Journal of Theoretical and Applied Information Technology
15th March 2019. Vol.97. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI-LAYER FRAMEWORK FOR SECURITY AND PRIVACY BASED RISK EVALUATION ON E-GOVERNMENT

[1]AJI SUPRIYANTO, [2]JAZI EKO ISTIYANTO, [3]KHABIB MUSTOFA

[1]Department of Information Technology, Universitas Stikubank, Indonesia

[123]Department of Computer Science and Electronics, Faculty of Mathematics and Natural Sciences, Gadjah Mada University, Indonesia

E-mail: [1]ajisup@edu.unisbank.ac.id, [2]jazi@ugm.ac.id, [3]khabib@ugm.ac.id

ABSTRACT

Security and privacy are an important aspect of *e-Government*'s success in providing online services to the public. The increase of electronic service usage including e-Gov can cause various risks, safety risks, and user's privacy risks. The lack of concern of security and privacy gives impact to some]problems of data and information so as to make the lack of public confidence in e-Gov services. So far the concern is the security aspect, while privacy is less attention. In many cases, the privacy aspect has many violations. This study aims to develop a *multi-layer* security and privacy framework as a basis for the evaluation of risk-based e-Government risk awareness. The steps in this research are creating the objectives of the security and privacy framework, the identification of requirements and the relevance of requirements, constructing the inclusive security aspect, identifying of the multi-layer framework, developing the development framework, and determining the elements for the risk-based evaluation model. The contribution of this research is the compilation of a multi-layer framework model for security and privacy. The relationship between the security and privacy domains forms a complete element of security and privacy which is the development of the Salman multi-layer framework. The resulting framework can be used as a basis for conducting security based on risk evaluations involving privacy factors.

Keywords: *Framework, Requirements, Security, Privacy, Multi-layer*

1. INTRODUCTION

E-Government (e-Gov) is an important tool that provides information and services to communities that can improve the efficiency, effectiveness and performance of public sector organizations[1]. E-Gov services may experience technical or non-technical security issues. In addition, the success of e-Gov services depends on the acceptance of its users[2]. This is related to the ability of e-Gov in interacting with users, collecting information and interconnected communications from feedback to users[3]. The ease usage of e-Gov services can cause some threats such as security threats in the absence of policies and strategies for secure access and information protection[4]. In e-Government governance, security protection is one of the biggest problems[5].

There are three major challenges of adoption on e-Gov, first, the application of technology; second, security and privacy issues, and infrastructure and administration; and third, is a social challenge[6]. The obstacle factor of e-Gov governance is the access of government system by so many users, big deals at all times, the sensitivity of personal information of citizens, the need to hide confidential government information, need to secure information systems and network channels[7]. Similarly with privacy, protecting citizens' privacy must become a government priority to gain the trust in e-Gov initiatives[4]. Security and privacy are major problems in communication through Internet[8]. It is important to understand the relationship between information security and privacy, and it is necessary to apply engineering system and risk management process that can solve the problem of security and privacy concerns[9]. Security issues need to get major attention in building e-Gov confidence[10]. The first step of e-Gov's security development concentrates on secrecy, and in its development, the need for privacy is essential[11]. The relationship between the community as the user of e-Gov

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

service with the device used affects security and privacy concerns[12].

Security threats are so dynamic and massive, therefore an evaluation policy is needed. One of the best ways to solve security issue is through a risk-based approach[13]. In order to conduct an evaluation of security and privacy assessments, it needs everything which is based on an evaluation framework. The framework can be used to guide planning and decision-making for e-Gov and to help identify unique issues for each stage of its compilation[14]. The framework for measuring e-Gov services in the context of the quality and quantity of e-Gov security services can provide increased security[15].

This study aims to develop a multi-layer framework as a basis for risk-based security and privacy evaluation on e-Gov. Motivation of research is to increase public confidence in the protection of security systems and maintain the privacy of e-Gov users. So that the research question is what aspects are needed to form inclusive security?

2. SECURITY PROTECTION AND PRIVACY

2.1 The requirement of Security and Privacy

Security is protection against threats. The framework of e-Gov security consists of three key elements: people, processes and technology[15]. The main objectives of the application of security are the protection of confidentiality, integrity, trust and asset availability[16]. The elements affecting e-Gov security are technological, physical, and human elements. Privacy is about the scarcity of personal data creation and the maximization of individual control toward their personal data[17]. Privacy ensures that information of the user is hidden from spies[8]. The purpose of privacy is to protect personal data, to ensure the legitimacy of personal and sensitive data processing, to comply with the right of information, and to ensure the confidentiality and security of personal data[17]. Privacy is related to personally identity information (PII). Protecting individual privacy is a fundamental responsibility of government organization. This is to build citizens' trust in e-Gov initiatives[4]. Privacy in an e-Gov perspective is a key building of citizen trust in using e-Gov services. The privacy layer of e-Gov consists of user privacy, service privacy, and data privacy[18].

Security requirements overlap with privacy requirements despite addressing different issues[19]. According to Salman, the security requirement of e-Gov is related to Confidentiality, Integrity, Availability, and Authentication (Authentication)[20]. The main criteria for evaluating e-Gov security are based on general security principles of Confidentiality / Privacy / Accessibility (C), Integrity (I), Accountability / Non-repudiation (A), Authentication (A), and Trust (T)[21]. The Privacy Terms consist of Unlinkability (U), Anonymity and Pseudonymity (An & P), Plausibility and Deniability (Pl & D), Undetectability and Unobservability (Ud & Ub), Confidentiality (C), Awareness (Aw.), And Compliance (Cp.)[22]. The privacy policy determines which data is being processed, how it is collected, where it is stored, what it is for and so on. The privacy requirements must not only complete the need of the users but also comply with the laws, standards, and service policies[23]. The security needs involving privacy by Tassabehji[24] and Zu'bi[25] are called inclusive security, aiming to increase citizen confidence.

2.2 Dimension and Relation between Security and Privacy

The dimensions or security domains are available on the site to provide security access to all application and facilities which is provided by e-Gov. Dimensions of security and privacy include Security, security technology, competence, operations and management, physical and environmental, and decisions[25]. Meanwhile, according to Kessler[26], domain privacy requirements in e-Gov include policy domains, technology, and citizens.

Security issues occur from illegal behavior system. The privacy issue comes from the product of the authority of the process of Personally Identifiable Information (PII)[22]. The issue of privacy and security is conceptualized as something different. Privacy issues on the Internet include tracking the use and collection of data, choice, and information sharing with third parties[27]. The security issues include incidents, threats, and security risks. Privacy focuses on the individual's ability to control the collection, use, and deployment of PII, with a primary focus on data collection. Meanwhile, the security provides a mechanism to ensure confidentiality, integrity, and availability. Therefore, security is focused on protecting data once when it is collected. Privacy is related only to personal information, whereas security and confidentiality can relate to all information[28].

The concept of privacy and security, however, they are intersected. In particular, the control of certain IT services created to ensure the confidentiality and integrity of the security

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

perspective also supports the privacy goals. For example, access controls ensure that only authorized individuals can read, alter, or delete PII[29]. The controls help to achieve confidentiality and integrity from a security standpoint. This helps ensure that the use of PII is limited to legitimate purposes and protection from unauthorized access, destruction and disclosure[28]. Privacy and security have a relationship with the concept of perceived risk[22]. Security also has a direct effect on trust. It shows a close relationship between trust and security in e-Gov (Colesca, 2009) in[4].

2.3 The Framework

The development of the e-Gov framework aims to define and classify e-Gov according to the use of advanced technology, citizen and government involvement[24]. The framework for building e-Gov confidence has five dimensions: human (ethics), information (content), Technical, Policy (law / legislation), government (politics) [30]. Fulfillment of the legal aspects (legislation) is one of the important dimensions in the governance framework of e-Gov security[7]. Legislation becomes a foundation for building trust, security and protecting citizens' privacy (Al-Omari & Al-Omari, 2006) in[4].

The framework can be used to guide planning and decision-making for e-Gov and to help identify unique issues for each stage of its compilation[14]. The framework needs to consider three obstacles: laws and regulations, technical feasibility, and user feasibility. The security framework is a development guide used to construct a security problem-solving structure. The e-Gov security framework consists of three main elements; people, processes and technology. The framework for measuring e-Gov services in the context of quality and quantity of security services and e-Gov services can provide security improvement[15].

2.4 Evaluation and Assesment Based Risk

Evaluation is a validity testing activity of the selected model, by providing feedback for development or development purposes. The evaluation is one of the most important steps in building the framework. Evaluation of e-Gov security can be used to increase the level of e-Gov, as well as the basis for determining the level of e-Gov security readiness[31]. Evaluation is also a way of measuring security performance[32]. e-Gov security evaluation can be used to increase the level of e-Gov[33]. The primary objective of assessing security is to identify all possible threats and attacks. An assessment measure that can be used as a guide in determining the e-Gov development stage is required. So it can be known the level of readiness and maturity of e-Gov[34].

One of the best ways to solve problems is through a risk-based approach. Risk assessment provides an accurate evaluation of assets. Any security that is applied needs to be evaluated for security assessment[13]. The purpose of the risk assessment is to identify all possible risks to the assets owned and evaluate them accurately to reduce risk appropriately[35]. A holistic approach is made inclusive of trust in the security system including the socio-technical security approach[24]. This paper discusses the framework as a basis for evaluation of inclusive security with a risk-based approach involving privacy to improve e-Gov security trust.

3. PREVIOUS STUDY

In the research Maskani[36] recommends a comprehensive engineering requirements security (SRE) method for developing a security framework. Maskani measures the quality of e-Gov with ISO framework based on 8 dimensions, one of them is Security, consisting of 5 sub-demension that is Confidentiality, Integrity, Non-repudation, Accountability, Authenticity. Al-Azazi[30] research describes a new framework that can be used as a tool to assess the level of e-Gov security readiness. Al-Azazi's[30] proposed multi-layer model can be implemented as an architecture or assessment tool, developing a multilayer (5-layer) model representing: technology, security policy, competencies, operational procedures, and above all the decision factors that play a role major in enforcing other layers. Multi-layers are used to facilitate the arrangement of the factors and security sub-factors involved which comprise 44 security elements. The approach used is qualitative. The generic model is suitable for *multi-layer* security approach[30]. The reasons for selecting *multi-layer* models in e-gov security framework are more structured than best practice models such as COBIT, BS7799, Bell lapadula, Biba, BSI II. In addition, it includes more complete aspects of technology, policy, behavior and human awareness, operations and management, making it suitable for e-Gov[30].

Al-Azazi's[30] research was further developed by Salman[20]. It discussed the recommendations proposed by Al-Azazi[30] which is combined the quantitative approach with a mathematical model to find sub layer combinations or IT Model subjects on each layer. The multi-layer model is also added to 6 layers, in example 1 layer

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

plus the physical layer before the decision layer, and consists of 59 security elements. These results it can be concluded that the proposed method is effective and reasonable and can provide support for the establishment of e-Gov. FEMRA method was previously used by Joints (for the risk assessment process of the Information Security Management System). It is proposed the creation of a generic-based generic framework to produce a special standard of risk management-based security management, in order to generate more effective value as it is based on criteria specific to an organization for in identifying sources and perceives risk.

Multi-layer model of e-Gov maturity is also done by Abdelghany[34]. It consists of four main factors: Components, management, Usability, Strategy. Human and Infrastructure Components; Management of ICT literacy, Trust, ICT human resources; Usefulness in the form of Quality of service, site design, e-readiness of citizens; and Strategy in the form of politics, economy, legislation. In previous study, Mutula[29] developed a Framework for building e-Gov trust. It is relatedto Security trust policy: Human dimension, Information demension, Technical dimension, Policy dimension, and dimension. Hassan and Khalifa[35] used the GUSF method for the development of a Comprehensive framework to gain confidence by combining technical and non-technical issues with e-Gov security. Unfortunately, the results are not sufficiently focused on security challenges, such as trust, privacy, and culture[2].

4. DEVELOPED MODEL

This study developed a framework model that can be used for security evaluation in an inclusive way to measure the level of e-Gov security readiness. The method used in developing this framework is the development of multi-layer models. The development of the framework used is the development of Salman framework[20], it was further modified in order to receive the privacy factor as part of the inclusive security factor. Description of the stages of model development can be seen in Figure 1.

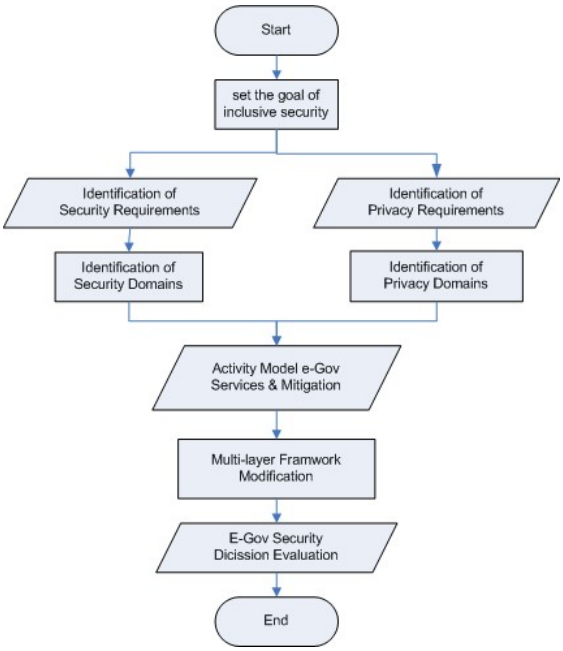

Figure 1: Framework Development Stage

5. RESULT AND DISCUSSION

5.1 Inclusive Security Framework of e-Gov

The inclusive security in e-Gov refers to Tassabehji[24] and Zu'bi's[25] opinion that involves security and privacy in building the framework. Therefore, the goal of inclusive security can be assumed as the application of security that involves security and privacy factors. case finds that it needs the security requirements, privacy requirements and also influential dimensions in building an inclusive security framework.

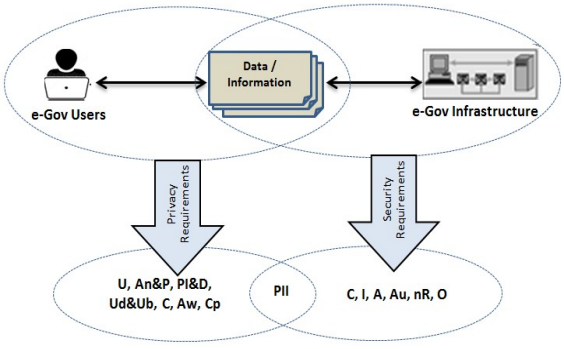

Figure 2: Relationship of e-Gov Service Access and of Security and Privacy Requirements

Security and privacy needs are intended to protect the privacy of citizens as users of e-Gov services, in addition to the security of the e-Gov service system itself. Interaction of entities between citizens and governments through the application of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

e-Gov services requires citizens of users of e-Gov service applications to trust the security mechanisms, privacy protection and application logic of e-Gov services.

The process of e-Gov included activity that occurs between users and in this case, the citizens need government service (the officers who serve) with technology facilities which are used on e-Gov. These activities can include access to data or information, write, store, update data pertaining to governance through information technology (IT / infrastructure) facilities provided by the government. The citizen who access data services or e-Gov information must complete the privacy requirements. The data or information that the user will access via IT or the available infrastructure must complete the security requirements. This indicates the need for a synergy of privacy and security requirements. The linkage of service access relation to data or information from users with the technology infrastructure used and requirement requirement is shown in Figure 2.

Figure 2 shows the privacy requirements encompassing the user area until the user can access the data or information service. The security requirement covers the area of accessing data or information which is done by the information technology (infrastructure) device. e-Gov user is a stageholder accessing e-Gov services. e-Gov technology infrastructure is a suite of tools used to provide data services. E-Gov data or information is a data asset that is caused by the process of collecting, processing or transactions, dissemination, storage, and renewals or changes made by e-Gov users. Figure 1 shows that privacy focuses on the individual's ability to control, collect, use and disseminate data, with the primary focus being collection. In this case, information privacy is a process that reflects actions that may affect personal privacy, such as protecting, using, managing, storing, distributing, and deleting records or documents containing personal data.

5.2. Identify the Relation of Security and Privacy Requirements

The form of relation between privacy requirements and security requirements are based on security and privacy domain indicators. Domain is as pillars form a security and privacy framework to build trust. Identified security domains involved are technology, policy, competence, operations and management, physical and environmental. The domain of privacy is the main actor as a stageholder in the security system that performs the activities of e-Gov services. Human is citizen who can access free or limited free e-Gov applications. Therefore, the aspects of the privacy domain can be raised in the security domain.

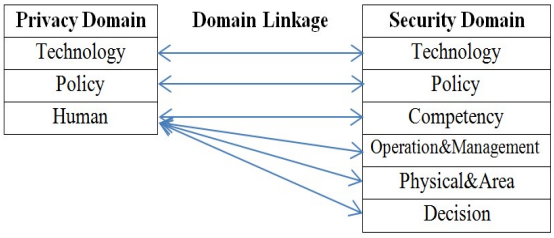

Figure 3: The Domain Relations between Privacy and Security

The combination of both creates a comprehensive consideration changes into socio-technical considerations. This socio-technical consideration makes the form of trustworthy system development in e-Gov services. The connection of privacy and security domains is shown in Figure 3.

In Figure 2 and Figure 3, it can be seen and concluded that the relationship between privacy and security in e-Gov are intertwined and intersect. This is indicated by the existence of problems with the processing of Personally Identifiable Information (PII). The activities related to the control of user access to data or information through information technology which used in e-Gov are such as the right to read, alter, and delete. It indicates that PII's activity aims to ensure users can only access specifically in accordance with the permissions granted. It is useful to protect against risks that may occur such as destruction, duplication, modification, discontinuation and unauthorized disclosure. The way to overcome this case is by using a Privacy Impact Assessment (PIA) and security risk assessment which is really required. Privacy focuses on identifying data collection, so that privacy-related issues must be solved by PIA procedures.

The arrangement of the security domain and privation linked is further derived in the form of privacy and security requirements. These requirements are used as a basis for compiling the necessary elements required for each layer of security and privacy domains. Further maps the mitigation of privacy with Privacy Enhancing Techniques (PET) is based on security and privacy requirements. The basic use of PET techniques is taxonomy of a privacy mitigation strategy consisting of two associations to hide the association, and maintaining the association. Hiding associations can be divided into two sub-strategies: (1) protect the user's identity during authentication, and (2) protect the data to be communicated to the system. Keeping the association after the data is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

used can be divided into two sub-strategies: (1) keeping being revealed and (2) maximizing accuracy. The strategy contains privacy entity entities can be arranged as Table 1.

Based on Table 1, it is illustrated the relationship between the security and privacy requirements of e-Gov as shown in Figure 4.

Table 1: PET Techniques for Privacy Mitigation

Mitigation	PET [1]	U	An&P	Pl&D	Ud&Ub	C	I	Aw&Cp
Anonymity system	Mix-networks, DC-networks, ISDN-mixes, Onion Routing, Crowds, Single Proxy, (Penet pseudonymous remailer (Anonymizer, SafeWeb), anonymous Remailer, Mixmaster Type, Mixminion Type 3,and Low-latency communication, Java Anon Proxy, Tor.	x	x			x	x^2	
	DC-net & MIX-net + dummy traffic,	x	x	x		x		
	ISDN-mixes.	x		x	x			
	Broadcast systems, + dummy traffic.							
Privacy preserving authentication	Private authentication, Anonymous credentials (single show), multishow.	x	x					
	Deniable authentication.	x	x	x		x		
	Off-the-record messaging							
Privacy preserving cryptographic protocols	Multi-party computation (Secure function evaluation).	x				x		
	Anonymous buyer-seller watermarking protocol	x	x			x		
Information retrieval	Private information retrieval + dummy traffic	x	x		x			
	Oblivious transfer	x	x			x		
	Privacy preserving data mining	x	x			x		
	Searchable encryption , Private search		x					
Data anonymization	K-anonymity model, l-Diversity	x	x					
Information hiding	Steganography	x	x		x			
	Covert communication	x	x		x			
	Spread spectrum	x	x		x			
Encryption techniques	Symmetric key & public key encryption					x		
	Deniable encryption			x		x	x^3	
	Homomorphic encryption					x	x^3	
	Verifiable encryption					x		
Access control Techniques	Context-based access control					x	x^4	
	Privacy-aware access control					x		
Policy and feedback tools	Policy communication.							x
	Policy enforcement.							x
	Feedback tools for user privacy awareness.							x
	Data removal tools (spyware removal, browser cleaning tools, activity traces eraser, harddisk data eraser).							x

Annotation : [1]Wuyt(2015), x^2Shen (2011), x^3Haus (2017), x^4 Brooks (2017)

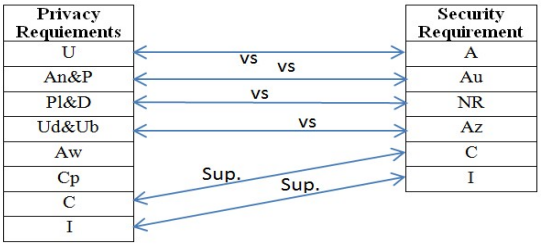

Figure 4: Forms Relationship Privacy and Security e-Gov

Figure 4 based on the description of security and privacy requirements occurs in the form of mutually supportive relationships (*Support / Sup.*), as opposed to vs. (*versus / vs*). Security and Privacy have a mutually supportive relationship (*Sup.*) that is in terms of (C) and (I). Whereas security requirements (A) are opposite to (A & P), (NR) as opposed to (Pl) & (D), (Az) as opposed to (Ud) & (Ub). The opposite form of the relationship

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

indicates that the occurrence of a problem on the privacy privacy requirement factor may cause a threat to the security requirement factor. Therefore, the necessary security and control measures are appropriate for the resistance relationship. For example the problem of unlinkability is required mitigation solutions availablability. Forms of mutually supportive relationships (*Sup.)* is a mitigation of existing solutions to both privacy and security concerns. While (Aw) and (Cp) has more users' policy control, then, the policy domain is subject to privacy and security requirements.

5.3. Arrangement of Inclusive Security Aspect

In the perspective of inclusive security identification of data collection includes aspects of authentication and authorization, data protection covers aspects of confidentiality and integrity. While, the non-repudiation aspect is a business process that occurs on the identification and protection of users and data. The availability aspect relates to the business process in which data is stored and when it should be provided when a user needs it. Data in a security perspective has a basic aspect of secrecy and integrity. The Authentication aspect relates to identifying the identity of the original user who will access the data. The authorization aspect relates to the right of access to data treatment. Authority limits include data range and data control such as read, edit, write, execute, and delete through the collection and update process. This access control is always related to the user and this involves privacy in e-Gov security. The non-repudiation aspect relates to can not or can not deny the user through an authenticated user identity performing e-Gov services activity as per its authority. A description of the e-Gov services activity and its relation to the inclusive security aspects can be shown in Figure 5.

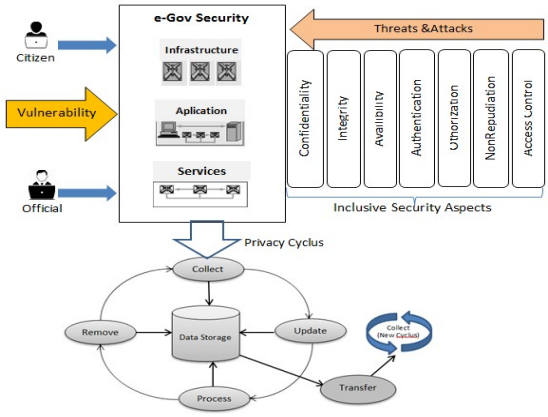

Figure 5: Aspect of Inclusive Security in e-Gov Activitie

The occurrence of government service activities using e-Gov may cause a risk to the data or information through the technology devices used. Risks to the device may occur through the network technology devices and savings used. Risk of threats and security attacks can occur due to various factors primarily due to the vulnerability of the technology used, as well as the competence and integrity of e-Gov service personnel. The vulnerability of the technology used will primarily be a threat from external e-gov organizations. So to minimize the external threat required a level of technology that meets the high security standards and competence of security officers. Then, the integrity of the officers will be a determinant of the internal threats of e-Gov organizations.

Salman[20] multi-layer framework model, has been developed with some changes and additions to the layers and elements as Table 2. The following is the explanation :

a. The addition of elements to the Technology layer. On the technological layers of compliance with security and privacy requirements are robustness against attacks, data authentication, and access control and client privacy. Technology to improve Privacy VPN, TLS, DNSSEC, and Onion Routing encrypts and mixes Internet traffic, PIR. Hasibuan added a keyloger[37].
b. Additions and changes to elements in the policy layer. In the previlage control element SSO is added as the user controller[38]. The legal and legislative elements in e-Gov governance are included in the policy dimension[14]. In addition, the Data privacy elements change with the privacy policy. The privacy policy determines what data is being processed, how it is collected, where it is stored, for what its use is and so on[39]. Addition of educational elements and user awareness is due to privacy respecting and protecting the rights protected by law. Addition of policy elements of sensitive data control is to protect assets at risk from open access. This can maintain public confidence in the protection of sensitive data[40].
c. On the layer of competence, there are additional elements of user logs and Previlage. This Competence aims to monitor every user activity, so that it can be known activity according to permissions and this is part of user privacy[9].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Tabel 2: Results of Modified Multi-layer Framework

Security layer	Element				
Technology Layer	A1: Access Control	A2: Intrusion Detection Prevention	A3: Anti-Virus & Malicious Codes Signature	A4 : Registration & Password	A5: File Integrity Check
	A6: Cryptography	A7: VPN	A8: vulnerability Tool Scan	A9 : Digital Signatures & Certificates	A10: Biometric
	A11: Logic Access Controller (Firewall)	A12: Security Protocol	A13: Non-repudiation	A14: VLAN	**A15: OTP & PIN**
	A16: TLS	**A17: DNSSEC**	**A18: Onion Routing Encrypts & Mixes Internet Traffic**	**A19: PIR**	**A20: Keylogger**
Policy layer	B1: Password Management	B2: Proses Log-In	B3: Logs Handling	B4: Computer Virus	B5: IPR
	B6: Privacy Policy	B7: Privilage Control **&SSO**	B8: Data Convidentiality	B9: Data integrity	B10: internet Connetivity
	B11: Administration Policy	B12: Encryption Policy	B13: Personal Security Policy	B14: Third-Party Policy	B15: Physical security Policy
	B16: Operational Safety Policy	**B17: Education & user awareness**	**B18: Legal & Legislation Policy**	**B19: Sensitive Data Control**	
Competency layer	C1: Management & Operation Security	C2: Security Archives & Development	C3: Ethical Hacking	C4: Development of Security Policy	C5: Computer Forensics
	C6: Cryptography	C8: Security Programming	C9: Security Configuration & Implementation	C10: Security Analysis	C11:CSIRT
	C12: Education & Awareness department	C13:Cyber Crime	C14: Social Engineering	**C15: User log & Privilage**	
Operation&Management Layer	D1: Security Procedures & Policies	D2: Tools Management	D3: Correlation & Data Mining	D4: Reporting and Response	D5: Human Analysis and Intervention
	D6: User Management				
Physical and Environment Layer	E1: Site Design	E2: Access Control Devices	E3: Alarm & Camera	**E4: ID Card**	**E5: Protecting Device**
	E6: Socio-culture	**E7: Disaster**			
Decision layer	F1 : Cost	F2 : Awareness	F3: Requirements	F4: Availability of Technology	F5: Sensitive Data
	F6: FUD (Fear, Uncertainty, Doubt)	**F7: Training**	**F8: Management Support**		

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

d. The addition of elements on the layer of operation and management. This layer added user management to the e-Governance system remains safe from any kind of attack. At the user level the actions taken are managing user identity, Access Management System, and Interaction Management System[7].
e. Physical layer name changes to physical layer and environment based on ISO / IEC 27001 frameworks[41]. Physical element addition of Id Card and Protecting Device. The addition of environmental element is in the form of social culture and user unauthentication. The socio-cultural element concerns the behavior of the people involved in e-Gov, this includes the acceptance of e-Gov and IT literacy.
f. Added elements to the decision layer. On this layer coupled with training elements, and management support as recommended[11]. The training edition supports the decision layers in the defense mechanisms used and how to configure services, and is the basis for developing safe programming guidelines and procedures for users and system administrators to follow.

An inclusive security framework is developed on the basis of basic security needs that are insufficient to protect e-Gov users. So that the need for further security, especially concerning the main security and privacy is needed to foster the trust of e-gov users. The novelty of this research is the addition of privacy aspects along with the elements involved as a basis for shaping e-Gov users' trust (see Table 2 in green). While the relationship between the requirements of security and privacy aspects can be seen in Figure 4.

Decision layers can influence the decision whether or not an e-Gov security is an evaluation. This provides the basis for further research to develop a risk-based security evaluation model. On the decision layer makes five important elements, namely Cost, Sensitive Data, Element Availability, Awareness, and Management Support.

6. CONCLUSSION

This study has resulted in a framework as a basis for risk-based security and privacy evaluation on e-Gov. The resulting framework can accept the basic security aspects of Confidentiality, Integrity, and Availability, and the key security aspects of Authentication, Authorization to generate the privacy factor. The non-repudiation aspect is required to improve business processes on e-Gov security and privacy factors. Fulfilling aspects of security and privacy is to generate inclusive security. Security and privacy factors to produce such frameworks require security and privacy requirements. Both requirements can be integrated based on the same domain. The resulting framework can be used as a basis for risk-based security evaluation. On the decision layer makes five important elements, that is Cost, Sensitive Data, Elements Availability, Awareness, and Management Support. On the decision layer makes five important elements, namely Cost, Sensitive Data, Element Availability, Awareness, and Management Support. These elements are useful for e-Gov evaluation decision process. Authorization and non-repudiation aspects, as well as awareness and management support elements are new aspects and elements in the findings of this study compared to previous multi-layer framework studies. These aspects and elements become important variables as the deciding factor for evaluating risk-based security and privacy in e-Gov.

7. FUTURE RESEARCH

The results of this study will continue as a basis for evaluating risk-based security and privacy in e-Gov. Further research is intended to assess risk factors and the level of security risk of e-Gov. Results from further research are expected to be used to assess the level of security readiness in e-Gov service applications.

REFERENCES

[1] S. Alshomrani, “A Critical Analysis of E-Government Development and Implementation in Saudi Arabia,” *Int. J. Appl. Inf. Syst.* –, vol. 7, no. 5, pp. 21–25, 2014.
[2] N. Alharbi, M. Papadaki, and P. Dowland, “Security Factors Influencing End Users ’ Adoption of E-Government,” *J. Internet Technol. Secur. Trans. (JITST),* vol. 3, no. 4, pp. 320–328, 2014.
[3] R. Kaushal, “Evaluation Metrics for e-Government System and Services,” *Int. J. Adv. Eng. Res. Sci.*, vol. 4, no. 2, pp. 16–20, 2017.
[4] M. I. Manda and J. Backhouse, “Addressing trust , security and privacy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

concerns in e-government integration , interoperability and information sharing through policy : a case of South Africa sharing through policy : a case of South Africa," in *International Conference on Information Resources Management (CONF-IRM)*, 2016.

[5] D. Kumar and N. Panchanatham, "A case study on Cyber Security in E-Governance," *Int. Res. J. Eng. Technol.*, vol. 2, no. 8, pp. 272–275, 2015.

[6] M. O. M. Baeuo, N. Zairah, B. Ab, A. Ali, and M. Alaraibi, "Technology Aspects of E-Government Readiness in Developing Countries : A Review of the Literature," *Comput. Inf. Sci.*, vol. 9, no. 4, pp. 1–12, 2016.

[7] C. R. Moharana, M. K. Pal, and D. Rout, "Informatioan And Network Security in E-Governanace," vol. 2, no. 11, pp. 347–362, 2012.

[8] S. U. Rehman, I. U. Khan, M. Moiz, and S. Hasan, "Security and Privacy Issues in IoT," *Int. J. Commun. Networks Inf. Secur. 147*, vol. 8, no. 3, pp. 147–157, 2016.

[9] M. Brooks, Sean, Garcia and E. Nadeau, "NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems An Introduction to Privacy Engineering and Risk Management," 2017.

[10] H. M. B. P. Ranaweera, "Perspective of trust towards e-government initiatives in Sri Lanka," *Springerplus*, vol. 5, no. 22, pp. 2–11, 2016.

[11] S. Smith, R. Jamieson, S. Smith, and R. Jamieson, "Key Factors in E-Government Information System Security," in *18th Bled eConference eIntegration in Action Bled,* 2005, pp. 1–15.

[12] A. J. M. Jr and S. E. Pippin, "Security and Privacy Trust in E-Government : Understanding System and Relationship Trust Antecedents," in *Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009 Individual*, 2009, pp. 1–10.

[13] A. Shameli-sendi, R. Aghababaei-barzegar, and M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)," *J. Comput. Secur. - ELSEVIER*, pp. 1–20, 2012.

[14] F. Belanger, J. S. Hiller, and J. S. Hiller, "A framework for e-government : privacy implications A framework for e-government : privacy implications," *Bus. Process Manag. J.*, vol. 12, no. 1, pp. 48–60, 2006.

[15] S. M. Shareef, "Enhancing Security of Information in E- Government Enhancing Security of Information in E-Government," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 7, no. 3, pp. 139–146, 2016.

[16] J. T. H. Jaafar, N. Hamza, and B. E. M. Hassan, "A proposed Security Model for E-government Based on Primary Key Infrastructure and Fingerprints," *Egypt. Comput. Sci. J.*, vol. 38, no. 2, pp. 85–100, 2014.

[17] E. Aïmeur, G. Brassard, and J. Rioux, "Data Privacy : An End-User Perspective," *Int. J. Comput. Networks Commun. Secur.*, vol. 1, no. 6, pp. 237–250, 2013.

[18] V. Tech, "Infrastructure for E-Government," *IEEE Internet Comput.*, no. February, 2003.

[19] S. Abu-Nimeh and N. R. Mead, "Privacy Risk Assessment in Privacy Requirements Engineering," *Requir. Eng. Law RELAW 2009 Second Int. Work.*, pp. 17–18, 2009.

[20] A. O. Salman, P. G. H. Abdul-majeed, A. Prof, and T. Z. Ismaeel, "Evaluation of elecronic Government Security Issues Applied to Computer Center of Baghdad University (Case Study)," *J. Engeneering*, vol. 18, no. 3, pp. 364–380, 2012.

[21] S. Zulhuda and A. Ibrahim, "The State of E-Government Security in Malaysia : Reassessing the Legal and Regulatory Framework on the Threat of Information Theft," in *ICCIT*, 2012, pp. 810–815.

[22] M. Haus, M. Waqas, A. Y. Ding, Y. Li, and S. Member, "Security and Privacy in Device-to-Device (D2D) Communication : A Review," *IEEE Commun. Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[23] J. Sarabdeen and B. S. Rodrigues, Gwendolyn, "E-Government users â€™ privacy and security concerns and availability of laws in Dubai," *Internatioanl Rev. Law, Comput. Technol.*, vol. 28, no. 3, pp. 261–276, 2014.

[24] J. Tassabehji, R., Elliman, T., Mellor, "Generating Citizen Trust in E-Government Security :," *Int. J. Cases Electron. Commer.*, vol. 3, no. 3, pp. 1–17, 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[25] H. H. zu'bi, Hazza M., Al-Onizat, "E-Government and Security Requireme ents for Inform mation Systems and Privacy (Performnce Linkage)," *J. Manag. Res.*, vol. 4, no. 4, pp. 367–375, 2012.

[26] K. Kessler and A. Add, "A Framework for Assessing Privacy Readiness of E-Government," Centre for Development Informatics- University of Manchester, UK, 21, 2011.

[27] Q. Ma, A. C. Johnston, and J. M. Pearson, "Information security management objectives and practices : a parsimonious framework," *Inf. Manag. Comput. Secur.*, vol. 16, no. 3, pp. 251–270, 2008.

[28] Wuyts, "Privacy Threats in Software Architectures," Arenberg Doctoral School Belgium, 2015.

[29] S. M. Mutula, "A Model for Building Trust in E-Government," *IGI Glob.*, vol. ch016, no. 2006, pp. 306–324, 2012.

[30] S. Al-azazi, "A multi-layer model for e-government information security assessment," Cranfield University, 2008.

[31] I. Bernik, K. Prislan, I. Bernik, and K. Prislan, "Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation," *PLoS One*, vol. 11, no. 9, pp. 1–33, 2016.

[32] A. Supriyanto and K. Mustofa, "E-gov readiness assessment to determine E-government maturity phase," in *Proceeding - 2016 2nd International Conference on Science in Information Technology, ICSITech 2016: Information Science for Green Society and Environment*, 2017.

[33] M. Alshehri, S. Drew, and O. Alfarraj, "A Comprehensive Analysis of E-government services adoption in Saudi Arabia : Obstacles and Challenges," *IJACSA - www.ijacsa.thesai.org*, vol. 3, no. 2, pp. 1–6, 2012.

[34] A. Abdelghany, H., El-Bastawissy, "E-Govemment Multi-Iayers Maturity Model," in *IEEE In Computer Engineering Conference (ICENCO)*, 2016, pp. 83–92.

[35] R. G. Hassan and O. O. Khalifa, "E-Government - an Information Security Perspective," *Int. J. Comput. Trends Technol.*, vol. 36, no. 1, pp. 1–9, 2016.

[36] I. Maskani, "Analysis of Security Requirements Engineering : Towards a Comprehensive Approach," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 11, pp. 38–45, 2016.

[37] M. S. Hasibuan, "Keylogger Pada Aspek Keamanan Komputer," *Teknovasi*, vol. 3, no. ISSN : 2355-701X, pp. 8–15, 2016.

[38] T. K. Priyambodo and D. Suprihanto, "Information Security On eGovernment As Information-Centric Networks," *Int. J. Comput. Eng. Res. Trends*, vol. 3, no. 6, pp. 360–365, 2016.

[39] S. Miyazaki, N. Mead, and J. Zhan, "Computer-aided privacy requirements elicitation technique," *Proc. 3rd IEEE Asia-Pacific Serv. Comput. Conf. APSCC 2008*, pp. 367–372, 2008.

[40] R. Meijer, P. Conradie, S. Choenni, and R. Meijer, "Reconciling Contradictions of Open Data Regarding Transparency , Privacy , Security and Trust," *J. Theor. Appl. Electron. Commer. Res.*, vol. 9, no. 3, pp. 33–44, 2014.

[41] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Integrated Solution Modeling Software : A New Paradigm on Information Security Review and Assessment," *IJSAT*, no. December, pp. 1–9, 2011.