E-Government - an Information Security Perspective

Rasha G. Hassan [#1] and Othman O. Khalifa [*2]

[#1] Faculty of Computer Science and Information Technology
Sudan University of Science and Technology, Sudan
[*2] Electrical and Computer Engineering
International Islamic University Malaysia, Malaysia

Abstract *The growth and rapid adoption of the Internet has greatly changed how all organizations deal with their respective stakeholders. As the move from administrative operations to service operations accelerates, e- government Network Platform is a solution to transform the way they do business and services. As well know, the E-government is a website that provides reliable content based on a strong infrastructure of a digital network, application servers and internet, an extensive database and other supporting services. It requires more advanced and secure e-Government networks to protect data from growing security threats and risks. Threats include unauthorized access to resources, malicious damage, and data intercepts. Security risks include virus, cyber-attacks, and key information leakages. Experts agree that the majority of government information leaks occur on networks, making information leakage control critical in government network design.*

Keyword: *E-government, Security, technical models, non-technical models, Trust.*

I. Introduction

Electronic government (e-government) or e-Gov is the use ICT tools and applications, wither it was internet-based or non-internet based to make better interaction through different delivery models and activities between government and citizens (G2C), government and business/commerce (G2B), between government agencies (G2G), or government and Households (G2H) (Valentina, 2004), but it may face a number of limitations that affect the way of interaction. Figure.1 illustrates agencies as a service provider and how information flow citizens.

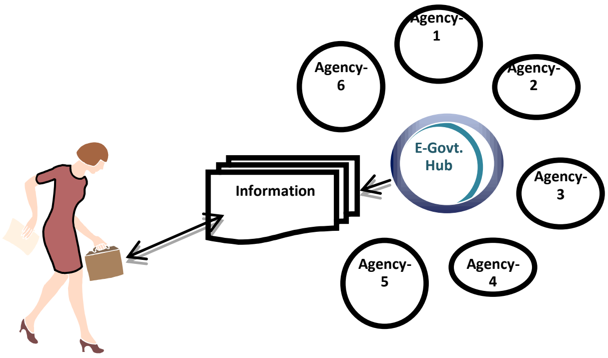


Figure.1 Typical E-Government Architecture Model

As the growth of using Internet through information revolution era, risks are increased and the need for security is become the most important thing to protect our valuable assets and to build trusteeship, therefore “Information security” the field arises to concern about providing security for the technical risks – including host security, network security and Internet security - and non-technical risks – including ethical issues, physical assets and also natural disasters – this field is always seek to provide confidentiality, authentication, availability and integrity of information.

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

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

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

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

1.4. A breach of security may be compromised to yield lack of availability of information to citizen, where majority of e-government projects in developing countries fail (J. Jang-Jaccard & S.Nepal, 2014) (Danish , 2006).

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

Figure.2 shows the need for secure relation between citizens and agencies through e-government.

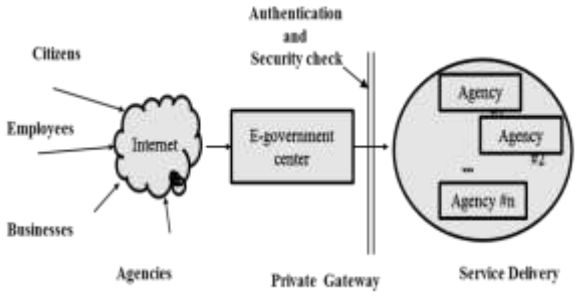


Figure.2 securing service delivery

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

II. LITERATURE REVIEW

A. *Problem of authentication:*

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

A.1. Binding force

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

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

A.2. Confidentiality

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

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

B. *Security Issues in E-government:*

In the designing of an efficient e-Government system, security becomes the main issues to be considered. E-Government system is type of on-line system that require a ICT based network to execute properly but e-Government system is different from other on-line system particularly with reference to security as an e-Government system handles a lot of secure and legal information that must be protected from unauthorized users. The Canadian Government is using an advanced Web portal called BusinessGateway.ca not only making available information and communication similar to the Austrian Help.gov but also secure transaction services for businesses (Alexander, 2003). Security is critical for their successful implementation for e-Government and transaction based services. Some of the security issues in e-Government are discussed below:

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

Table1: Security Threats and their solution in an on-line system/project(Alexander, 2003)

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

C. Technology Framework for Online Trust

C.1 Digital Envelope

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

C.2. Digital Signature

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

C.3. Digital Certificate

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

D. Industry Solutions for Online Trust and Security

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

E. United Nations as a great environment that evaluate the use of e-government:

According to the 2012 United Nations E-government Survey rankings, the Republic of Korea is the world leader (0.9283) in the use of e-government followed by the Netherlands (0.9125), the United Kingdom (0.8960) and Denmark (0.8889), with the United States, France, Sweden, Norway, Finland and Singapore close behind, this according to the UN's 2012 e-Government Readiness Index. The survey focuses on to what degree countries involved the use of ICT in different areas such as entrepreneurship, innovation, research and development, promoting distance learning, e-health, the use of cellular technology, Bridging the digital divide, therefore the United Nations e-government assessment concentrate on the concept of integrated services that exploit inter-linkages (may be interoperability) among different public services (United Nations, 2012), however they didn't assess any security aspects in e-government.

F. Applications of e-government and provided security:

F.1. Electronic voting machines will become important to be adopted by many countries, however any failure in electing the correct candidate may result in untruthfulness (Dominique, et al, 2007), these errors may be due to the interfaces are not well designed or software bugs or even hardware malfunctioning, ensuring validation in software may be good solution, however it's not provide a total security.

F.2. Some countries e-transaction through e-government portal, such as retrieving driving citations, require confidential information and authentication and data may be exposed to modifications, (Danish , 2006) suggest a good solution that preserve Authentication, Confidentiality, Integrity and Non-repudiation of data through different levels as the most critical characteristics of secured data, however the study concentrate a specific application underplaying the risks comes from other e-government applications and underlying infrastructures.

F.3. Another threat may appear from the use of e-government application is cloning and tampering passports electronically (Luca & Dario, 2014) the e-passport contains the information on chip and according to International Civil Aviation Organization (ICAO), The chip stores owner's personal data and biometric features, and other information, in (Luca & Dario, 2014) provide a comprehensive study which views that the inspection process of e-passport doesn't reject a document in many cases such as old version chips or using different security protocols while passport is valid hence it durable from 5 to10 years, this may be vulnerable and attacker may exploit it and ignore a security measure to accept reading chip information and clone it into a new blank chip and tampering information, additional check is provided as an enhancement security to control inspection process so, it cannot be sidestepped by the attacker(Luca & Dario, 2014), however it's not official implemented yet.

G. Assessment of e-government security:

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

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

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

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

- Technical models: such as Bell-LaPadula (BLP) Model(focus in confidentiality), BibaModel(focus on integrity), Clark-Wilson Model(focus on integrity), The Chinese Wall (focus on Privacy and integrity), Lambrinoudakis Security Framework (availability and authentication), InfosecModel (focus on availability, integrity and confidentiality) (Alharbi, 2013), (Sabri, 2008).
- Non-Technical Models and Theories: such as Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Technology Acceptance Model (TAM), Diffusion of Innovation (DOI), Motivational Model (MM), Social Cognitive Theory (SCT), Model of PC Utilization (MPCU), Unified Theory of Acceptance and Use of Technology (UTAUT), the last model encompasses all above non-technical theories, where Figure.3 state a relation between the eight factors of accepting new technologies.

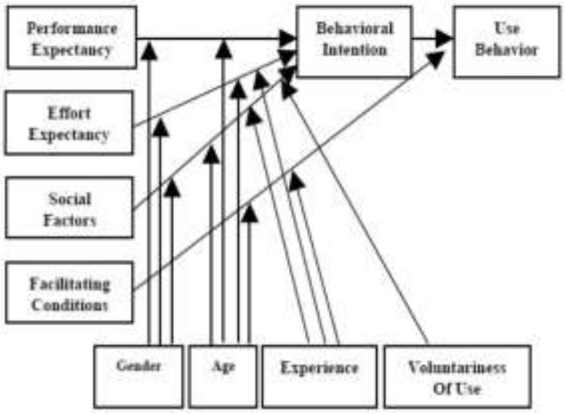


Figure .3: the eight factors of UTAUT (Alharbi, 2013)

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

H. Biometrics and Security in E-government:

Government systems wither it was electronic or non-electronic need to ensure identity and authentication of citizen, bioinformatics as a science uses computers to better understand biology, with the aid of biometric as a tool can asset in the field of computer forensics that search the evidence about cyber-crime, the biometric systems may function either in verification mode or identification mode; where systems need to perform a number of comparing and recognizing processes to deal with authorized user, biometrics data may be characterized through face recognition, fingerprint, Iris, voice, hand & finger geometry, whoever there are possible attacks on biometric systems as shown in figure.4 (Piyush et al, 2012).

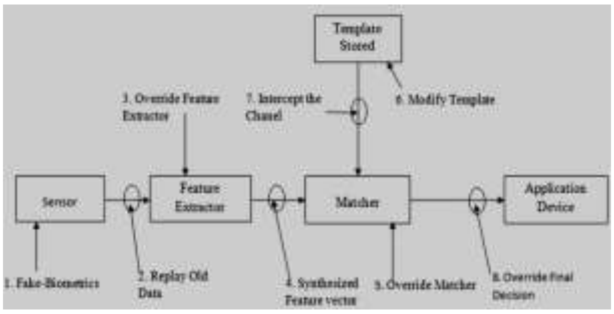


Figure.4: shows possible attacks on biometric systems

As in (Piyush et al, 2012) there is a proposed system to recover vulnerabilities rely on applying two security strategies (diversity of defence and defence in depth strategies) which consider an advantage. The solution shown in Figure.5 depends on four mechanisms

a. Multi-biometrics: do not depend on a single biometric data i.e. use fingerprint, iris, face, hand geometry or voice all together.

b. Use sequence number: protection from replay old data.

c. Access control: use of multilevel security

d. Cryptographic techniques: use of encryption algorithms or digital signature

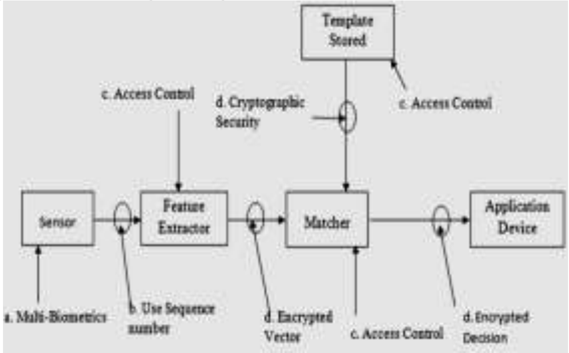


Figure.5: Solution to remove vulnerabilities in system (Piyush et al, 2012)

I. Cloud computing and security in E-government:

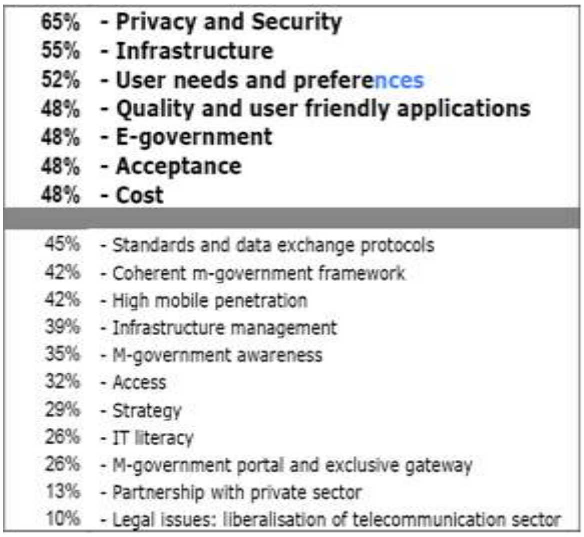
Could computing is a technology to provide a service to clients through Internet in different models, a) Infrastructure as a Service (IaaS), b) Software as a Service (SaaS) and c) Platform as a Service (PaaS) (Charalampos, Marinos , 2011), (Bernd et al, 2013), Although cloud computing has a number of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

The study (Smitha & Chitharanjan, 2012) proposed a new mechanism for database encryption with flexible performance and database access, where it ensuring confidentiality of government sensitive data. The mechanism rely on an encrypt/decrypt AED (advanced encryption standard) symmetric key algorithm, which encrypt all data before storing into the cloud, it uses coarse index to improve the query performance which avoid the full table scan, once the scheme uses secret keys the proposed solution is to embed the key in a finger print image that uses DCT based image (Ali, 2013).

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

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

The research (Shadi et al, 2007) study the transition from E-government to M-government and stating the success factors as it is shown in Figure 6, the factors are ordered according to the importance percentages, where the privacy and security considered as the most important factor that affects on the use of M-government.



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

Figure 6: M-Gov success factors and importance percentages (Shadi, 2007)

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

K. Building trust through authentication:

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

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

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

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

III. PROPOSED FRAMEWORK FOR SECURING E-GOVERNMENT:

Providing secure e-government services is challengeable and critical issue, so that the government and the users trust the system and feel confident in using it. An extensive study is required to encompass all factors that affect on e-government services, e-Government services face a lot of security problem such as: identity theft, hacking and denial of service or issues related with e-government users, or invader who steals the information from the government or other agencies. So, protecting the citizen's privacy, security and giving them assurance that their information will be violated or changed became the important aspect of service success, however all these aspects are related to technical issues, still we need to examine the none technical issues such as social engineering.

Social engineering are used to compromise security which considered as a non-technical threats exploited a human factor technique, attacker uses deception, persuasion, and influence authorized users to get information, where he easiest way to get into a computer system is to simply ask permission. As result of these threats attacker gain unauthorized access to act sabotage and vandalism or espionage and trespass on governmental information through,

Constructing a framework need to review the strength and weakness of existing framework/models/approaches. Figure .7 illustrates proposed framework that tackle both technical and non-technical issues act as a unified framework for securing e-government by integrating the existing models and theories according to requirements. E-government unified security Framework (e-GUSF) this may consider an appropriate Framework to gain trust.

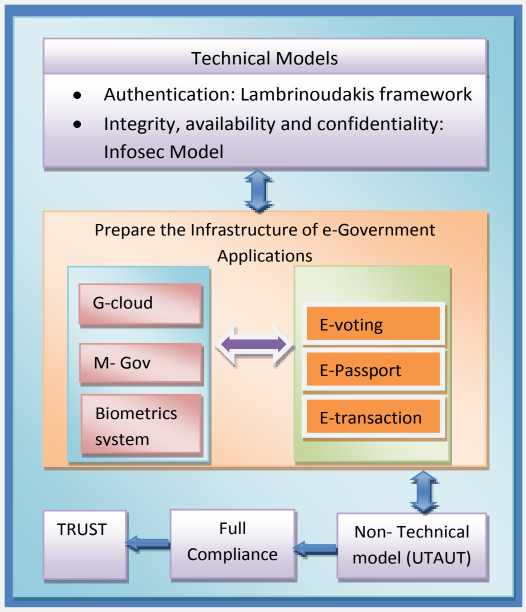

Technical Models
Authentication: Lambrinoudakis framework
Integrity, availability and confidentiality: Infosec Model
Prepare the Infrastructure of e-Government Applications
G-cloud
M- Gov
Biometrics system
E-voting
E-Passport
E-transaction
TRUST
Full Compliance
Non- Technical model (UTAUT)

Figure. 7: eGUSF in context diagram

A. *Technical models:*

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

- Lambrinoudakis security framework:

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

- InfoSec model:

This model can minimize the vulnerabilities and security holes of completed attacks and selecting the best action to protect the system from electronic eavesdropping (Alharbi, 2013), it covers availability, integrity and confidentiality of information, Figure.8 represent the InfoSec model which considered as a multilayered model (Sabri, 2008).

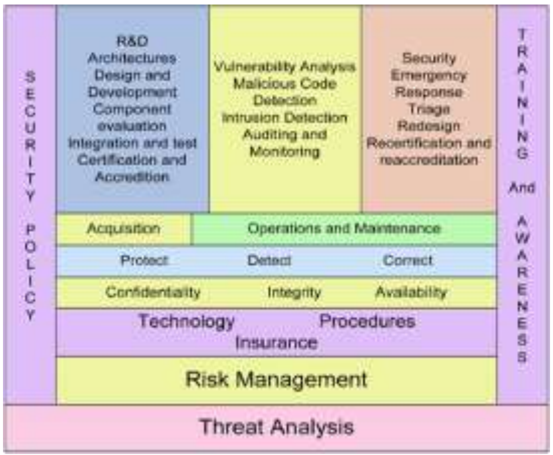


Figure.8 the InfoSec Model

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

B. *Non- Technical model*

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

C. *Prepare the Infrastructure of e-Government Applications*

This part is about to build the appropriate security measure to the infrastructure of each e-government services and provide secure communication between them, in addition apply the technical models that provide solutions to ensure authentication of users, availability, integrity and confidentiality of information.

The use of chosen models above will fit with the requirements of securing e-government services; however implementation should go through the following steps:

1. State security requirements of e-services: review what/how/when to access information; state the priorities and privileges according to e-service.

2. State security strategies: according to security requirements state the strategy and the defence mechanism wither (diversity of defence, defence in depth, choke point, and weakest link, least privilege, etc) it's recommended to combine mixed defence mechanism.

3. State security policy: once the requirements and strategies states well, it's time to write down a document as a regulations and procedures of incident handling to adhere every one for the acceptable use.

4. Build secure integrated infrastructure according to e-service: the great structure may PKI and using other tools and techniques.

5. Evaluation: test the validity of the chosen models.

6. Risk assessment and review: this step may lead to recycle step one in the approach.

IV. Conclusion

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

References

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

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

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

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

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

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

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

8) Dilip Kumar Sharma, Vinay Kumar Pathak and G.P. Sahu, Digital Watermarking for Secure E-Government Framework, Computer society of India.

9) Dimitrios Zissis, Dimitrios Lekkas, (2011) Securing e-Government and e-Voting with an open cloud computing architecture, Government Information Quarterly 28 239–251.

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

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

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

13) Geoffrey Rwezaura Karokola, (2012) A Framework for Securing e-Government Services, PhD Thesis , Stockholm University,Sweden

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

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

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

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

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

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

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

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

22) Rabah Alshboul, (2012) Security and Vulnerability in the E-Government Society, Contemporary Engineering Sciences, Vol. 5, no. 5, 215 – 226

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

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

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

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

27) Sofia Elena Colesca , (2009) Understanding Trust in e-Government, ISSN 1392 – 2785 Inzinerine Ekonomika-Engineering Economics(3).

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

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

30) Valentina (Dardha) Ndou, (2004) E-government for developing countries opportunities and challenges, EJISDC , 18, 1, 1-24

31) Zhou Feng, (2012) The research and implementation of a unified identity authentication in e-government network, physics procedia 242032 – 2038