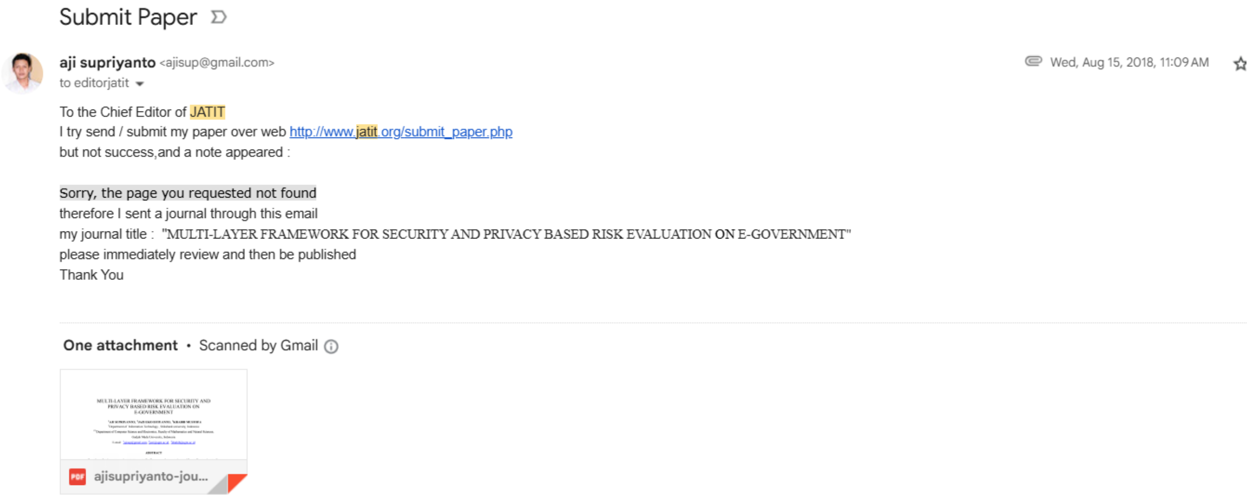
## BUKTI KORESPONDENSI JURNAL INTERNASIONAL JATIT Q3- 2019

JUDUL

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

AJI SUPRIYANTO*, JAZI EKO ISTIYANTO, KHABIB MUSTOFA

https://www.jatit.org/volumes/Vol97No5/2Vol97No5.pdf



Submit Paper

**aji supriyanto** <ajisup@gmail.com>
to editorjatit

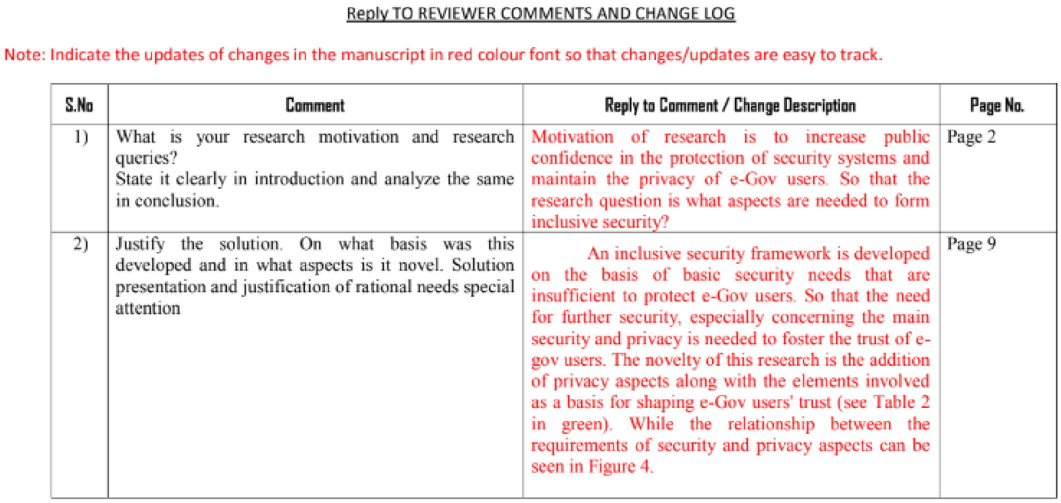
Wed, Aug 15, 2018, 11:09 AM

To the Chief Editor of JATIT
I try send / submit my paper over web http://www.jatit.org/submit_paper.php
but not success,and a note appeared :

Sorry, the page you requested not found
therefore I sent a journal through this email
my journal title : "MULTI-LAYER FRAMEWORK FOR SECURITY AND PRIVACY BASED RISK EVALUATION ON E-GOVERNMENT"
please immediately review and then be published
Thank You

**One attachment** • Scanned by Gmail

ajisupriyanto-jou...



Reply TO REVIEWER COMMENTS AND CHANGE LOG

Note: Indicate the updates of changes in the manuscript in red colour font so that changes/updates are easy to track.

| S.No | Comment | Reply to Comment / Change Description | Page No. |
|---|---|---|---|
| 1) | What is your research motivation and research queries?<br>State it clearly in introduction and analyze the same in conclusion. | 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? | Page 2 |
| 2) | Justify the solution. On what basis was this developed and in what aspects is it novel. Solution presentation and justification of rational needs special attention | 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. | Page 9 |

# 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@gmail.com, [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 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), Plausible 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 perspective also supports the privacy goals. For

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.

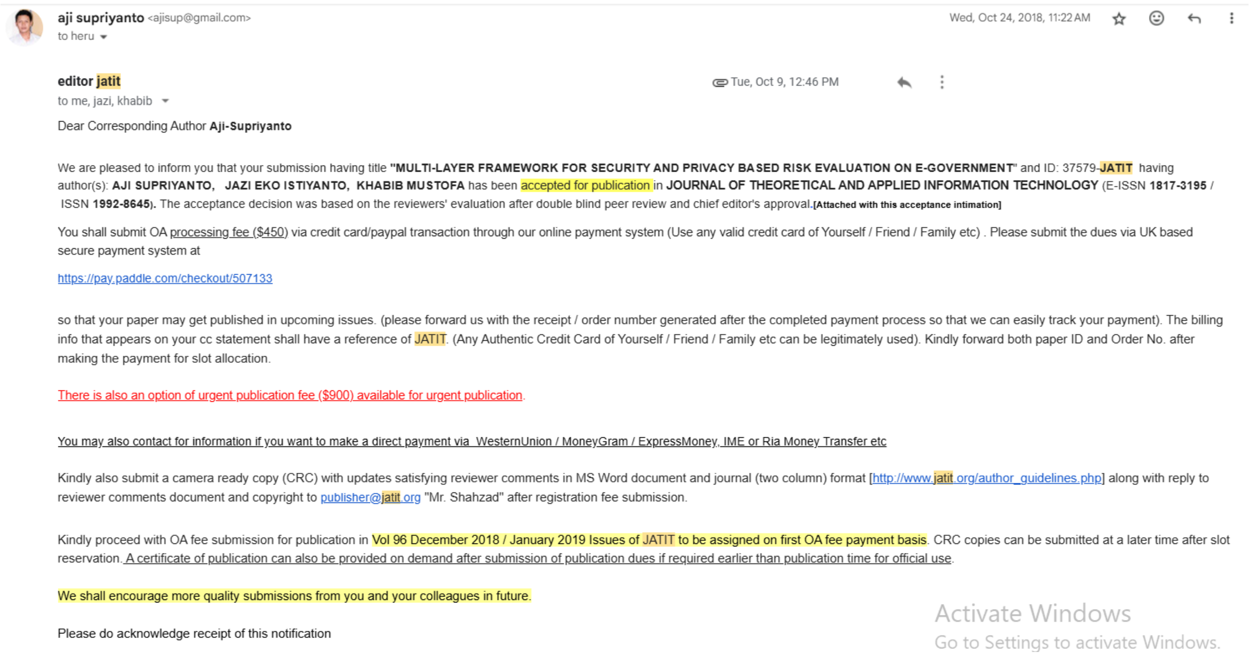
## REFERENCES

[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 concerns in e-government integration , interoperability and information sharing through policy : a case of South Africa sharing through policy : a case of South



**aji supriyanto** <ajisup@gmail.com>
to heru

Wed, Oct 24, 2018, 11:22 AM

**editor jatit**
to me, jazi, khabib

Tue, Oct 9, 12:46 PM

Dear Corresponding Author **Aji-Supriyanto**

We are pleased to inform you that your submission having title **"MULTI-LAYER FRAMEWORK FOR SECURITY AND PRIVACY BASED RISK EVALUATION ON E-GOVERNMENT**" and ID: 37579-**JATIT** having author(s): **AJI SUPRIYANTO, JAZI EKO ISTIYANTO, KHABIB MUSTOFA** has been accepted for publication in **JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY** (E-ISSN **1817-3195** / ISSN **1992-8645**). The acceptance decision was based on the reviewers' evaluation after double blind peer review and chief editor's approval.**[Attached with this acceptance intimation]**

You shall submit OA processing fee ($450) via credit card/paypal transaction through our online payment system (Use any valid credit card of Yourself / Friend / Family etc) . Please submit the dues via UK based secure payment system at

https://pay.paddle.com/checkout/507133

so that your paper may get published in upcoming issues. (please forward us with the receipt / order number generated after the completed payment process so that we can easily track your payment). The billing info that appears on your cc statement shall have a reference of JATIT. (Any Authentic Credit Card of Yourself / Friend / Family etc can be legitimately used). Kindly forward both paper ID and Order No. after making the payment for slot allocation.

There is also an option of urgent publication fee ($900) available for urgent publication.

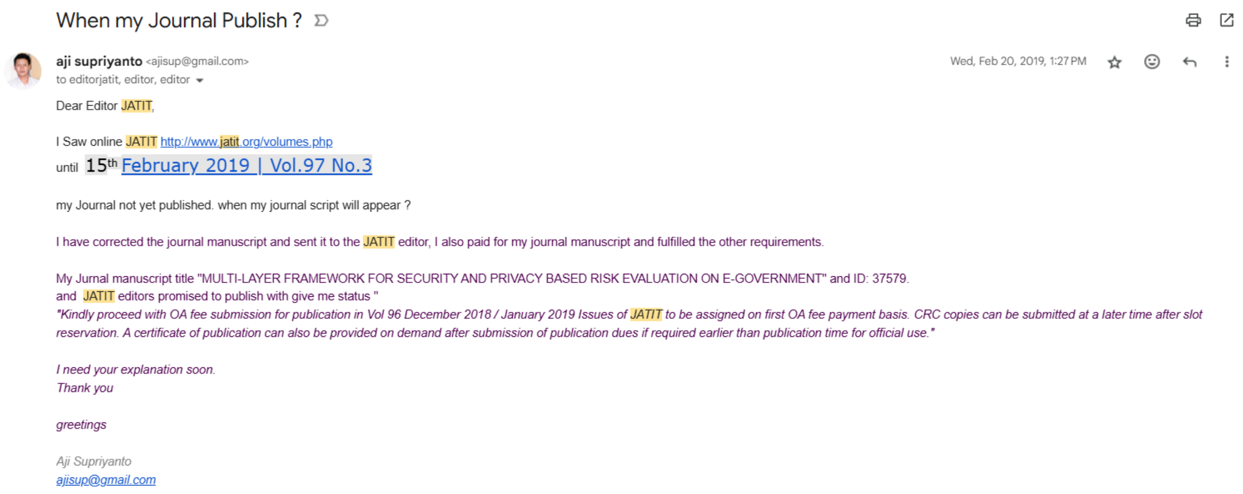
You may also contact for information if you want to make a direct payment via WesternUnion / MoneyGram / ExpressMoney, IME or Ria Money Transfer etc

Kindly also submit a camera ready copy (CRC) with updates satisfying reviewer comments in MS Word document and journal (two column) format [http://www.jatit.org/author_guidelines.php] along with reply to reviewer comments document and copyright to publisher@jatit.org "Mr. Shahzad" after registration fee submission.

Kindly proceed with OA fee submission for publication in Vol 96 December 2018 / January 2019 Issues of JATIT to be assigned on first OA fee payment basis. CRC copies can be submitted at a later time after slot reservation. A certificate of publication can also be provided on demand after submission of publication dues if required earlier than publication time for official use.

We shall encourage more quality submissions from you and your colleagues in future.

Please do acknowledge receipt of this notification



When my Journal Publish ?

**aji supriyanto** <ajisup@gmail.com>
to editorjatit, editor, editor

Wed, Feb 20, 2019, 1:27 PM

Dear Editor JATIT,

I Saw online JATIT http://www.jatit.org/volumes.php
until 15th February 2019 | Vol.97 No.3

my Journal not yet published. when my journal script will appear ?

I have corrected the journal manuscript and sent it to the JATIT editor, I also paid for my journal manuscript and fulfilled the other requirements.

My Jurnal manuscript title "MULTI-LAYER FRAMEWORK FOR SECURITY AND PRIVACY BASED RISK EVALUATION ON E-GOVERNMENT" and ID: 37579.
and JATIT editors promised to publish with give me status "
*"Kindly proceed with OA fee submission for publication in Vol 96 December 2018 / January 2019 Issues of JATIT to be assigned on first OA fee payment basis. CRC copies can be submitted at a later time after slot reservation. A certificate of publication can also be provided on demand after submission of publication dues if required earlier than publication time for official use."*

*I need your explanation soon.*
*Thank you*

*greetings*

*Aji Supriyanto*
*ajisup@gmail.com*