Inclusive Security Models To Building E-Government Trust

Aji Supriyanto[1], Budi Hartono[1], Dwi Agus Diartono[2], Herny Februariyanti[2]
[1]*Department of Informatic Engeenering,* [2]*Department of Information System*
Universitas Stikubank Semarang, Indonesia
ajisup@edu.unisbank.ac.id, budihartono@edu.unisbank.ac.id, dwieagus@edu.unisbank.ac.id, hernyfeb@edu.unisbank.ac.id

***Abstract*— The low attention to security and privacy causes some problems on data and information that can lead to a lack of public trust in e-Gov service. Security threats are not only included in technical issues but also non-technical issues and therefore, it needs the implementation of inclusive security. The application of inclusive security to e-Gov needs to develop a model involving security and privacy requirements as a trusted security solution. The method used is the elicitation of security and privacy requirements in a security perspective. Identification is carried out on security and privacy properties, then security and privacy relationships are determined. The next step is developing the design of an inclusive security model on e-Gov. The last step is doing an analysis of e-Gov service activities and the role of inclusive security. The results of this study identified security and privacy requirements for building inclusive security. Identification of security requirements involves properties such as confidentiality (C), integrity (I), availability (A). Meanwhile, privacy requirement involves authentication (Au), authorization (Az), and Non-repudiation (Nr) properties. Furthermore, an inclusive security design model on e-Gov requires trust of internet (ToI) and trust of government (ToG) as an e-Gov service provider. Access control is needed to provide solutions to e-Gov service activities.**

Keywords—e-gov, privacy, inclusive security, trust

I. INTRODUCTION

A. Background

The success of *e-Government* (e-Gov) services depends on user acceptance [1], this is related to the ability of e-Gov to interact with users, collect information, and doing interactions with users [2]. One of very important issue in *e-Gov* is security [3]. Security is one of the main obstacles in e-Gov project [1], [4]. In addition to efficiency issues, security is a critical factor in the successful implementation of e-Gov [5], and e-Gov security is considered as an important factor in gaining the level of maturity of e-Gov [6]. Higher level of security is needed because e-Gov service functions are so widely accessed by the wider community [7] - [9]. This matter means that e-Gov security is considered as one of the important factors to reach the advanced stages of e-Gov [7], and it becomes part of maturity level of e-Gov [10].

In the initial stages of building e-Gov information security it concentrates on confidentiality, but in its development privacy needs are very important [20]. Security and privacy are closely related issues, but a secure e-Gov infrastructure does not always guarantee privacy [17]. Security and privacy are the main problems in communication through the internet network. Because it is related to authentication, identification, and heterogeneity of the device. In addition the main challenges include integration, scalability, ethical communication mechanisms, business models and supervision. Identification of privacy needs is the key to internet communication [2]. The importance of security and privacy needs in e-Gov is because e-Gov's own goal is to conduct interactions and transactions G2G, G2C, G2E, G2B, G2NG [21] that are easy, inexpensive, convenient, transparent, secure, and accountable to realize governance the good one.

Violation of security norms can affect citizens trust, and trust contains technical and nontechnical aspects [5]. Trust is an important element for the success of e-Gov projects, and privacy is a key element in building citizens trust in e-Gov services [26]. The link in the form of maintaining security in the privacy of citizens, this can make citizens satisfied, and satisfaction using e-Gov services can lead to trust [27]. Particularly related is the control of ICT access to ensure confidentiality and integrity strongly support privacy goals [28]. In the context of privacy organizations require the application of laws, policies, standards and processes by which personal information is managed [29].

The lack of trust in the e-Gov system is one of the obstacles in the expansion of e-Gov services [30]. The internet as the main medium of e-Gov has a number of threats and vulnerabilities, and this has become an obstacle for the implementation of e-Gov, especially in terms of public participation [31], which can impact on the decline of public trust [32]. The level of citizens' trust in e-Gov is influenced by two things namely on the internet connection and the government itself [33]. The e-Gov trust consists of trust of the Internet (ToI) and trust of the Government (ToG) [34]. Trust in government includes capability and integrity. Internet trust in e-Gov means people's trust in the media which is reliable, accurate and safe information. The combination of these two beliefs is called multidimensional trust [34].

B. Literature Review

Safety issue is not only in the form of technical but also non-technical issues[4], [5], [9]. The technical security aspects include vulnerabilities caused by poor system design, development, implementation, configuration, integration, and maintenance. However, nontechnical security aspects are included some aspects such as ethical and cultural norms, legal and contract documents, administrative and managerial policies, operational guidelines and procedures, and user awareness [6]. This opinion is supported by Shareef's research [13] which proposes a solution by considering two security perspectives which are called as technical and nontechnical by identifying critical success factors to improve e-Gov security. On e-Gov security perspective which involves technical and nontechnical infrastructure can generate trust to the users [14]. This shows that e-Gov's trust is related to the perception of security and privacy of personal information [15].

Technical security includes the property of confidentiality, integrity, and availability (C, I, A) [5], which Al-Azazi through Supriyanto's research called basic security [16]. Whereas further security contains privacy requirements in a security perspective consisting of authentication, authorization, and non-repudiation properties (Au, Az, Nr) [17]. Meeting security and privacy requirements through existing properties are both called inclusive security [16]. This is in accordance with the comprehensive e-Gov security requirements in that it includes properties C, I, A, Au, Az, Nr [11], [18]. Problems that arise in technical security such as: identity theft, hacking and DoS or problems related to e-Gov users, and stealing information [5]. Furthermore technical security solutions concentrate on functionality such as digital signatures, PKI, firewalls or antivirus mechanisms. Meanwhile, according to Karokola, technical security solutions include access control mechanisms, encryption of network security mechanisms (firewalls, IDPS, VPN), application of data backup and disaster recovery, as well as the application of antivirus software and malicious codes [19]. Furthermore, Shareef's research combines technical challenges with physicality to provide solutions about the security triangle C, I, A, and other security such as network security, infrastructure, identification, privacy, access control, electronic authentication, information sharing, data types, work flow, Bridge Certification Authority (BCA), DoS, malware, packet sniffers, probes, firewalls [13]. On the other hand, nontechnical or sociotechnical security aspects can result in a lack of ethical and cultural norms, legal and legislative issues, administrative and managerial policies, operational guidelines and procedures, and lack of user awareness, social engineering [11], and public trust [19]. Nontechnical solutions such as trust, legal protection, privacy, authentication and confidentiality [5], awareness, security policies and standards, interoperability, and expediency [13].

Several cases of security and privacy violations as conveyed by Heeks in Napitupulu [22], e-Gov projects in developing countries 35% failed, 50% were partial failures, and only 15% were successful [22]. Another case occurred in the US, many people who refuse the use of software such as e-filling due to several reasons including security and privacy. This has prompted the US government to increase individual trust in security and privacy mechanisms [23]. According to Breach QuicVew Report data, in 2017 there were 5,200 security violations in the world, with more than 7.8 billion suspicious or dangerous records. While in 2016 there were 6.3 billion suspicious records [24].

The occurrence of cases as above shows the need for anticipation and vigilance against hazards or risks to security and privacy. Security must be designed from the initial phase when starting to build or develop a system, and not when there are new security problems carried out maintenance or recovery [25]. This shows that security challenges are not only technically but also nontechnical [1]. This challenge requires comprehensive treatment to reduce and prevent greater risks to the security and privacy of e-Gov services

C. Motivation and Contribution

The problem occurs that in the study of Belanger and Carter [34] did not specifically mention the model of trust in security and privacy aspects to develop an inclusive security system as proposed by Supriyanto which is using the elicitation method [16]. However, Supriyanto's research has not yet discussed the stages of security solutions that need to be carried out as recommended by NIST such as identification, protection, detection, response, and recovery [35], although it has mentioned the problem of security risks due to threats, vulnerabilities, and assets. From the result, we can conclude that it is really needed a solution as a form of mitigation in the application of inclusive security, so the process that occurs requires a recurring solution (cycle) on security and privacy.

The contribution of this research is to develop an inclusive security model as a trust for eGov. Based on the description of the development of the model, an inclusive security solution model can then be arranged. The difference with previous studies is that the Belanger and Carter research studies do not mention inclusive security properties (C, I, A, Au, Az, Nr). While previous research by Supriyanto mentions inclusive security properties, it has yet to discuss an inclusive security solution model based on risk and mitigation.

II. METHOD

This study discusses the development of an inclusive security model to build e-Gov trust. The method used is elicitation, which combines the requirements of security and privacy requirements in e-Gov. This method begins by identifying an overview of inclusive security properties, the relationship between security and privacy, a perspective of trust in inclusive security, and an analysis of e-Gov service activities and the role of inclusive security. This research is limited to the discussion and identification of inclusive security solutions as a basis for developing a risk-based e-Gov inclusive security evaluation framework and evaluation.

III. DISCUSSION

A. Property of Inclusive Security

According to the concept defined by Supriyanto et al states that inclusive security is security on e-Gov which meets security and privacy requirements. In this case, the security requirements refer to the basic security requirements which consist of the C, I, and A properties. Meanwhile, privacy requirements from a security perspective refer to advanced security requirements consisting of Au, Az, and Nr properties. In security requirements, the technical aspects are more dominant than nontechnical privacy requirements. In this case, the Au concerns to the problem of user identification, while the Az is related to the problem of using data. This means that the users can do anything (data) which is available in e-Gov service. In the service process there is control of access to users in accessing data. Control of access to data can be done when collecting, storing, processing, using, retrieving, deleting, updating and distributing data.

Access control for every e-Gov transaction can be identified by applying a Nr property, where every service activity on the system will always be recorded in the transaction. The transaction record can be in the form of identifying who (the user), doing what (type of transaction), and when (time), even the transaction capacity can be recorded. This can be interpreted that Au is related to users, Az relates to data, and Nr related to services (transactions). Every service process or transaction which is carried out by the user of the data can be controlled by the application of security in the form of C, I, and A. The link between e-Gov inclusive security properties can be illustrated as in Fig. 1.

Explanation of each property in Fig. 1 is as follows:

a) Confidentiality (C) is used to prevent the disclosure of information to individuals or unauthorized systems. This is to ensure that the information is only received by those who have authorization. Information can be kept confidential due to privacy reasons.

b) Integrity (I) means that data cannot be changed or modified without authorization. Changing or deleting data is an act of violating the integrity of information.

c) Availability (A) means that information must be available when needed. High availability systems aim to remain available at all times, preventing service interruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing DoS attacks.

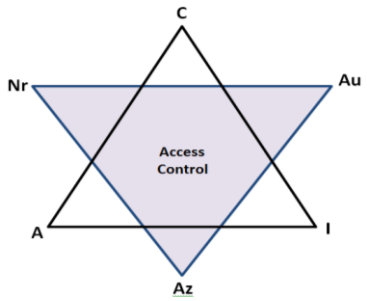

Fig. 1. Overview of the linkages of inclusive security properties

d) Authentication (Au) proves that the user is a true or legitimate person. The evidence involves something that the user knows (such as the user's name & password), something the user has (such as a smartcard, token, digital certificate), or something about the user that proves the person's identity (such as a fingerprint, retina, or other biometrics).

e) Authorization (Az) is an action to determine whether a particular user (or computer system) has the right to carry out certain activities, such as reading files or running programs. Authorization verifies what is permitted by the user. The methods used include access control from URLs, secure objects and methods, access control lists (ACLs).

f) Non-repudiation (Nr) to guarantee that authentication can be confirmed as genuine and not denied later. The legal perspective, non-repudiation implies a person's intention to fulfill his obligations for the contract. It also implies that one party cannot deny having received a transaction cannot another party deny having sent a transaction.

B. Security and Privacy Relationship

Based on the opinion of Medjahed that security and privacy are closely related. The security mechanism focuses on providing protection which includes authentication, access control, availability, confidentiality, integrity, retention, storage, backup, incident response and recovery. Privacy mechanisms focus on handling personal information, addressing individual rights and aspects such as fair use, notification, choice, access, and accountability. The relationship between privacy and security requirements is based on domain indicators. The domain as a pillar forms a security and privacy framework to build trust. The security domain consists of technology, policy, competence, operations and management, physical and environmental, and decisions. The Privacy domain consists of technology, policies, and citizens. In both domains there are similarities in technological and policy aspects, this can show a direct relationship because it has the same aspects. While the human aspect in the privacy domain is the main actor in the security system that carries out e-Gov service activities.

Table I. Differences of Privacy and Security

Privacy	Security
Includes Au, Az, Nr. Use of information to the right user.	Includes C,I,A. Orientation on information protection.
Ability to decide what information someone is aiming	Offers the ability to be confident that decisions are respected.
Refers to the user's right to protect his information from other parties	Providing confidentiality. The goal is to protect from other parties who are not authorized
It is possible to have bad privacy and good security practices	However, it is difficult to have good privacy practices without a good security program
Implemented through e-Gov service organization policy, authorization and demands for user awareness.	E-Gov service: encryption, digital signatures, firewalls, to prevent the disclosure of data from threats and or vulnerabilities in network or internet.

This makes aspects of the privacy domain can be raised in the security domain. Form of human relations in the privacy domain is a process in e-Gov services. The process requires competence, operations and management, which are influenced by the physical and the environment, and decisions. The merger of the two causes comprehensive consideration into sociotechnical considerations. These sociotechnical considerations make the form of building systems that can be trusted in e-Gov services. The preparation of the security domain relationship and activation is then differentiated in the form of privacy and security requirements.

C. *A Perspective of Trust in Inclusive Security*

In accordance with the objectives of e-Gov, namely to conduct interactions and transactions electronically between G2G, G2C, G2E, G2B, G2NG, it is necessary to provide guarantees given by the government as the organizer of e-Gov for those it serves. One of the main guarantees is security and privacy. Citizens' satisfaction with providing security and privacy guarantees in e-Gov services can lead to trust in e-Gov. This is based on previous research conducted by Belanger and Carter supported by research from Tassabehji et al., Dharma, and Sigwejo and Pather.

In Fig. 2 is the perspective of an inclusive security model to build e-Gov trust. Based on Fig. 2, the important components of building inclusive security are people, processes and technology. Humans as users consist of citizens as users served, and government officials as users who operate e-Gov and serve citizens. The technology consists of network infrastructure, software, hardware, and security and privacy control technologies. The process is an activity that occurs because of the input to produce output.

The process that occurs in accordance with Fig. 2 is :

1) The e-Gov service officer prepares the e-Gov service application device that is supported with other system-related devices so that the e-Gov service can operate. Officers must ensure that the e-Gov application must be ready to carry out transactions such as receiving input, storing, updating, deleting, processing, transferring, presenting, and transmitting data or information. The process shows the fulfillment of property availability (A).

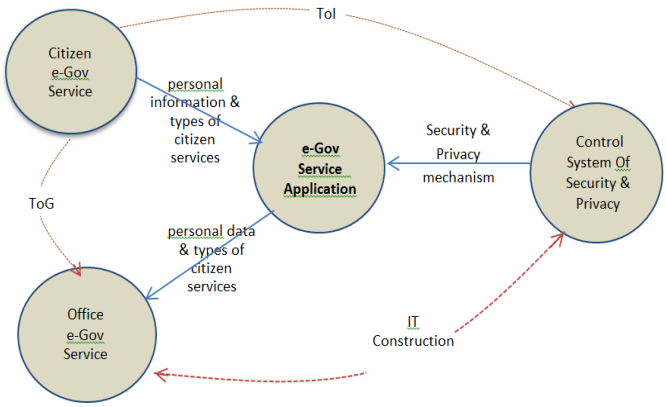

Fig. 2. Inkluisf security model for e-Gov trust

2) Citizens access e-Gov services. There are two citizen services, first is free access, and second citizens in accessing e-Gov services by registering the user's identity via login using the user's username and password. The process shows compliance with the Authentication (Au) property.

3) Residents who are successful in the login process can then carry out activities in accordance with the rights of citizens granted by the service officer. User rights indicate the legal activities that can be carried out on the contents of e-Gov services. These rights as given in activity number 1 above, which can fill or provide input, save, update, delete, process, move, present, and transmit data. The process shows compliance with the Authorization (Az) property.

4) Every activity carried out by all users, both citizens and e-Gov service officers, must be monitored for transactions, such as who the user is, what activities are done, when, where, and how much capacity must be recorded or recorded through transaction log process. This transaction log is to avoid denial or can not refuse the user in the transaction. The process shows the fulfillment of Non-repudiation (Nr) property.

5) In order to maintain the confidentiality of the user's identity and data relating to users that are private and must be protected, the e-Gov application must prepare the technology both through programming and the provision of technological devices in order to maintain its confidentiality. The process shows the fulfillment of the Confidentiality (C) property.

6) The e-Gov service application must also provide technology and programs so that the user's identity and data related to the user when it is stored, transferred, and transmitted must be maintained intact and there is no change by unauthorized persons. The process shows the fulfillment of integrity (I) property.

In the process that runs from number 1 to number 6 above it can be stated that inclusive security control can and must be carried out by e-Gov service officers through the construction of information technology (IT Construction) that has been developed. In this connection two important things are needed so that the application of e-Gov services can be trusted. First; trust in the government in this case is represented by the organization or service officer (Trust of Government / ToG) through its policy in launching e-Gov service applications. Second; trust of the internet (ToI), i.e. the application and use of e-Gov service technology that is able to meet the inclusive security requirements in the form of C, I, A, Au, Az, Nr properties as described in numbers 1 to 6 above.

D. *Analysis of e-Gov Service Activities and the Role of Inclusive Security*

The process that occurs in the e-Gov service is that every citizen who accesses the e-Gov service application must authenticate the user, unless the information service is free (without protection). User authentication is done by entering the user's identity which is usually in the form of a user name and password. If the first time a citizen will access the e-Gov service application, they must make a new registration. The

authentication process is the first step in convincing individual citizens to trust their identity. This is a form of protection or privacy of one's identity. The process of interaction that occur between citizens and e-Gov service offices through the e-Gov service application requires a security and privacy mechanism. In this case e-Gov security covers C, I, A, Au. E-Gov security is formed in a security mechanism of encryption, protection, verification, and authentication.

In order to develop an internet-based security system, a security framework is needed to produce a complete and reliable security solution. Security issues such as incidents, threats, and security risks to assets are needed security solutions by preventive detective, reactive, and adaptive as a form of inclusive security mitigation. In accordance with Fig. 2, three layers of security are needed: (1) infrastructure security layers in the form of physical (such as rooms and computers), communication (such as cable, wifi, vsat, routers, switches, servers), logical (such as DNS, directory service, VPN); (2) service security layer in the form of access control services using identification technology (such as SSO, retina, finger, key locker file); (3) application security layers (such as antivirus, legal software, logic correctness). The involvement of the three layers of security forms a multidimensional security system. In addition, e-Gov assets are data and people. E-Gov data are data assets that are caused by the process of collection, transfer, storage, remove and update.

The above explanation shows that privacy focuses on the ability of individuals to control, collect, use and disseminate data, with the main focus being on collection. In this case information privacy is a process that reflects actions that can affect personal privacy, such as protecting, using, managing, storing, distributing, and deleting records or documents that contain personal data. Privacy focuses on identifying data collection. Whereas security focuses on protecting data after it has been collected, so security issues must be resolved by assessing security risks.

In the inclusive security perspective, identification of data collection includes Au and Az properties, data protection includes C and I properties. While Nr property is a business process that occurs in the identification and protection of users and data. Data from a security perspective has the basic property of C and I. Availability (A) of property is related to business processes where data is stored and users who access or need it. The Au property is related to identifying the identity of the original user who will access the data. The Az property relates to access rights granted to users for the use or treatment of data. Authority limits include the extent of data coverage and data controls such as read, edit, write, execute, transfer and delete. This access control is always related to the user and this involves privacy in e-Gov security. The Nr property is related to being unable or unable to deny the user through the authenticated user's identity carrying out e-Gov service activities according to their authority. This Nr property also includes receiving e-mail services. An overview of e-Gov service activities and their relation to inclusive security properties can be shown in Fig. 3.

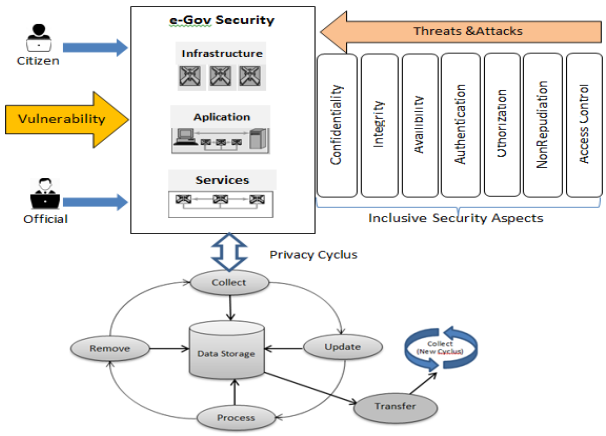

Fig. 3. Inclusive security properties in e-Gov service activities

The e-Gov service activities can pose a risk to data or information through the technology tools used. Risks to devices can occur through network and deposit technology devices. The risk of threats and security attacks can occur due to various factors, mainly due to the vulnerability of the technology used, as well as the competency and integrity of e-Gov service personnel. The vulnerability of the technology used will mainly cause threats from external e-Gov organizations. In order to minimize external threats, a level of technology that meets high safety standards and competency of security personnel is needed. While the integrity of officers such as operators and administrators will determine internal e-Gov organization threats. Vulnerabilities can occur with e-Gov assets. E-Gov assets can be identified as user, DNS, databases, licenses, routers and networks, servers, storage devices, supporting devices, and space used for places such as hardware, software, and brainware.

The form or type of security threat can be in the form of interruptions, interception, modification, and fabrication. Interruptions can threaten availability, interception threatens confidentiality, modification and fabrication threatens integrity. This happens because unauthorized parties can access and intervene even damage data or information without any control or restrictions on access rights (access control). Unauthorized parties can access because the authentication process on the user's identity is weak, wrong giving control rights, and *non-repudiation* process on the service system cannot detect the user by doing any activity (*logging*) or transactions on e-Gov service system.

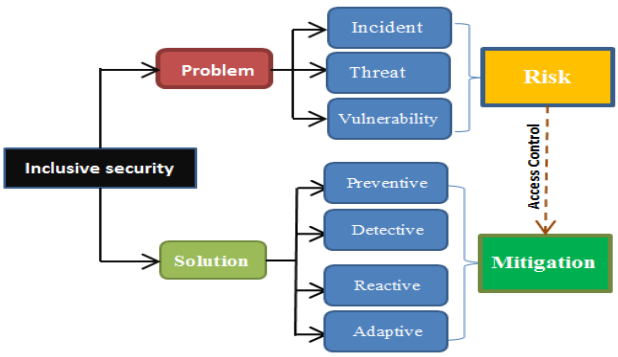

Fig. 4. Inclusive Security Problems and Solutions

Meanwhile, the types of threats to e-Gov can be in the form of human errors both from within and from outside the organization, damage to devices (hardware and software), malicious code, *SQL injection*. Furthermore *hackers*, *intruders*, *Dos* attacks, *XSS*, and social engineering are usually through internet social media networking. The identification of threats and vulnerabilities in e-Gov assets in the next chapter is used as an evaluation to determine the security risk effects of e-Gov.

IV. Conclusion

The security which is trustable needs to involve security and privacy requirements. Identification of security requirements involves confidentiality (C), integrity (I), availability (A) properties, while privacy requirements involve authentication (Au), authorization (Az), and Non-repudiation (Nr) properties. Inclusive security is built by requiring trust in internet (ToI) and trust in the government (ToG) as an e-Gov service provider. The implementation of inclusive security requires control in accordance with the developed security solutions. This research needs to be continued by constructing technology, so that technical solutions can truly be implemented as a form of real security mitigation to anticipate risks that might occur at any time.

References

[1] 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.

[2] 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.

[3] M. H. Zu'bi and H. H. Al-Onizat, "E-Government and Security Requirements for Information Systems and Privacy (Performance Linkage)," *J. Manag. Res.*, vol. 4, no. 4, pp. 367–375, 2012.

[4] H. A. A. Almagwashi, "A Framework for Preserveing Privacy in E-Government," 2014.

[5] 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.

[6] R. Ihmouda, N. Hayaati, M. Alwi, and I. Abdullah, "A Systematic Review on E-government Security Aspects," vol. 3, no. 6, pp. 60–67, 2014.

[7] J. Wang, "E-government Security Management: Key Factors and Countermeasure," *2009 Fifth Int. Conf. Inf. Assur. Secur.*, pp. 483–486, 2009.

[8] W. Zhong, "Research on E-Government Security Model," *2010 Int. Conf. E-bus. E-Government*, pp. 699–702, May 2010.

[9] N. O. . Elsseid, O. Ibrahim, A. A. Al-Azazi, and A. Yousif, "Review Paper : Security in E-government Using Fuzzy Methods," *Int. J. Adv. Sci. Technol.*, vol. 37, no. December, pp. 99–112, 2011.

[10] 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*, 2016, pp. 270–275.

[11] P. Milic and K. Kristijan, "The Importance of Secure Access to E-Government Services," *Communication*, vol. 26, no. 16, pp. 1873-18893., 2016.

[12] A. Ramadhan *et al.*, "Kegiatan Penelitian Model e-Livestock Indonesia Sebagai Suatu Sistem e-Government untuk Ketahanan dan Keamanan Sumberdaya sapi Potong Nasional," in *InSINas*, 2012.

[13] 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.

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

[15] A. Sigwejo and S. Pather, "Citizen-Centric Framework For Assessing E-Govenment Effectiveness," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 74, no. 8, pp. 1–27, 2016.

[16] A. Supriyanto, J. E. Istiyanto, and K. Mustofa, "Multi-layer Framework for Security and Privacy Based Risk Evaluation on E-Government," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 5, pp. 1423–1433, 2019.

[17] B. Medjahed, A. Rezgui, A. Bouguettaya, and M. Oussani, "Infrastructure for E-Government Web Service," *IEEE Internet Comput.*, vol. February, no. February, pp. 58–65, 2003.

[18] Y. Nugraha and A. Martin, "Investigating Security Capabilities in Service Level Agreements as Trust-enhancing Instruments," *IFIP Adv. Inf. Commun. Technol.*, vol. 505, no. March, pp. 57–75, 2017.

[19] G. R. Karokola, *A Framework for Securing e-Government Services The Case of Tanzania*, no. 12. Department of Computer and Systems Sciences, 2012.

[20] S. Smith and R. Jamieson, "Determining Key E-Government Information System Security," *Inf. Syst. Manag.*, vol. 23, no. 2, pp. 23–32, 2006.

[21] D. Zautashvili, "E-government Maturity Model by Growth Level of E-services Delivery," *l Tech. Sci. Technol.*, vol. 6, no. 2, pp. 17–22, 2017.

[22] D. Napitupulu, "The Critical Success Factors Study for e-Government Implementation," vol. 89, no. 16, pp. 23–32, 2014.

[23] A. J. McLeod 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*, 2009, pp. 1–10.

[24] D. Solove, "Data Security Is Worsening – 2017 Was the Worst Year Yet," *https://teachprivacy.com/data-security-is-worsening-2017-was-the-worst-year-yet/*, p. Founder of TeachPrivacy, February 16, 2018, 2018.

[25] 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.

[26] A. Alawneh, H. Al-Refai, and K. Batiha, "Measuring user satisfaction from e-Government services: Lessons from Jordan," *Gov. Inf. Q.*, vol. 30, no. 3, pp. 277–288, 2013.

[27] M. Dharma, "The Contribution of e-Government to Trust in the Government : Correlating trust in the government with satisfaction with e-service by using transparency, responsiveness, accessibility, and security as determinants," 2015.

[28] Mitre, "Privacy Engineering," *Mitre Publication*, 2014. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive-enterprises/privacy-systems-engineering.

[29] S. Pearson, "Privacy, Security and Trust in Cloud Computing," *Springer, London*, pp. 3–42, 2013.

[30] Y. Imamverdiyev, "E-Government Information Security Trust Assessment Model," *Int. J. Res. Stud. Comput. Sci. Eng.*, vol. 3, no. 2, pp. 29–34, 2016.

[31] T. K. Priyambodo and Y. Prayudi, "A Proposed Strategy for Secure and Trusted Environment in e-Government," *Adv. Comput. Commun. Eng. Technol.*, pp. 449–459, 2016.

[32] 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.

[33] N. Alharbi, "E-government Security Mod deling : Explaininng Main Factors and Analysing Existing Models," *Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng. V*, vol. 7, no. 9, pp. 2585–2587, 2013.

[34] F. Belanger and L. Carter, "Trust and risk in e-government adoption," *J. Strateg. Inf. Syst.*, vol. 17, pp. 165–176, 2008.

[35] NIST, "Framework for Improving Critical Infrastructure Cybersecurity (version 1.1)," 2018.