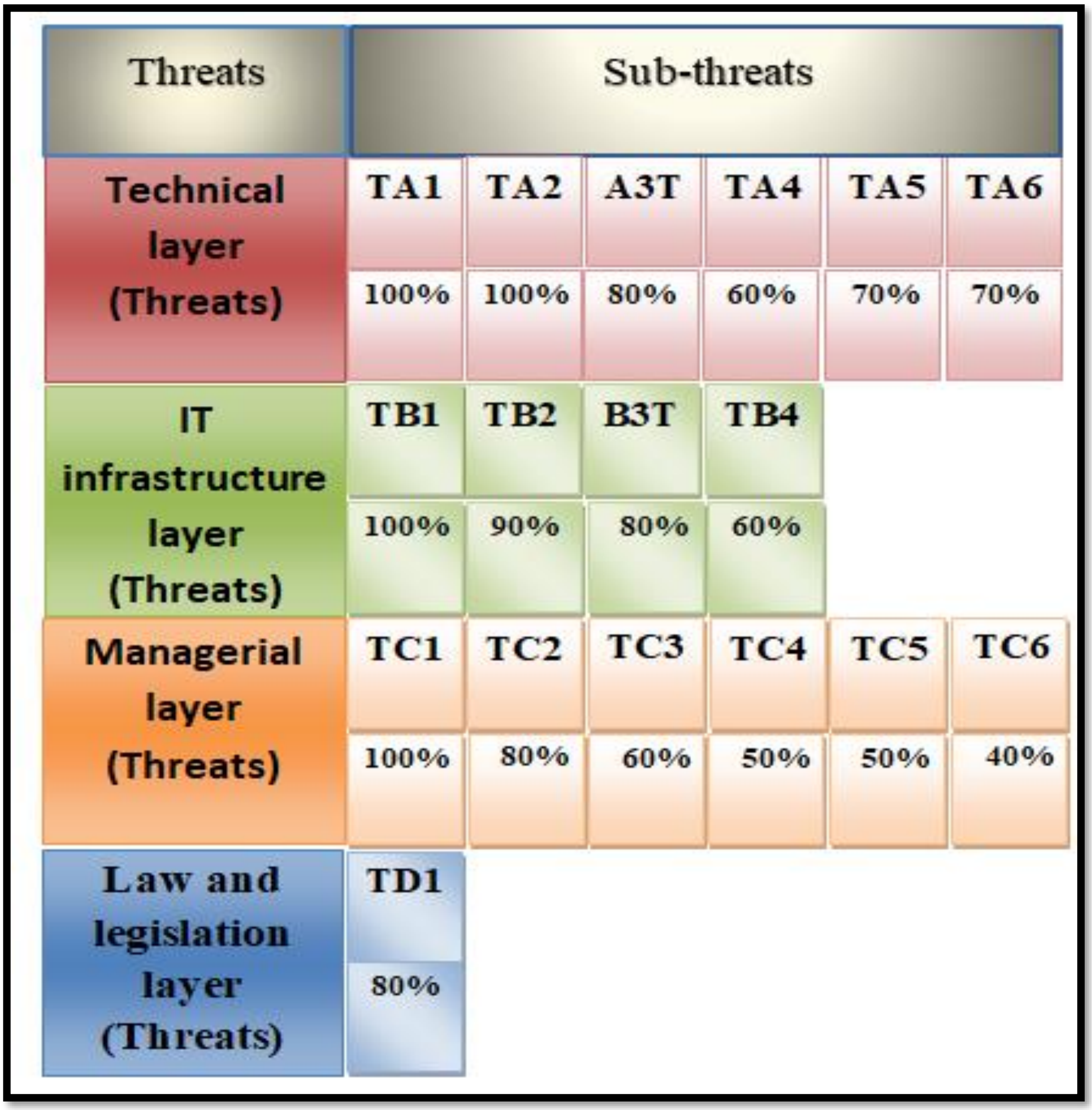


Figure 4.3: This figure shows the Challenges and Obstacles in e-government in Sudan framework

4.4 Questionnaire analysis

After the analysis of the questionnaire -in appendix A- and the correlation questions related to the layers of the model, it has been observed that all the layers were required and selected by both the security practitioners and the government departments management surveyed. The selection was based on understanding the needs of different aspects of protection and correlation between the threats and the security measures required in any government departments.



Threats	Sub-threats					
Technical layer (Threats)	TA1	TA2	A3T	TA4	TA5	TA6
	100%	100%	80%	60%	70%	70%
IT infrastructure layer (Threats)	TB1	TB2	B3T	TB4		
	100%	90%	80%	60%		
Managerial layer (Threats)	TC1	TC2	TC3	TC4	TC5	TC6
	100%	80%	60%	50%	50%	40%
Law and legislation layer (Threats)	TD1					
	80%					

Figure 4.4: Show the threats affecting e-government security and it's percentage

4.3.1 IT infrastructure issues

According to specialists in National Information Centre (NIC) which is a responsible body for e-government project in Sudan, there are many detailed points related to this issue.

4.3.1.1 Lack of skills

Many of people whom have skills in IT sector in Sudan have has immigrated to Arab States the reason is the low salary and income.

4.3.1.2 Lack of users' trust and confidence to use e-government services

The embargo and sanction on Sudan since 1996 particularly the technological sanction led to the country isolation and has great impact on influencing the country ICT and its projects development which e-government is one of them. And also this technological sanction have affected Sudan ability to import technology and industrial infrastructure necessary for the growth of its productivity. The impact of this sanction reflected on the information security in Sudan which leads to the use of open access software's in the websites design and development which leads to unreliability in the infrastructure. According to Edrees R. and Khalifa O. [178] study there are 48.1% agreed on lack of users’ trust and confidence to use e-government services in Sudan.

4.3.1.3 Lack of consultation issues

Management consultancy for e-government is a new and emerging field. It has certain unique features that distinguish it from other types of management consultancies, most notably that in management consultancy for e-government, the management consultant is also a hidden stakeholder as a citizen and thus can, and should, very successfully look after the interests of both the state as well as the citizens [139],[136].

The main goal of consultation in large scale projects like e-government project is to improve all technical issues that related to e-government project. But in case of Sudan there are lack of consultation, because of embargo and technological sanction, and also immigration of professional in the IT field due to low salary. All these previous factors led to lack of consultation in Sudan.

4.3.1.4 Lack of software houses

There are many software houses in Sudan but it is inappropriate to achieve or support e-government project. Most of Software Development Companies in Sudan are classified to be of small size compared with international Companies. Software Development Companies in Sudan has lack financial, organizational, and human resource necessary to manage and improve variety of activities. Software Development Companies in Sudan need to be acquainted with differentiated knowledge about best practice adoption through various co-operative strategies with international Companies and institutions in order to cope with the rapid improvement in the field of Software Development [139], [136].

4.3.2 Managerial issues

There are fundamental changes that have to take place in the mentality of decision makers in Sudan, they should be more aware to enable e-government project. These changes are often met with great fear and resistance by employees who can easily slow down the implementation of e-government.

4.3.2.1 Lack of budget

E-government systems require considerable financial resources: resources must be allocated to developing and managing systems, building up technical infrastructures, and coordinating systems and initiative [140],[136].

E-Government project is mega projects, budgeting should be taken into account, each stage of the project needs the money, each program the government intends to work need the money, and provide all sources for the purposes of the project needs the money.

4.3.2.2 Lack of policy and regulation for e-usage in Sudan

There are huge lack of protection and enforcement of policies placed on most organization in Sudan because of the lack of a mechanism to support these policies that could be due to the favoritism. According to Edrees R. and Khalifa O. [178] study there are 42 % of Sudanese people agreed with lack of policy and regulation for e-usage.

4.3.2.3 Resistance to change in top management and administration

E-government project is needed well care from the top of the pyramid in the administrative. E-government cannot be implemented without supported, sponsored, and commitment of top leadership.

4.3.2.4 Conflict of interest

One of the benefits that gained by using e-government project is the transparency which is rejected by some employees in some organizations in Sudan, so there is a strong resistance to implement e-government project.

4.3.2.5 Social engineering attacks

Social relations take an effective role in the community of Sudan, so the employees of e-government must be aware to the risk that may be come from this type of attack. Social engineering exploits human nature and human behavior. Social engineering attacks are particularly dangerous for users and the threat of it can also be seen when dealing with physical security.

4.3.2.6 Lack of physical security

Physical security is the term used to describe protection needed outside the computer system. Typical physical security controls include guards, locks, and fences to deter direct attacks. Physical security emphasizes the need for security of computers running the Web servers and how these machines should be kept physically secured in a locked area. Physical security is applied to prevent attackers from have a facility to gain data stored on servers, computers, or other mediums. Physical security comes in many forms including site design, access control devices, alarms and cameras.

4.3.3 Law and legislation issues

The legislation concerned with e-government is new in Sudan, it is not an old pursuit which is solidified by practice. Therefore there is no national legal framework developed for the purpose of regulating e- government implementation in Sudan. E-government needs legislation to be prepared prior to the implementation phase, but many acts and laws related to e-government and ICT have only been approved relatively recently. It is also crucial for the success of e-government initiatives to develop legislative protection in order to reassure citizens.

4.3.3.1 Legal Framework

The NIC Act (1999), did not contain any reference to, or authorisation of, e-government. The new Act (2010) passed by the Council of Ministries gave authority to the NIC to coordinate the e-government project. The Act authorised the NIC to establish IT units in public organisations, to coordinate with it and collect data from a variety of sources. The Act also permitted the NIC to access to information stored in data centres.

There is no national legal framework developed for the purpose of regulating e-government implementation in Sudan. E-government needs legislation to be prepared prior to the implementation phase, but many acts and laws related to e-government and ICT have only been approved relatively recently. It is also crucial for the success of e-government initiatives to develop legislative protection in order to reassure citizens. This increases their confidence in organisations which use the Internet, as this is still culturally new. It has been reported:

“The legislation concerned with e-government is new … it is not an old pursuit which is solidified by practice, it is dynamic and wide in scope … Therefore, it is important because of every movement in this field.”

The recent acts and laws covered important issues which have direct influence in the adoption of e-government, as shown in Table 4.1.

Table 4.1: shows the status of law

Law	Status
Law of National Telecommunication Authority	adopted
Law of National Information Centre	adopted
Law of Science and Technology Minister	adopted
Law of Computer Crime – 2007	adopted
Electronic transaction Law	To be approved
Information Access Law	To be approved
E-authentication Law	To be approved
Computational Methods Profession and Employees	To be approved

4.3.4 Technical category

Technical issues have important role in securing the systems and applications supporting the e-government. Technologies such as Intrusion Detection, Antivirus, Cryptography, Digital Signature and security protocol contribute to the success of the e-government application by providing the users high trust. Not having all or some of the security measures will have a negative impact and can be considered as a threat on the e- government application.

4.3.4.1 Risk analysis for the technical issues

Generally there are three steps to manage the risks that e-government security is facing, first step is identifying the risk, second step is analyzing the risk, and the third step is controlling the risk. The e-government application which is based on internet meets fatal security problems due to the complexity and vulnerability of networks. These risks are:

Information interception: An information interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

Information tampering: An information tampering is modification on original data by internet attackers through various technical methods.

Services denying: service denying is an incident in which a user or organization is deprived of the services of the resource they would normally expect to have.

System resources stealing: The stealing of the system resources is very common in the network environment.

Information faking: It means that after the attackers know the rules of the data in the network information or after they have decoded the government information; they could pretend to be legal users or make false information to cheat other users. The main forms include pretending users to get illegal certifications, forging e-mails, etc.

- Risk identification

The main purpose of security risk identification step is to recognize risks existing in the network environment, and data or data exchange. Finding the source of security risk is very important issue to use a suitable method to countermeasure it. There are many categories of security risks sources.

Persons with purposes: It caused by terrorists, criminals, hackers, and people who dissatisfied with the organization, or has a mental imbalance insiders who colluding with alien enemies.

Persons without purposes: This type caused by mis-operations from system users mis-operations from system chargers or protectors.

Natural factors: It caused by earthquake, volcanic eruption, hurricane, flood, and thunder and lightning.

- Risk analyzing

The final goal of risk analyzing step is to figure the general risk probability. The factors influencing risk probability include motivations and ability of risks source, system vulnerabilities, and effect of relative security measures. For the securities risks from people with certain purposes, some possible motivations are listed in next paragraph:

- obtaining access privileges of secrets or sensitive data
- tracking or monitoring the operations of target system
- disturbing the operation of target
- stealing money, things or services
- using resources without authorization (such as computers, website resource and so on)
- technology challenges
- curiosity

There are many ways to obtain information about vulnerability like investigation network scanning, and penetration testing, etc.

Also there is a simple method to describe the risk probability according to the risk resource level which is high, medium, and low.

High: in this level risk source has high motivation and ability, security measures are invalid.

Medium: in this level risk source has some motivation and ability, but security measures are effective; or risk source does not have motivation; or it does not have obvious ability.

Low: in this level risk source lacks of motivation and ability, security measures can keep vulnerabilities from attacking effectively.

- Risk controlling

Risk controlling is the most important step in the risk management. The goal of e-government security risk controlling is to reduce the risk probability. Generally speaking, there are two kinds of risk controlling methods. First kinds are risk controlling measures, such as risk reducing, avoiding, or transferring, and losses managing. Second kinds are measures funding for risk compensation, which include insuring, or taking risk by oneself.

4.4 Summary

This chapter has identified many types of challenges and obstacles facing the e-government in Sudan. And also has identified the technological risks that effected the e-government in Sudan.

The information obtained from this chapter is carried on to the next phase of the research, as a guideline for security requirements for e-government in Sudan.

CHAPTER V

SECURITY REQUIREMENTS

5.1 Introduction

Any security model depend on levels or layers in its structure is a robust and better success rate in preventing organizations from various categories of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services.

The proposed security model for the Sudanese electronic government is a four layers model that is divided into sub layers. The model is not generic and cannot apply by other countries. It designed for Sudanese situation.

The sub layers of each layer or level needed in any information security system or programme. The purpose of the research is to establish any sub layer which may be used in the future in constructing a comprehensive model which will consist of multiple layers that complement each other.

5.2 The holistic security model for Sudanese electronic government

According to review of literature academic and industrial, a holistic approach that could be used to analyze threats of e-services offered by e-governments was not found. Most of the literature studied emphasized the challenges of e-government through the technical infrastructure protection alone [132]. There is no doubt that the approach of the technical infrastructure protection will mitigate some of the risks to e-services, but it will not be sufficient to counter all threats.

Holistic security is a form of security which operates on multiple, fully integrated levels or layers. This approach to security can be taken to secure a structure, a computer network, a campus, and any number of other things which might need securing. The underlying idea behind holistic security is that systems need to be considered as wholes to achieve the greatest level of security; while it is important to be aware of individual aspects of a system, the ways in which these aspects work together are also a key part of a security system. See figure 5.1 to illustrate the holistic security layers for Sudan e-government.

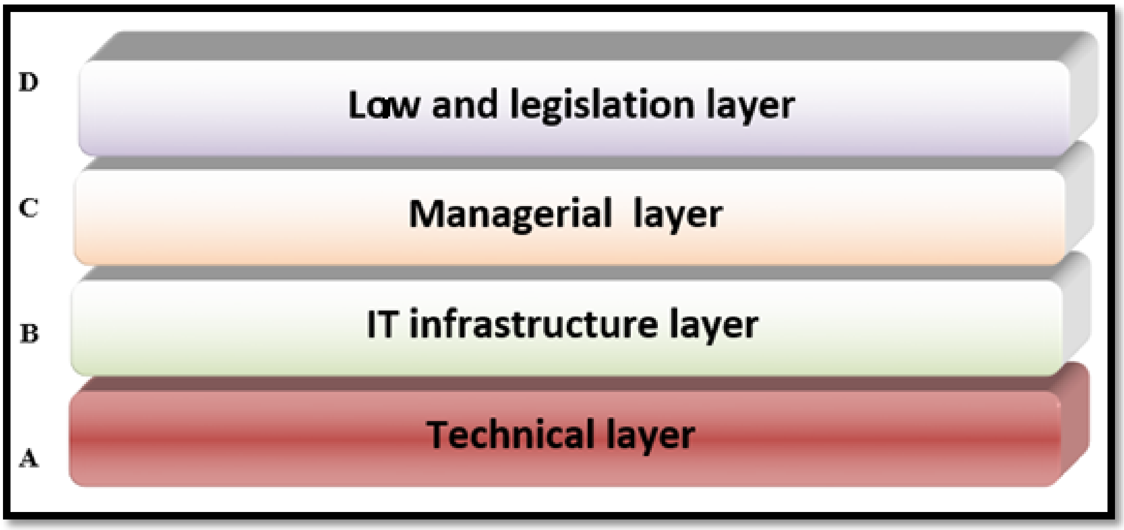


Figure 5.1: This figure shows the security layers of e-government in Sudan

5.3 Security Requirements

Security requirements provide foundations upon which the security of Sudanese e-government is built. Security requirements are driven by security threats facing Sudanese e-government.

5.3.1 Build the IT infrastructure

IT infrastructure refers to the fundamental factors necessary for conduct and continuity the project of e-government in Sudan and its security. The factors that affect the IT infrastructure in Sudan e-government are:

5.3.1.1 Availability of skilled staff is obviously a strong requirement of any e-government security project. So by increasing the staff's salary and good training may be minimize the threats of IT infrastructure. The staff who are not competent to run the security programme or maintain it will put the overall security system at great risk [134], [135].

5.3.1.2 Reliability of infrastructure is an important factor to secure the e-government systems. The use of open access software's in the websites design and development leads to unreliability in the infrastructure.

Trust is an issue that has been widely inspected and defined in various differently ways. According to Rotter [179], trust is considered as “the expectancy that the promise of a person or group can be relied upon”. Trust in the e-government is measured through two dimensions: trust in the particular entity (which, in this case, is the government), and trust in the reliability of the enabling technology [180].

5.3.1.3 Consultation in large scale projects like e-government project is an important factor to improve all technical issues that related to e-government project.

5.3.1.4 Software houses are an important issue to achieve or support e-government project.

See figure 5.2 to illustrate the IT infrastructure layers

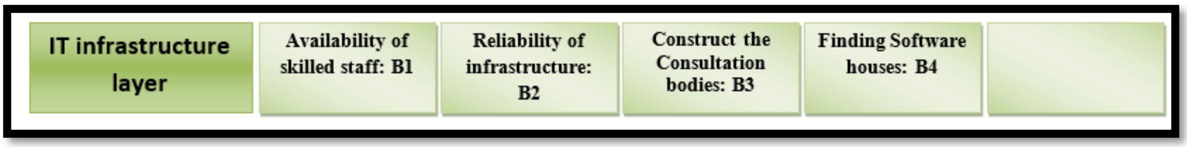

IT infrastructure layer
Availability of skilled staff: B1
Reliability of infrastructure: B2
Construct the Consultation bodies: B3
Finding Software houses: B4

Figure 5.2: This figure illustrates the IT infrastructure layer

5.3.2 Managerial layer

These type of level is deal with the decision makers in Sudan they should be more aware to enable e-government project. There are many factors that must be considered illustrated in figure 6.3.

5.3.2.1 Prepare Budget

E-government systems require considerable financial resources: resources must be allocated to developing and managing systems, building up technical infrastructures, and coordinating systems and initiative.

5.3.2.2 Finding policies and find mechanisms to enforce it

Finding policies and find mechanisms to enforce it is an important factor to satisfy the purpose of a good way to manage the e-government issues that lead to best e-government in Sudan.

5.3.2.3 Government has to introduce the benefits of e-government to the top management and administration.

It is very important thing to build top administrator and employee awareness via means such as training, gridline posters, and newsletters.

5.3.2.4 Avoiding financial corruption through the punishment of the guilty

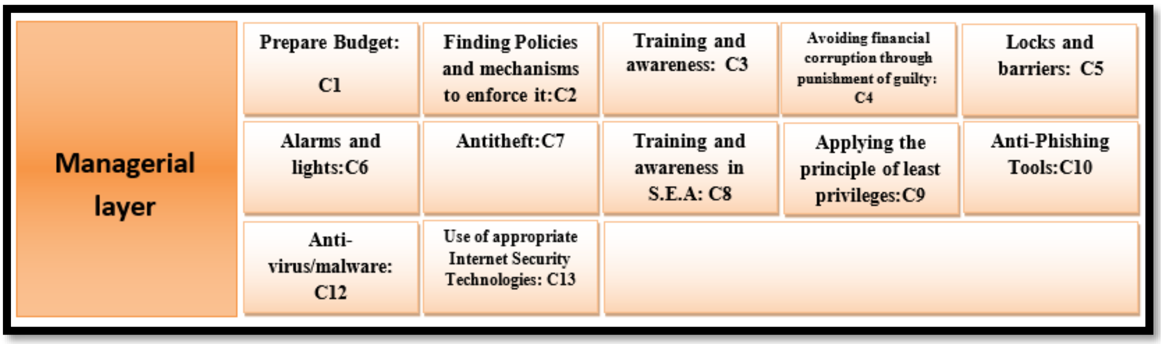
To avoid the conflict of interest on each organization the punishment policies must be imposed.

5.3.2.5 Countermeasure of Social engineering attacks

- Training and awareness against this type of threats.
- Applying the principle of least privileges is also done to mitigate this type of threats.
- Anti-Phishing Tools: The use of Anti Phishing Tools that connect to a database of blacklisted phishing websites is recommended.
- Use of appropriate Internet Security Technologies: Businesses with online presence should ensure their Secure Sockets Layer (SSL) or the more robust version of the technology, Extended Validation (EV) SSL certificates are updated and are from well-known reputable providers; this is
- Ant-virus/malware: System Administrators and individuals should update computer software (operating system, anti-virus, anti-spyware, anti-phishing, safe browsing and firewall) regularly. It is important to note that free anti-virus software has limited protection.

5.3.2.6 Countermeasure of Physical security

- Locks and barriers (referred to as locking devices by the professionals), and barriers include walls, fences, doors, bollards, and gates. A surprising amount of technology and thought goes into the design of barriers.
- Alarms and lights: Alarms are primarily for letting us know if that control is functioning properly — that is, has it been breached? Alarms tell us when some sort of action must be taken, usually by a human. Lights allow to see.
- Antitheft**:** It is obvious that the theft of computers and peripherals can directly affect the availability and confidentiality of data. However, tampering is also an issue, particularly with data integrity.



Managerial layer

Prepare Budget: C1

Finding Policies and mechanisms to enforce it:C2

Training and awareness: C3

Avoiding financial corruption through punishment of guilty: C4

Locks and barriers: C5

Alarms and lights:C6

Antitheft:C7

Training and awareness in S.E.A: C8

Applying the principle of least privileges:C9

Anti-Phishing Tools:C10

Anti-virus/malware: C12

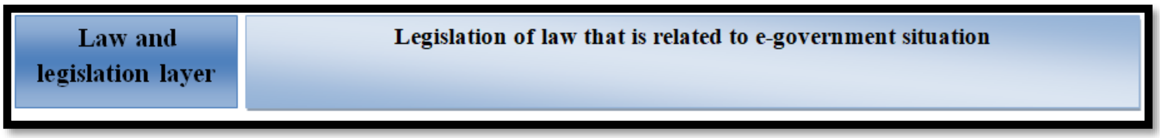
Use of appropriate Internet Security Technologies: C13

Figure 5.3: This figure shows the managerial issues in e-government in Sudan

5.3.3 Developing legislative protection and law

The success of e-government initiatives and processes are highly dependent on government's role in ensuring a proper legal framework for their operation. The lack of legal equivalence between digital and paper process can impede the take up of e-government.

A requirement for e-government processes to be introduced and adopted is their formal legal equivalence and standing with the paper process. See figure 6-4.



Law and legislation layer

Legislation of law that is related to e-government situation

Figure 5.4: This figure shows the law and legislation

5.3.4 Technical layer

Since information systems are the heart of any organisation and the mean of users access to the e- services, authenticating the identity of the user is one of the fundamental controls an organization needs to put in place.

Authentication is the process of positively verifying the identity of a user in a computer system, usually based on a user name and password. In security systems, authentication is distinct from *authorization* , which is the process of giving individuals access to system objects based on their identity. Authentication merely access rights of the individual. Authentication definitely plays a major role in elevating the trust of users in the computer system and the services launched over the Internet and it needs to be part of the government departments security architecture or model. See figure 5.5.

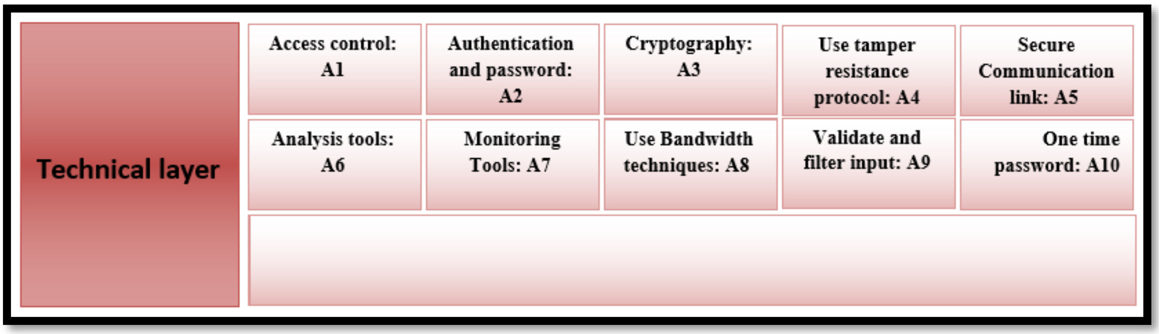

Technical layer
Access control: A1
Authentication and password: A2
Cryptography: A3
Use tamper resistance protocol: A4
Secure Communication link: A5
Analysis tools: A6
Monitoring Tools: A7
Use Bandwidth techniques: A8
Validate and filter input: A9
One time password: A10

Figure 5.5: This figure shows the sub-layers of technical layer

5.3.4.1 Access control

Access control is a mechanism of controlling entry to any perimeter or a boundary. The control might be through prevention of unauthorized entries, monitoring authorized entries, or limiting entries through predefined rules and roles. The assets can be in format of systems, information resources in any manifestation or an environment where confidential discussions can be held. All organisations will need some level of access control to its offices, computer centres, or even staff areas. An e-government model is as an example of an e-enabled organisation and will have a strong requirement of access control to the computer centres where governmental data are held, offices of the staff handling the e-government services, and even cables carrying the data between governmental departments.

5.3.4.2 Authentication and password

The demand of protecting the privacy and the integrity of corporate information has been increasing recently. Since information systems are the heart of any organisation and the mean of users access to the e- services, authenticating the identity of the user is one of the fundamental controls an organization needs to put in place [158].

5.3.4.3 Cryptography

Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds. The authenticity of data can be protected in a similar way. Encryption is one solution to the problem of reveal information of others by intruders.

5.3.4.4 Use tampering resistance protocol

Tamper-proof hardware devices have been used quite massively in industrial and commercial applications. There exists a wide spectrum of tamper-proof devices, ranging in their price and security. So far, secure hardware devices have been used to implement some strong security protocols with the hypothesis that they are tamper-resistant.

5.3.4.5 Secure communication link

Secure communication link is the prevention of unauthorized access to telecommunications traffic, or to any written information that is transmitted or transferred.

5.3.4.6 Analysis tools

There is an desperately need to use analysis tools because of the increasing evolution of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise.

5.3.4.7 Monitoring tools

Networks should be subject to continuous monitoring to maintain confidence in the security of any site network and data resources.

5.3.4.8 Use bandwidth techniques

A bandwidth techniques is used to improve the rate and volume of traffic flows on the network.

5.3.4.9 Validate and filter input

It's pretty obvious that one of the major security issues for web applications - in any language - is the effective filtering and validation of the data it's using from external sources. It acts as a first line of defense. This could be coming from any number of places including database, outside APIs or, the worst of them all, your own users. Bad data could be just about anything. It can come in the form of badly formatted text someone copy and pasted all the way out to something malicious from a would-be attacker.

5.3.4.10 One time password

One time passwords avoid a number of shortcomings that are associated with traditional (static) password. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks.

5.4 The security layers, risks and countermeasures

The idea of this model is stemmed from the risk analysis that facing the Sudanese electronic government which has been done in the previous chapter which are listed in the second column of the tables (5.1), (5.2), (5.3) and (5.4).

Table 5.1: illustrates the technical layer, risk analysis and Countermeasure of risks

Layer	Risks Analysis	Countermeasures of risks
Technical layer	-Unauthorized access to a place or other resource.	-Access control -Authentication password
	-Information interception	-Cryptography
	-Information tampering	-Authentication password -Using tamper-resistant protocol across communication links -Secure communication links with protocols that provide message integrity. -Cryptography
	-Denial of services attacks	-Analysis tools -Monitoring tools -Using resource and bandwidth throttling techniques -Validate and filter input
	-System resources stealing	-Access control -Authentication password -Analysis tools -Monitoring tools
	-Information faking	-One time password -Cryptography

The third column of the table 'countermeasures of risks' compose the sub-layer of the model. The collection of the same issues (sub-layers) that mentioned in the third column of the table (5.1) are collected together to form the main layer of the model which are listed in the first column of the table (5.1) and figure (5.1).

The 5.2 table the IT infrastructure layer, risk analysis and the countermeasures of these risks.

Table 5.2: illustrates the infrastructure layer, risk analysis and Countermeasure of risks

Layer	Risks Analysis	Countermeasures of risks
IT infrastructure layer	-Lack of technical skills	-Availability of skilled staff by increasing their salary and trainings.
	-Lack of users' trust and confidence to use e-government services.	-Reliability of infrastructure
	-Lack of consultation	-Construct the Consultation bodies
	-Lack of software houses	-Finding software houses

The table 5.3 below illustrates the managerial layer, risk analysis and the countermeasures of these risks.

Table 5.3: illustrates the infrastructure layer, risk analysis and Countermeasure of risks

Layer	Risks Analysis	Countermeasures of risks
Managerial layer	-Lack of Budget	-Prepare budget
	-Lack of policy and regulation for e-usage in Sudan	-Finding policies and mechanism to enforce it
	-Resistance to change in top management and administration	-Government has to introduce the benefits of e-government to the top management and administration.
	-Conflict of interest	-Avoiding financial corruption through punishment of guilty.
	-Social engineering attacks	-Training and awareness in S.E.A -Applying the principle of least privileges -Anti-Phishing Tools -Anti-virus/malware -Use of appropriate Internet Security Technologies
	-Lack of physical security	-Alarms and lights -Antitheft

The table 5.4 below illustrates the law and legislations layer, risk analysis and the countermeasures of these risks.

Table 5.4: illustrates the Law and legislation layer, risk analysis and Countermeasure of risks

Layer	Risks Analysis	Countermeasures of risks
Law and legislation layer	-Lack of law and legislation related to e-government	-Legislation of law that is related to e-government situation.

5.5 The security layers for Sudanese e-government

In order to reach to a comprehensive method to check the security requirements for any e-enabled organization to allow or not to allow the interchange of information with other e-organizations in Sudan; the multiple security layer was proposed. See figure 5.1

Any model contains more than one level or layer of security is comprehensive model, and prevent organization from wide range of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services. For example the technical layer will address all the technological threats while the IT infrastructure will address the threats on e-services related to the requirements that are important to continuity to e-government projects. There are four security layers that contribute in construct the security model for Sudanese security e-government model see figure 6.6. The model extracted from the interviews and collected data from the responsible body of the e-government projects in Sudan.

Each layer of the model contains of detailed layer or sub-layer see figure 5.7. See figure 5.6 that show the orientation of the model.

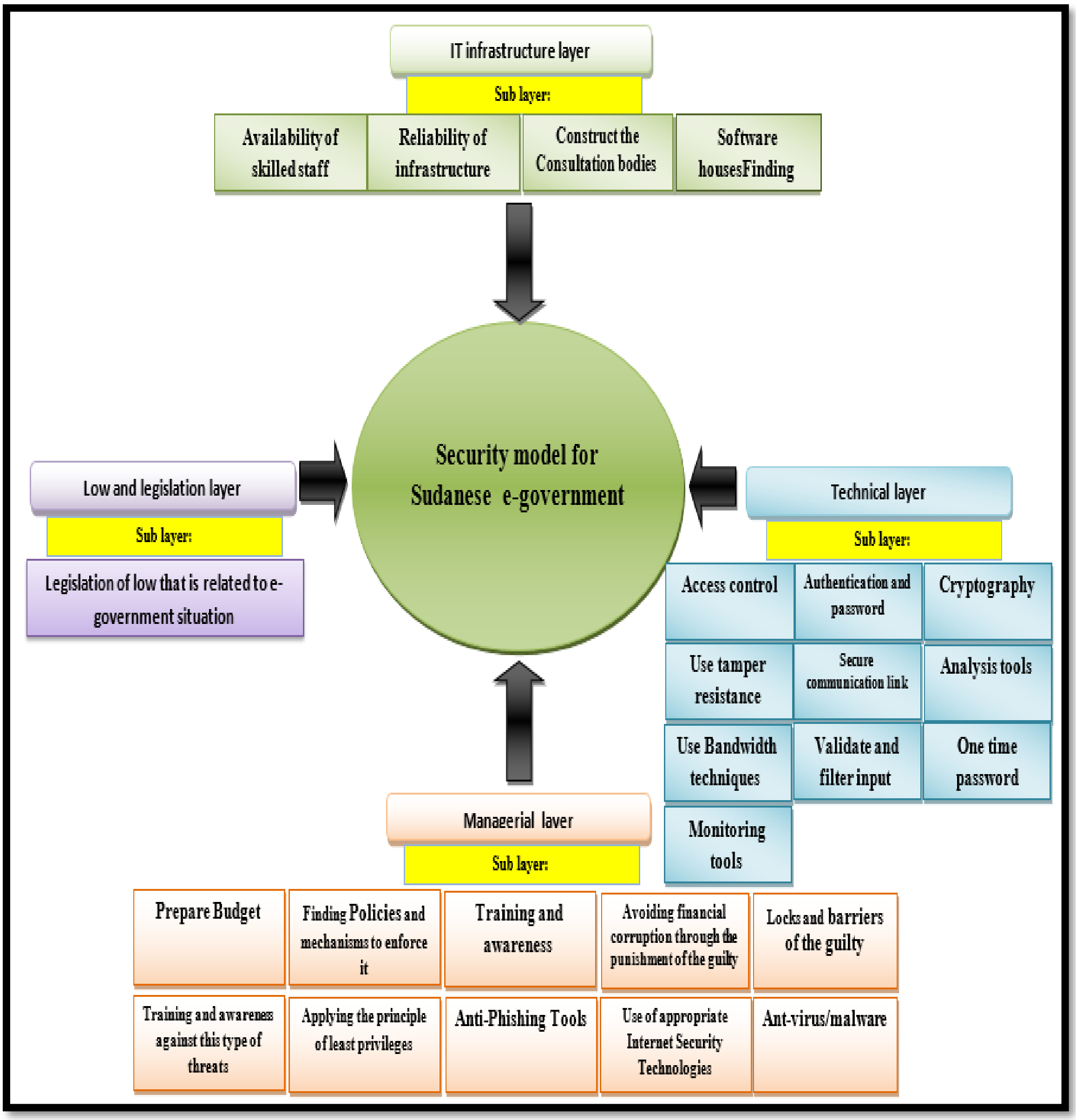
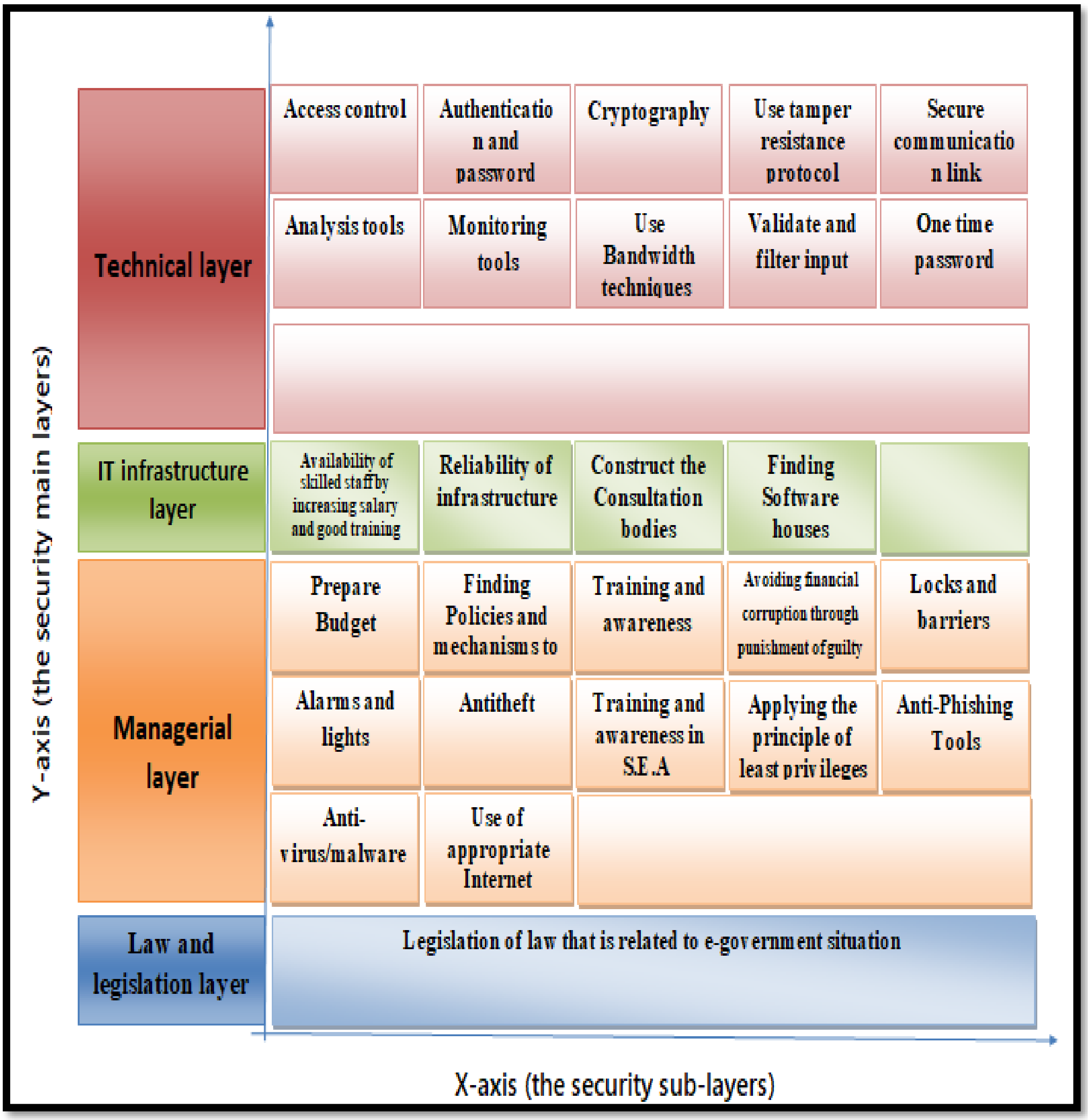

IT infrastructure layer
Sub layer:
Availability of skilled staff
Reliability of infrastructure
Construct the Consultation bodies
Software housesFinding
Security model for Sudanese e-government
Low and legislation layer
Sub layer:
Legislation of low that is related to e-government situation
Technical layer
Sub layer:
Access control
Authentication and password
Cryptography
Use tamper resistance
Secure communication link
Analysis tools
Use Bandwidth techniques
Validate and filter input
One time password
Monitoring tools
Managerial layer
Sub layer:
Prepare Budget
Finding Policies and mechanisms to enforce it
Training and awareness
Avoiding financial corruption through the punishment of the guilty
Locks and barriers of the guilty
Training and awareness against this type of threats
Applying the principle of least privileges
Anti-Phishing Tools
Use of appropriate Internet Security Technologies
Ant-virus/malware

Figure 5.6: This figure shows the sub layer of the model

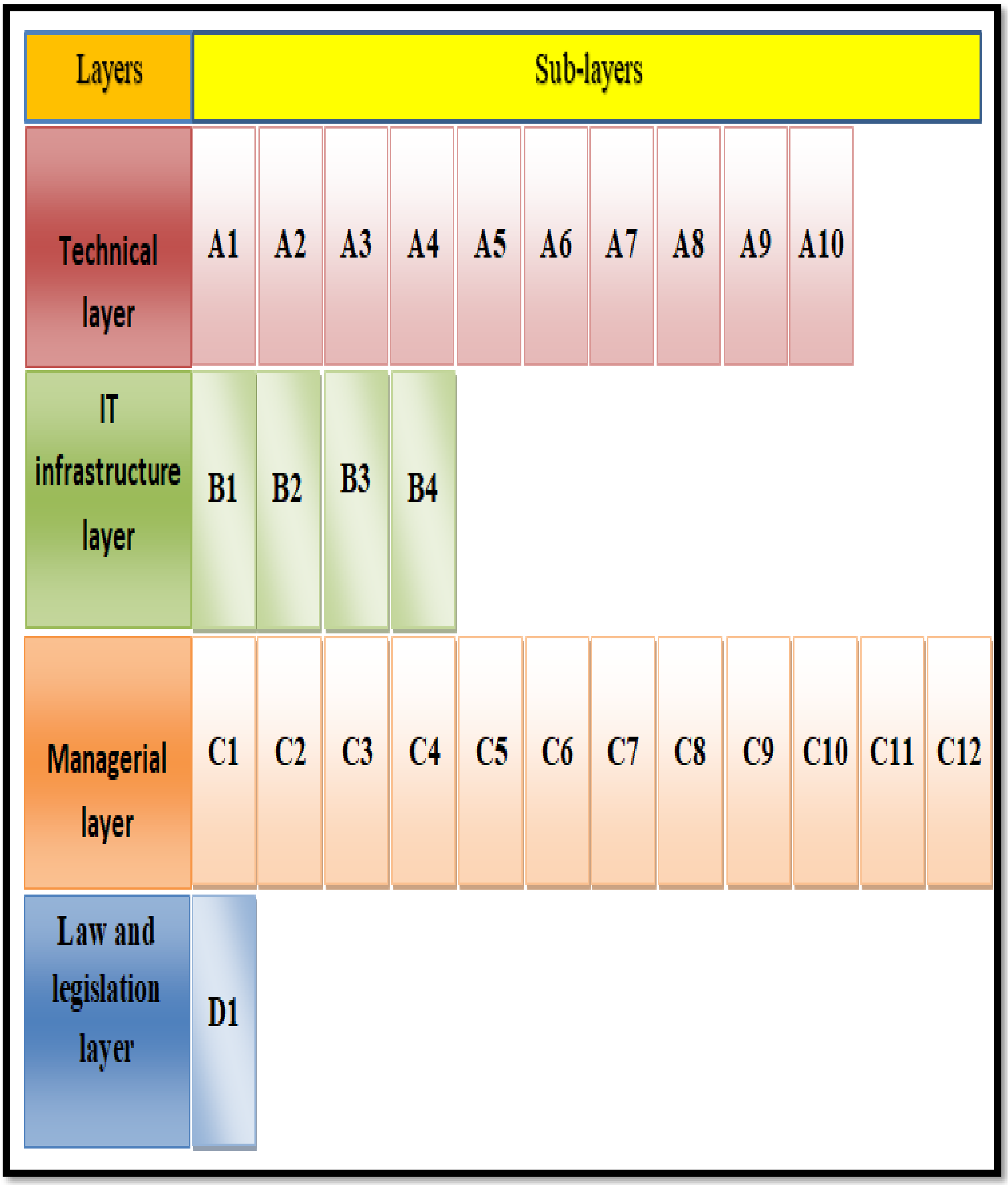
The final model in this research composed of vertical axis that represent the main layers and horizontal axis that represent the sub-layers. The main layers (vertical axis) are positioned according to Sudanese security situation, they are the aspects or risks that facing the security of e-government in Sudan. The sub-layers (horizontal axis) are detailed layers with respect to each main layer. The final model is a coherent and understandable model because of its structure vertical and horizontal axis. See figure 5.8.



Technical layer	Access control	Authentication and password	Cryptography	Use tamper resistance protocol	Secure communication link
	Analysis tools	Monitoring tools	Use Bandwidth techniques	Validate and filter input	One time password
IT infrastructure layer	Availability of skilled staff by incresing salary and good training	Reliability of infrastructure	Construct the Consultation bodies	Finding Software houses	
Managerial layer	Prepare Budget	Finding Policies and mechanisms to	Training and awareness	Avoiding financial corruption through punishment of guilty	Locks and barriers
	Alarms and lights	Antitheft	Training and awareness in S.E.A	Applying the principle of least privileges	Anti-Phishing Tools
	Anti-virus/malware	Use of appropriate Internet			
Law and legislation layer	Legislation of law that is related to e-government situation				

Y-axis (the security main layers)
X-axis (the security sub-layers)

Figure 5.7: This figure shows the layers and sub-layers of e-government security model for Sudan



Layers	Sub-layers											
Technical layer	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10		
IT infrastructure layer	B1	B2	B3	B4								
Managerial layer	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
Law and legislation layer	D1											

Figure 5.8: This figure shows the security model for Sudanese e-government

5.6 The key of the model

In this section, the model is proposed as a form of symbols where each symbols refers to a particular layer and its sub-layers as shown in Figure 5.10, for example A1 represents the first sub-layer in the technical layer and B2 represents the second sub-layer in IT infrastructure layer. See table 5.5 that illustrates the model key.

Table 5.5: illustrates the model key

Layer	Category		Category	
Technical layer	Access control	A1	Analysis tools	A6
	Authentication and password	A2	Monitoring Tools	A7
	Cryptography	A3	Use Bandwidth techniques	A8
	Use tamper resistance protocol	A4	Validate and filter input	A9
	Secure Communication link	A5	One time password	A10
IT infrastructure layer	Availability of skilled staff by increasing salary and good training	B1	Construct the Consultation bodies	B3
	Reliability of infrastructure	B2	Finding Software houses	B4
Managerial layer	Prepare Budget	C1	Antitheft	C7
	Finding Policies and mechanisms to enforce it	C2	Training and awareness in S.E. A	C8
	Training and awareness	C3	Applying the principle of least privileges	C9
	Avoiding financial corruption through punishment of guilty	C4	Anti-Phishing Tools	C10
	Locks and barriers	C5	Anti-virus/malware	C11
	Alarms and lights	C6	Use of appropriate Internet Security Technologies	C12
Law and legislation layer	Legislation of law that is related to e-government situation	D1		

5.7 Summary

From the analysis conducted on the results of the questionnaire, it can be conclude that e-services have technical and non-technical threats. These threats can be categorized as technical layer, IT infrastructure layer, managerial layer and law and legislation layer. Taking the combination of the technical and non-technical threats with the different categories of them, it can be derived that an e-service will have a set of threats (technical and non-technical) and a set of different categories of threats This will lead into a need of a comprehensive model to tackle all types of threats.

CHAPTER VI

VALIDATION

6.1 Introduction

Any security model depend on levels or layers in its structure is a robust and better success rate in preventing organisations from various categories of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services. The countermeasure of authentication security level for example will address all issues related to the lack of authentication while the countermeasure of lack of safety defense level will the threats caused by the malware, internet infra-structure, denial of services, packet sniffer, probe, remote to local attack and user to root attack.

The sub layers of each layer or level needed in any information security system or programme. The purpose of the research is to establish any sub layer which may be used in the future in constructing a comprehensive model which will consist of multiple layers that complement each other. In this research there are five areas that contribute in building strong security architecture and system in Sudanese electronic government.

According to the methodology diagram used in this research, the validation was an essential process of the whole processes of methodology. It was an important process to confirm of model applicability. See figure 3.7.

6.2 The analysis

The layers and sub-layers of the proposed security model for the Sudanese e-government were specified by security practitioners in National information center (NIC), observations, literal reviews and documents. The specification of these layers and sub-layers were based on variations of views.

6.3 Modeling process

A model is an unambiguous, abstract conception of some parts or aspects of the real world. Models focus on specific aspects of the real world, based on the purpose for which the model is created. Hence, modelling is part of a goal-driven communication process [141].

6.3.1 The standards contained in success the proposed model

According to Wood, C. and Lankhorst. M. [129] [141], there are many standards or factors that lead to the success of the models. These factors are:

6.3.1.1 Simplicity of the model

The model must be clear to the targeted users or stakeholders (government departments or individuals). The layers of the model must be explicit should make sense to a non-security or IT expert.

6.3.1.2 The possibility of applying

The model must be appropriate to any organisation which plans to use it for its internal or external communication or information sharing.

6.3.1.3 Standards compliant

The model must meet the terms with the security standards in terms of acronyms, references, objectives.

6.3.1.4 Achievable

The model must be possible for the e-government authority and its government affiliates.

6.3.1.5 Flexible

The model must be flexible and can be implemented in phases.

6.3.1.6 Open standards

The model must tackle general technologies, and non-technologies issues.

6.3.1.7 Renewable and expandable

The model must be easy to renew with the introduction of new trends in the security field and it also can allow merge group of security technologies.

The following checklist entitled as “Validation Form” (Table 6.2) was developed for the e-government to use in order to evaluate and validate the model where (SA): Strongly Agree, (A): Agree, (N): Neutral and (D): Disagree

Table 6.1: shows the validation form

Factors that lead to the success of the models	**Description**	**Rate**			
Simplicity of the model	The model must be clear to the targeted users or stakeholders (government departments or individuals). The layers of the model must be explicit should make sense to a non-security or IT expert.	SA	A	N	D
The possibility of applying	The model must be appropriate to any organisation which plans to use it for its internal or external communication or information sharing.	SA	A	N	D
Standards compliant	The model must meet the terms with the security standards in terms of acronyms, references, objectives.	SA	A	N	D
Achievable	The model must be possible for the e-government authority and its government affiliates.	SA	A	N	D
Flexible	The model must be flexible and can be implemented in phases.	SA	A	N	D
Open standards	The model must tackle general technologies, and non-technologies issues.	SA	A	N	D
Renewable and expandable	The model must be easy to renew with the introduction of new trends in the security field and it also can allow merge group of security technologies.	SA	A	N	D

The validation process of the security model was having three dimensions. It was started before creating the model. The first dimension was to answer the questions listed in table 7.1. The second dimension was to check standards or factors that lead to the success of the model. The third dimension was to check the model value and its usability aspects. This was achieved through a distribution of a validation form developed in table 7.2 to assist the participant to select the rate of validity from different success standards.

6.4 Summary

The objective of this chapter was to discuss the validation form results deployed to 6 highly recognized security practitioners. The results of the analysis confirmed the standards contained in success the proposed model.

CHAPTER VII

CONCLUSION

Information security plays a key role to enable e-services offered by government departments or authorities, information sharing inter or intra government departments, and above all to improve the trust between authorities and their affiliates. The level of trust or the net confidence is directly related to the security confidence of any organisation. The usability of the e-services over the Internet can increase if the security level is enhanced within the service provider and the users' security awareness is elevated. Some of the developed models were successful in resolving issues related to the system security, while others were policy oriented addressing either confidentiality or integrity of the information. During the literature review phase and through all the research conducted, no comprehensive security model was found which addresses the different aspects of security.

The development of the new model for Sudanese e-government security was based on scientific knowledge and a thorough analysis process. The new model consists of four layers. Each layer represents a dimension of security which need to be addressed in order to mitigate threats associated with it. Each layer has one or more of sub layer.

Questionnaire was deployed to the e-government programme in Sudan. The objectives of the questionnaires were:

- To identify the types of threats on different e-services.
- To get a view from management of the government departments on different types of threats.
- To identity the layers required in the model and their sub layers also.
- To get the security practitioners feedback on the need of technologies, IT infrastructure, managerial and law and legislation as layers of the new model.

The objectives of the research were met and a new model is proposed through this thesis document. The new model can be applicable for any governmental department and it can be implemented as architecture or an assessment tool.

7.1 Future work

Future work can be conducted on a mathematical representation of the model which will assist in defining the best combination of all sub layers in order to come up with the highest security score for an organisation which need to launch an e-service or share information over the Internet. The mathematical formula can be used in the future for finding the combination of sub layers or any IT model subject that the importance of each layer or sub layer is defined, a thorough dependency analysis is conducted, the scenarios are well defined and the quantification of the important factors can be achieved.

REFERENCES

[1]Adam J. Mambi, (2010). *ICT Law Book A Source book for Information and Communication Technology Cyber Law in Tanzania and East Africa Community*. Mkuki Na Nyota, Dar-Es-Salaam.

[2] Hans J.Scholl, (2010). E-Government, Information, Technology, and Transformation.*Volume17.* Advances in Management Information systems. London

[3] DrissKettani and Bernard Moulin, (2014). *E-Government for Good Governance in Developing Countries Empirical Evidence from the eFez Project.* Anthem. London.

[4] AkeGronlund, (2002). *E-government Design Applications and Management*. Idea Group Publishing. London.

[5] Wayne Huang; KengSiau; Kwok Kee Wei, *(2005). Electronic government strategies and implementation***.** Idea Group Publisher. Hershey.

[6] Al Nagi, E., &Hamdan, M. (2009). Computerization and e-Government implementation in Jordan: Challenges, obstacles and successes. *Government Information Quarterly*. **26**(4)*:* 577-583

[7] Atreya, M., Hammond, B., Paine, S., Starrett, P. and Wu, S. (2002), *Digital Signatures,* McGraw Hill, New York.

[8] Heeks, R. (2002). Information Systems and Developing Countries: Failure, Sucess, and LaocalImprovistions,*The Information Society*. **18**: 101-112.

[9] Gupta, M. P. and Jana, D. (2003). E-government evaluation: A framework and case study, *Government Information Quarterly*. **20**: 365-387.

[10] Heeks, R., Bailur, S. (2007): Analyzing E-Government Research. Perspectives, philosophies, theories, methods, and practice. *Government Information Quarterly***24**: 243–265

[11] Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Prentice-Hall, Englewood Cliffs.

[12] Bandura, A. (2001). Social Cognitive Theory: An Agentic Perspective. *Annual Review of Psychology***52**: 1–26

[13] Layne, K., Lee, J.W. (2001) Developing Fully Functional E-government: A four stage model. *GovernmentInformation Quarterly***18**: 122–136

[14] Carter, L., Weerakkody, V. (2008). E-Government Adoption: A cultural comparison. *Information Systems Frontiers***10**: 473–482

[15] Jasperson, J., Carter, P.E., Zmud, R.W. (2005) A comprehensive conceptualization of postadoptivebehaviours associated with information technology enabled work systems. *MIS Quarterly***29**: 525–555.

[16] Al-Hakim, L(2007).*Global e-government: Theory, applications and Benchmarking volume1.* Idea Group Publishing. London.

[17] Yildiz, M. (2007), E-government research: reviewing the literature, limitations, and ways forward. *Government Information Quarterly* **24**: 646-665.

[18] Oyomno, G. (2004). Towards a framework for assessing the maturity of government capabilities for e-government. *The Southern African Journal of Information and Communication* **4**: 77.

[19] Wimmer, M. A., Codagnone, C. and Ma, X. F. (2007). Developing an e-government research roadmap: method and example from E-GovRTD2020, *Electronic Government, Proceedings* **4656**: 1-12.

[20] Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change.* Brookings. Washington D.C.

[21] Metaxiotis, K. and Psarras, J. (2004). E-government: new concept, big challenge, success stories. *Electronic Government, an International Journal.***2**: 141-151.

[22] Dada, D. (2006). The failure of e-government in developing countries: A literature review. *Electronic Journal of Information Systems in Developing Countries.***26**:. 1-10.

[23] Oyomno, G. (2004). Towards a framework for assessing the maturity of government capabilities for e-government, *The Southern African Journal of Information andCommunication***4**: 77.

[24] Moon, M. J. (2002). The evolution of e-government among municipalities: Rhetoric or reality? *Public Administration Review* **62**:424-433.

[25] Grant, G. and Chau, D. (2005). Developing a generic framework for e-government Journal *of Global Information Management***13**:1-30.

[26] Ndou, V. (2004). E–government for developing countries: Opportunities and challenges, *Electronic Journal of Information Systems in Developing Countries* **18**: 1-24.

[27] Heeks, R., (2003). *Most egovernment-for-development projects fail: How can risks be reduced?*, Institute for Development Policy and Management. Manchester.

[28] Seifert, J. W. and Petersen, R. E. (2002). The promise of all things E? Expectations and challenges of emergent electronic government, *Perspectives on Global Developmentand Technology***1**: 193-212.

[29] Tambouris, E. (2001). An integrated platform for realising online one-stop government: The e- government project. In: *12th International Workshop on Database and Expert Systems Applications* (Dexa) . pp. 0359. IEEE. Munich, Germany.

[30] Lenk, K. and Tranmüller, R. (2000). A framework for electronic government.*Institute of Electrical and Electronics Engineers***1**:271-277.

[31] Stoltzfus, K. (2005). Motivations for implementing e-government: an investigation of the global phenomenon, *Digital government research***89**: 333.

[32]http://extsearch.worldbank.org/servlet/SiteSearchServlet?q=e-government (retrieved 9 June 2010).

[33] Chen, Y. N., Chen, H. M., Huang, W. and Ching, R. K. H. (2006). E-government strategies in developed and developing countries: An implementation framework and case study, *Journal of Global Information Management***14**: 23-46.

[34] Tahrani, S. M. (2010). A model of successful factors towards e-government implementation. *Electronic Government, an International Journal***7**: 60-74.

[35] Nour, M. A., AbdelRahman, A. A. and Fadlalla, A. (2008). A context-based integrative framework for e-government initiatives, *Government Information Quarterly***25**: 448-461.

[36] Smith, A. D. (2008). Business and e-government intelligence for strategically leveraging information retrieval, *Electronic Government, an International Journal.***5**: 31-44.

[37] UN (2010). *E-government survey 2010: Leveraging e-government at a time of financial and economic crisis.* United Nations Department of Economic and Social Affairs Division for Public Administration and Development Management. UNDESA and ASPA. New York.

[38] West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes, *Public administration review* **64**: 15-27.

[39] UN 2014 New York

[40] https://www.computerhope.com/tips/tip161.htm (retrieved Feb2015)

[41] Conklin, A. and White, G., B. (2006). *E-Government and cyber security: The role of cyber security exercises. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06).* pp. 79b. IEEE. Kauai, United States.

[42] Benabdallah, S., Fatmi, G. E. and Ourdiga, N. B. (2002). Security issues in Egovernment models: what governments should do?.In: *Proceedings of the IEEE*

International Conference on Systems, Man and Cybernetics.(Institute of Electrical and Electronics Engineers Inc.). pp. 398-403. *IEEE*, Yasmine, Hammarnet, Tunisia.

[43] Mitra, A. (2005). Direction of electronic governance initiatives within two worlds: case for a shift in emphasis, *Electronic Government***2**: 26.

[44] Turban, E., King, D., Lee, J., Warkentin, M. and Chung, M. H. (2001). *Electronic Commerce 2002: A Managerial PerspectiveVolume1*, Prentice Hall. New York.

[45] Priyambodo, T.K., Prayudi, Y. (2015). Information security strategy on mobile device based eGovernment. *Journal of Engineering and Applied Sciences*. **10**(2): 652–660.

[46] Karokola, G.R. (2012). *A framework for securing e-Government services the case of Tanzania*. Stockholm University, Sweden.

[47] Teo, T.S.H., Srivastava, S.C., Jiang, L. (2009). Trust and electronic government success: An empirical study. *Management. Information. Syst*ems. **25(3)**: 99–131.

[48] Moen, V., Klingsheim, N., Inge, K., Simonsen, F., Hole, K.J. (2007) Vulnerabilities in E-Government web portals. *International Journal of Electronic* Forensics **1(1):** 89–100.

[49] Colesca, S.E. (2009). Understanding trust in e-Government. *International economic*. **3**: 7–15.

[50] Alsaghier, H., Ford, M. (2009). Conceptualising citizen's trust in e-Government: application of Q methodology. *International Journal of Electronic Government*. 7(4): 295–310.

[51] Santos, N.M.C. (2013). *Improving Trust in Cloud, Enterprise, and Mobile Computing Platforms*. Universitat de Saarlandes, Saarbrücken.

[52] Burmester, M., Mulholland, J.(2006). The advent of trusted computing: implications for digital forensics. *Symposium on applied Computing***6**: 23–27.

[53] Wada, K., King, P.(2001). IT policy: an essential element of IT infrastructure. *Educause Review***1:** 14–15.

[54] Gikas, C.(2010). A General Comparison of FISMA, HIPAA, ISO 27000. *Information Systems Security***19:** 132-141.

[55] Taylor, C., Endicott-Popovsky, B., Frincke, D.A. (2007). Specifying digital forensics: a forensics policy approach. *Digital Investigation***4**: 101–104.

[56] Sandhu, R. (2010). *Security Models Past, Present and Future*. Institute for Cyber Security, University of Texas at San Antonio San Antonio USA.

[57] Security Document World (2014). *The Role of Trusted Digital Identity in Enabling the eGovernment 2020 Vision*. Secure identity alliance. France.

[58] Stallings, W. and Brown, L. (2008). *Computer Security: Principles and Practice, Volume3*. Pearson Education, Inc, Upper Saddle River, NJ.

[59] Mclean, J. (1990). Security Models and Information Flow. In: *Proceeding.1990 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE*. 180-187. IEEE. Oakland, CA. USA.

[60] Goguen, J. A. and Mesequer, J. (1982). Security policies and security models. In *Proceedings of the 1982 Symposium on security and privacy, IEEE*. 11-20, Oakland, CA, USA, IEEE, New York, NY, USA.

[61] Lindgreen, E. E. O. R. and Herschberg, I. S. (1994). On the Validity of the Bell-LaPadula model. *Computers & Security,* vol. **13**: 317-33.

[62] Anderson, R. (2008). *Security Engineering: A Guide Building Dependable Distributed Systems Volume2.* Wiley. U.S.

[63] Mclean, J. (1990). Security Models and Information Flow. *In:Proceeding of 1990 IEEEComputer Society Symposium on Research in Security and Privacy,* pp. 180-7. IEEE Computer Security. Oakland, CA, USA.

[64] Fraster, T. (2001). LOMAC: MAC you can live with. *In:Proceedings of the FREENIX Track. 2001 USENIX Annual Technical Conference.*pp 1-13Boston, MA, USA, USENIX Assoc, Berkeley, CA, USA.

[65] Brewer, D. F. C. and Nash, M. J. (1989). Chinese Wall security policy, *Security and Privacy, 1989 IEEE Symposium,* pp. 206-214.Oakland, CA, USA.

[66] Akers, R. L., Krohn, M. D., Lanza-Kaduce, L. and Radosevich, M. (1979).*Social learning and deviant behaviour: a specific test of a general theoryvolume 44*Blackwell, MI, USA.

[67] Lanotte, R., Maggiolo-Schettini, A., Tini, S., Troina, A. and Tronci, E. (2004). Automatic Analysis of the NRL pump, *Elsevier Science/Electronic Notes in Theoretical Computer Science*, pp. 245-266.

[68] https://www.gov.uk/government/organisations/department-of-health (retrieved Feb2016)

[69] Jie, W., Fernandez, E. B. and Zhang, R. (1992). Some extensions to the lattice model for computer security, *Computers & Security***11:** 357-69.

[70] Gopala Krishna Behara, Vishnu VardhanVarre and MadhusudhanaRao (2009).*Service Oriented Architecture for EGovernance* , BPTrends.

[71] http://www.infodev.org/publications (retrieved Feb2016).

[72] Dr. Ali M. Al-Khouri(2012). PKI in Government Digital Identity Management Systems, *European Journal of ePractice***16:**1-25.

[73] Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G. (2003). Security Requirements for e-government services: a mathematical approach for developing a common PKI-based Security Policy, *ELSEVIER* **26**: 1873-1883.

[74] Bodeau, D. J. (1992). A Conceptual Model for Computer Security Risk Analysis. *In: Proceedings Eighth Annua Computer Security Applications Conference.* (the MITRE Corporation) . pp. 56-63. IEEE Conference Publications, Bedford, USA.

[75] Hansen, J. (2001). Internet Commerce Security: Issues and models for control checking, *Journal of the Operational Research Society* **52**: 1159-1164.

[76] Keller, J. (1974). Optimum checking schedules for systems subject to random failure, *Management Science* **21**: 256-260.

[78] Ebrahim, Z. and Irani, Z. (2005). E-government adoption: Architecture and barriers, *Business Process Management Journal***11:** 589-611.

[79] Bakry, S. H. (2004). Development of e-government: a STOPE view, *International Journal of Network Management***5**: 339-350.

[80] Kennett, P, 2004. *A handbook of Comparative Social Policy*. Edward Egar, Cheltenham UK.

[81] Zhang. H (2012). E-government information security management. *Proceedings of the 2nd International Conference on Green Communications and Networks* (Y. Yang and M. Ma) Pp31-38 Springer-Verlag Berlin Heidelberg.

[82] Yang HP (2000). Network information security research. *Information Sciences* **17(10):** 74–77

[83] Ousley, M. R., (2013). *Information Security: the complete reference volume2*. McGraw-Hill London UK.

[84] Bragg R, Ousley M R, Strassberg K, (2004). *Network Security: The complete reference volume* 1. McGraw-Hill London UK.

[85] Elmasri R, Navathe S B, (2011). *Fundamentals of Database Systems Volume 6*. Addison-Wesley Boston USA.

[86] Stuttard D, Pinto M ,(2011). *The Web Application Hacker's Handbooks Finding and Exploiting Security Flows Volume 2.*Wiley Indiana USA.

[87] http://www.e-envoy.gov.uk (retrieved 23 May2012)

[88] www.mampu.gov.my/ (retrieved 23 May2012)

[89] http://www.teamiss.com/ (retrieved 23 April2015)

[90] http://www.digitalgovernance.org/index.php/models/critical-flow (retrieved 23 April2016)

[91]http://www.digitalgovernance.org/index.php/models/comparative-analysis (retrieved 23 April2016)

[92] http://www.cddc.vt.edu/digitalgov/gov-e-advocacy-models.html (retrieved 23 April2016)

[93] http://www.govtech.com/e-government/2012-Best-of-the-Web-Award-Winners-Announced.html (retrieved 23 May2012)

[94] Metz, H. (1991), *A country study: Sudan, Volume*2, Library of Congress, Washington. USA.

[95] http://www.state.gov/r/pa/ei/bgn/5424.htm (retrieved 23 May2012)

[96]http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/SU
DANEX
TN/0,,menuPK:375432~pagePK:141132~piPK:141107~theSitePK:375422,00.html
(retrieved 23 April2011)

[97] Young, T. (2004). *Sudan: conflict in Darfur*, House of Commons, UK.

[98]http://www.sudan.gov.sd/en/index.php?option=com_content&view=article&id=50 &Itemid=67 (retrieved 23 May2012)

[99] http://sudan.sd/en/sudan/index.html (retrieved 03 May2016)

[100] http://www.cbs.gov.sd/ (retrieved April2016).

[101] http://www.acdi-cida.gc.ca/sudan (retrieved May2014)

[102] http://www.un.org/(retrieved April2016)

[103] https://idl-bnc.idrc.ca/(retrieved April2016)

[104] Hamdy, A. (2007).*ICT in education in Sudan,*, Survey of ICT and Education in Africa: SudanCountry Report-infoDev.

[105] http://www.ntc.org.sd (retrieved April2011)

[106] ESCWA (2009). *National profile of the information society in the Sudan.* E/ESCWA/ICTD/2009/12/Add.11, United Nations. Economic and Social Commission for Western ASIA (ESCWA), New York.

[107] Mahdi, M. O. S. and Dawson, P. (2007). The introduction of information technology in the commercial banking sector of developing countries: voices from Sudan, *Information Technology & People***20**: 184-204.

[108]http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/SUDANEXTN/0,,menuPK:375432~pagePK:141132~piPK:141107~theSitePK:375422,00.html (retrieved September2011)

[109] http://www.cia.gov/cia/publications/factbook (retrieved April2011)

[110] NCSP. (National Council for Strategic Planning), (2001), *National strategy for ICT industry* (unpublished Report), Sudan.

[111] http://egov.comesa.int/index.php/fr/regional-e-government-framework (retrieved March2010)

[112] http://nic.gov.sd/ (retrieved March2014)

[113] Neuman, W. L. (1994). *Social research methods: Qualitative and quantitative approaches Volume2*. Allyn and Bacon Boston USA.

[114] Remenyi, D., Williams, B., Money, A. and Swartz, E. (1998). *Doing research in business and management*, SAGE, London.

[115] AL-Shehry, A., Rogerson, S., Fairweather, B. and Prior, M. (2006). *The motivations for change towards e-government adoption: Case studies from Saudi Arabia*, , Brunel University, UK.

[116] McGrath, J. E., Martin, J. and Kulka, R. A. (1982). *Judgment calls in research,* SAGE Publications Inc, Beverly Hills, CA.

[117] Yin, R. K. (2003). *Case study research: Design and methods Volume3* SAGE, Thousands Oaks, CA.

[118] Robson, C. (2002). *Real world research Volume2* Blackwell, UK.

[119] Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed method approaches Volume2* SAGE, Thousand Oaks, CA.

[120] McMillan, J. H. and Schumacher, S. (2001). *Research in education: A conceptual introduction Volume5* Longman, New York.

[121] Royce, D. (1995). *Research methods in social work Volume2* Nelso-Hall Publishers, Chicago.

[122] Merriam, S.B., (1998). *Qualitative research and case study applications in education*, San Francisco. Jossey-Bass.

[123] Cornford, T. and Smithson, S. (2006). *Project research in information systems Volume2* Palgrave, London.

[124] Altameem, T. A. (2007). *The critical factors of e-government adoption: An empirical study in the Saudi Arabia public sectors* (Ph.D. thesis), Brunel University, Uxbridge.

[125] www.nova.edu/ssss/QR/QR2-3/nau.html (retrieved April2013)

[126] Yin, R. K. (2009). *Case study research: Design and methods Volume4* SAGE, Thousand Oaks. CA.

[127] Weber, R. (1995). *Basic content analysis,* SAGE, Thousand Oaks. CA.

[128] Krippendorff, K. (2004). *Content analysis: An introduction to its methodology,* SAGE, Thousand Oaks. CA.

[129] Wood, C. (2005). *Security Policy Made Easy Volume10* Information Shield, U.S.

[130] Lankhorst, M. (2005). *Enterprise Architecture at Work Volume1* Springer, Berlin.

[131] Tudor, J. K. (2002). *Information Security Architecture-An Integrated Approach to Security in the Organization Volume2.* Auerbach USA

[132] Smith, D. A. and Garton, P. R. (1989). Specifying specific deterrence, *American Sociological Review* **54**: 94-106.

[133]https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Risk_Management.pdf (retrieved April2016)

[134] Kesh, S, Nerur, S. and Ramanujan, S. (2002). Quality of Service – Technology and Implementation. *Information Management and Computer Security* **10**:85-91.

[135] Gottfredon, M. and Hirschi, T. (2007). A General Theory of Crime. *International Journal of Offender Therapy and Comparative Criminology***3**:1-18.

[136] Mozamel M. Saeed, (2014). General Characteristics of Software Development Companies in Sudan and its Impact on Production. *International Journal of Engineering Science and Innovative Technology* **3***:*72-77.

[137] L. Jorgensen (1989). *Participant Observation A Methodology for Human Studies Volume15.* Sage. London.*UK.*

[138]C.R Kothari (2004). *Research Methodology Method and TechniquesVolume2.* New Age International. New Delhi.

[139]http://unpan1.un.org/intradoc/groups/public/documents/UNPAN/UNPAN035135.pdf (retrieved May2016).

[140] Nkwe. N (2012). E- Government: Challenges and Opportunities in Botswana. *International Journal of Humanities and Social Science***2**:39-48

[141] Lankhorst. M.(2009). *Enterprise Modelling, Communication and Analysis Volume2.* Springer. London. UK.

[142] Layne. K, Lee. J (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly***18:**122-136.

[143] Al-Azazi, S (2008). *Amulti-layer model for e-government information security assessment*. Grandfield university, dubai

[144] Hana, M (2013). E-Government Cloud Computing Proposed Model: Egyptian E_Government Cloud Computing. *International Conference on Advances in Computing, information security technical report*. **6**: 60 – 70.

[145] Waziri , M. Yonah , Z. (2014). *A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania*. *Advances in Computer Science: an International Journal* **3**: 98-106.

[146] G. Karokola and L. Yngström, (2009). Discussing E-Government Maturity Models for the Developing World- Security View. *Information Systems Security Association* Pp81-98.

[147] Zhang, F.(2008). Design of E-government Security System based on Information Security Model. *2008 International Conference on Advanced Computer Theory and Engineering*. **(***Research Center of Cluster and Enterprise Development***)** Pp359-362. Jiangxi

[148] www.clknet.or.tz J. Yonazi, Adoption of Transactional Level e-Government Initiatives in Tanzania. (Retrieved 13Apr2014)

[149] www.utumishi.go.tz, President's Office, Public Service Managements, Tanzania e-Government Strategy, ed, 2012. (Retrieved 10Feb2013)

[150] Erl, T, (2005). *Service-oriented Architecture: Concepts, Technology, and Design.* Volume2. Upper Saddle River: Prentice Hall PTR, USA

[151] Ziyao W, Junjie N, Z Duan, (2008). SOA core technologies and application, Publishing House of Electronics Industry, Beijing, Pp.495-497, University of Finance and Economics. China

[152] L Lin, Yongzhao Z, Yi N. (2006) Improved RBAC model based on organization. Journal of Jiangsu University (Natural Science Edition) **27**(2):147-150

[153] Zeng Zhongping, Li Zonghua, Lu Xinhai. (2007). The Access Control Policy Study of E-government Information Resource Based on RBAC. *Journal of Information,* **10**:39-41

[154] Barka E, Sandhu R S. (2000). Framework for role-based delegation models. *In: Proc. of the 16th Annual Computer Security Application Conf. IEEE Computer Society Press*. Pp 168-176

[156] Asgarkhani, M. (2005). Digital government and IT effectiveness in public

management reform, a local government perspective. *Electronic Journal of e-Government* **7(3)**: 465-487.

[157] Dutton, W. H. and Shepherd, A. (2006). Trust in Internet as an experience technology , *Information Communication & Society* **9(4):** 433-451.

[158] Zviran,M. and Haga, W,J. (1990). *A COMPARISON OF PASSWORD TECHNIQUES FOR MULTILEVEL AUTHENTICATION MECHANISMS.* NAVAL POSTGRADUATE SCHOOL. California.

[159] Morris, R. and Thompson, K. (1979). Password Security: A Case History. *Association for Computing Machinery*. **22**: 594-597.

[160] Peter G. Neumann RISKS OF THE PASSWORD. (1994). *Association for Computing Machinery*. **37**: 126-126.

[161] Anita K. Jones (1981). Password Authentication with Insecure Communication. *Association for Computing Machinery* **24**:770-772.

[162] Hong, J. and, Reed, D. (2013). Passwords Getting Painful, Computing Still Blissful. *Association for Computing Machinery* **56**: 10-11.

[163] Communications. *(2000). Securing User Passwords*. *Association for Computing Machinery* **43**: 11-12.

[164] Adams, A. and Sasse, M, A. (1999). USERS ARE NOT THE ENEMY. *Association for Computing Machinery* **42**:40-46.

[165] http://csrc.nist.gov/. (Retrieved 18Dec2016)

[166] Cheswickm W. (2012). Rethinking Passwords. Our authentication system is lacking. Is improvement possible? *Association for Computing Machinery* **11**: 1-7.

[167] https://www.nist.gov/ (Retrieved 11Dec2016)

[168] Ives, B. Walsh, K. R. and Schneider H. (2004) The Domino Effect of Password Reuse. *Association for Computing Machinery* **47**:75-78

[169] JAIN, A, K. and ROSS, R. (2004) Multibiometric Systems. *Association for Computing Machinery* **47**:34-40

[170] Karen Renaud and Antonella De Angeli (2009). Visual Passwords: Cure-All or Snake-Oil? *Association for Computing Machinery* **52**:135-140.

[171] Hassan R. G., Khalifa O.O. (2016). Towards user Awareness and Acceptance of Sudan E- government: Adoption and Security perspective. *Third International Conference for ICT in education and training*. Pp 280-289. Khartoum

[172] Bojinov, H. Sanchez, H. P. Reber, Boneh D. and Lincoln P. (2014). Neuroscience Meets Cryptography: Crypto Primitives Secure Against Rubber Hose Attacks. **57**:110-118.

[173] Ghafir, I; Prenosil, V; Alhejailan, A; Hammoudeh, A.(2016). Social Engineering Attack Strategies and Defence Approaches. *Institute of Electrical and Electronics Engineers* **0***:*145-149.

[174] K. Mitnick with W. L. Simon. (2005) The Art of Intrusion: the Real Stories behind the Exploits of Hackers, Intruders and Deceivers.

[175]Tucker Bailey, Josh Brandley, and James Kaplan, "How good is your cyber incident response plan?" McKinsey Quarterly, December 2013.

[176] Osuagwu E. U. and Chukwudebe G. A, SMIEEE, Salihu T., SMIEEE* and Chukwudebe V. N+. (2015). Mitigating Social Engineering for Improved Cybersecurity. *Institute of Electrical and Electronics Engineers.Pp 91-100*. International Conference on Cyperspace. Abuja.

[177]http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-031-eng.htm(Retrieved 22Dec2016)

[178] Edrees R. and Khalifa O. (2015). Challenging Development Citizen-Centric E-Governance in Sudan. *International Journal of Innovative Science, Engineering & Technology.* **42***:*451-456.

[179]] J. Rotter, "Generalized expectancies for interpersonal trust", American Psychologist, Vol. 26, No. 5, pp. 443-452, May 1971, http://dx.doi.org/10.1037/h0031464.

[180] F. Bélanger, and L. Carter, "Trust and risk in e-government adoption", The Journal of Strategic Information Systems, Vol. 17, No. 2, pp. 165- 176, June 2008, http://dx.doi.org/10.1016/j.jsis.2007.12.002.

APPENDICES

Appendix A: Questionnaire A

Distinguished government department leader information

Questions to Security related

This questionnaire is designed to specify the critical factors (threats) affecting e-government security in Sudan. We have identified several risks factors as reported in the academic literature, which are considered as the important.

Threat (A): Technical layer:

This type of threats related to technical factors called technical layer. The layer is divided into detailed layers called sub-layers.

TA1: *Unauthorized access to a place or other resource*

□ Important

□ Neutral

□ Not-important

TA2: *Information* interception

□ Important

□ Neutral

□ Not-important

TA3: *Information tampering*

□ Important

□ Neutral

□ Not-important

TA4: *Denial of services attacks*

□ Important

□ Neutral

□ Not-important

TA5: *System resources stealing*

□ Important

□ Neutral

□ Not-important

TA6: *Information faking*

□ Important

□ Neutral

□ Not-important

Threat (B): IT infrastructure layer

This type of threats related to IT infrastructure factors called IT infrastructure layer. The layer is divided into detailed layers called sub-layers.

TB1: Lack of technical skills

□ Important

□ Neutral

□ Not-important

TB2: Lack of users' trust and confidence to use e-government services.

□ Important

□ Neutral

□ Not-important

TB3: Lack of consultation

□ Important

□ Neutral

□ Not-important

TB4: Lack of software houses

□ Important

□ Neutral

□ Not-important

Threat (C): Managerial layer:

This type of threats related to managerial factors called IT managerial layer. The layer is divided into detailed layers called sub-layers.

TC1: Lack of Budget

□ Important

□ Neutral

□ Not-important

TC2: Lack of policy and regulation for e-usage in Sudan

□ Important

□ Neutral

□ Not-important

TC3: Resistance to change in top management and administration

□ Important

□ Neutral

□ Not-important

TC4: Conflict of interest

□ Important

□ Neutral

□ Not-important

TC5: Social engineering attacks

□ Important

□ Neutral

□ Not-important

TC6: Lack of physical security

□ Important

□ Neutral

□ Not-important

Threat (D): Law and legislation layer:

This type of threats related to law and legislation factors called law and legislation layer. The layer is divided into detailed layers called sub-layers.

TD1: Lack of law and legislation related to e-government

□ Important

□ Neutral

□ Not-important

Appendix A: Evaluation form to evaluate some academic and specialists

Factors that lead to the success of the models	**Description**	**Rate**			
Simplicity of the model	The model must be clear to the targeted users or stakeholders (government departments or individuals). The layers of the model must be explicit should make sense to a non-security or IT expert.	SA	A	N	D
The possibility of applying	The model must be appropriate to any organisation which plans to use it for its internal or external communication or information sharing.	SA	A	N	D
Standards compliant	The model must meet the terms with the security standards in terms of acronyms, references, objectives.	SA	A	N	D
Achievable	The model must be possible for the e-government authority and its government affiliates.	SA	A	N	D
Flexible	The model must be flexible and can be implemented in phases.	SA	A	N	D

Open standards	The model must tackle general technologies, and non-technologies issues.	SA	A	N	D
Renewable and expandable	The model must be easy to renew with the introduction of new trends in the security field and it also can allow merge group of security technologies.	SA	A	N	D