Volume 3, Issue 6, June-2016, pp. 360-365 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Information Security On eGovernment As Information-Centric Networks

Tri Kuntoro Priyambodo[1], Didit Suprihanto[2]

[1]*Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia*
mastri@ugm.ac.id,

[2]*Department of Electrical Engineering, Mulawarman University, East Kalimantan, Indonesia*
didit.suprihanto@ft.unmul.ac.id

Abstract : Information security is a major factor in the service of eGovernment. The using of host to host in previous services of eGovernment is considered as lacking in security. Therefore, it needs more security to serve clients more efficiently and to obtain reliable data provided from the host. One of approach ways to solve the previous security services are based on the safety approach on the contents. The approach on content is used to improve the security which has been used. The approach offered in this paper is called Information Centric Network, this approach is one of the alternatives that is used to secure the content on eGovernment, in addition to approaches by using encryption and captcha. Human aspect is also included as one of the factors of eGovernment security itself.

Keywords - Information, eGovernment, Security, ICN

I. INTRODUCTION

Availability of all government services is the purpose of every government and the current government wants to change the manual service into electronic service [1]. According to [2] era of information and globalization have changed the way people view the government bureaucracy services with the support of Information and Communication Technology (ICT) and it makes a new standard against government bureaucracy. Through the utilization and ease of ICT, society demands that government performance should fast, cheap, and give priority on process-oriented.

eGovernment involves the use of Information and Communication Technology (ICT) to support government operations and to provide government services [3]. However, eGovernment goes even further and aims at fundamentally changing the production process in which public services are produced and delivered, thus it changes the entire range among public relations with citizens, companies and other government [4].

Implementation of eGovernment is a valuable and beneficial expectation. The implementation of eGovernment can obtain some advantages such as all of the work on governance can be performed faster, accurate, transparent, effective, efficient, and accountable. However, there are many challenges and obstacles that must be faced in implementing E-government well, appropriately, and consistently as expected [5]. This opinion is based on Smith and Jamieson opinion in [1] which stated that the key factors in eGovernment is a security system. The consequence of the use of Internet as the main media in eGovernment is the case that Internet is susceptible to threats and vulnerabilities. According to [6] in addition to security issues, another important thing to consider in the implementation of eGovernment is to realize of the Trust to the system, so that it will increase public participation in utilizing all services provided through eGovernment, including those things related to the transaction of data which are confidential.

In particular [1] and [7] in [6] had discussed a wide range of potential vulnerability that is often experienced in the implementation of eGovernment.

Meanwhile, according to [8] there are nine factors that included into the challenges and constraints of eGovernment implementation, such as: ICT Ifra Structure, Privacy, Security, Policy & Regulation Issues, Lack Of Qualified personnel and training, lack of partnership and collaboration, Digital divide, culture, Leaders and management support.

eGovernment implementation requires support from the highest levels of government to achieve successful implementation. Top management support refers to the commitment of the top management to provide a positive environment that encourages participation in the application of eGovernment [9], and according to [10] there are two characteristics or key criteria that must be present on the system eGovernment; those are the availability and accessibility. It supports the opinion from [6] stated that the new trends of internet architecture which is known as information-centric network (ICN) is the paradigm of the Internet architecture that the network content focused on the communication host-to-host.

According to [11], ICN architecture is securing the content itself instead of securing the communication link. Although the concept of future ICN will be worthier to secure the interests of information in the sphere of eGovernment, but the focus of this paper will reveals how information security in eGovernment is equal to the security paradigm of host-to-host. eGovernment still faces a number of challenges in its security aspect. One of the latest solutions approach on security is ICN concept. This ICN concept also can be applied in the concept of eGovernment security. The conventional approach on eGovernment security uses host to host principle. Meanwhile, ICN uses the security content. One of the main points of the eGovernment is the element content, and then the approach to the ICN can be applied on eGovernment to give viewpoint and others alternative of eGovernment security.

II. GENERAL SECURITY PROBLEMS IN EGOVERNMENT

A common problem that occurs in eGovernment is found in the safety factor. This is in accordance with the opinion [1] stated that the eGovernment security is an important topic for the research community, many researchers including government agencies which conduct various research on the security issues. In addition to this opinion, according to [12], the security of eGovernment is an important aspect of eGovernment and should take into consideration at all stages of planning and development, and according to [13] firstly concerned that eGovernment should be approached with the direction of individual privacy protection. Both technical and policy response may be required when dealing with privacy issues in the context of eGovernment and demonstrate that the security of information referred to be cyber security or computer security. It becomes an important eGovernment challenge because it is a vital component in the relationship of trust between citizens and government.

According to [14], privacy and security are important obstacle in the implementation of eGovernment to highlight that eGovernment is an important component in the overall reform agenda because it is functioned as a tool for reform; renewed the interest in public management reform; highlighting internal consistency, and asserting the commitment to actualize good governance objectives. Meanwhile, according to [8], there are nine factors that becomes challenges and constraints of implementing EGovernment, such as: ICT Infra Structure, Privacy, Security, Policy & Regulation Issues, Lack Of Qualified personnel and training, lack of partnership and collaboration, Digital divide, culture , Leaders and management support.

According to [15], eGovernment security requirements should be considered from the viewpoint of non-technical. The availability of the non technical viewpoint makes eGovernment can be distinguished from a variety of e-Commerce. Therefore, there are unique challenges of the process, legal factors and strategies.

According to [16], he stated that eGovernment is not a technical issue, but a matter of the organization. The application of the principles of eGovernment and its functions require new rules, policies, laws and governments to address the changes in the electronic activities including electronic archiving, electronic signature, the transmission of information, data protection, computer crime, intellectual property rights and copyright issues.

According to [17], in an effort to provide direction for the development of eGovernment strategic for the EU (European Union) countries, starting in January 2007 launched RTD2020 eGovernment program in the form of strategic plan development of eGovernment through 13 research areas. In the 13 areas of such research, there

are at least four areas that can be grouped into areas of information security, such as:

- *Trust in eGovernment*, one of its problems is on how to build and improve the concept of trust in eGovernment environment.
- *Information quality*: there are some problems in this topic, one of them is about how the framework can be built to ensure the quality of information and trustworthy certification mechanisms, then how to ensure the quality of information that will be used for the benefit of decision-making.
- *Cyber Infrastructures for eGovernment*. In line with technological developments, the technology platform for eGovernment will involve the involvement of many platforms that must maintain its reliability. The approved standard, prepared module and service must have interoperability with each other and support the growth of industries that support the field of eGovernment.
- *Data privacy and personal identity.* If the personal data is used properly, it will improve the quality of eGovernment services. Unfortunately, on the other hand there is also a potential for abuse itself. Therefore, it all the matters related to policy, security protocols and data management will be very important to maintain a balance between the use of personal data for the benefit of eGovernment services and protection from possible abuse

The opinions about security issues of eGovernment above are an illustration that is used to solve the problems on eGovernment. The general approach that is used to solve security problems on eGovernment is found in the security aspects of the host. Meanwhile, one of the most important elements contained in eGovernment is content, and therefore, contents on eGovernment are a major focus of security problems on eGovernment.

III. BASIC PRINCIPLES OF ICN

Information-Centric Network (ICN) is a new communications paradigm that focuses on the content search from the network regardless of storage location or the physical representation of the content. In ICN, securing the content is much more important than securing the infrastructure [18]. According to [19], in the approach of host-centric network architecture, the things required are the location of its contents to obtain the contents, and also the network communications based on a host name, for example: web servers, PCs, laptops, handsets and other peripheral devices. While, in ICN architecture, the users get the content regardless of location or server host-centric, this mobility allows users to share content and their data anywhere and anytime. Moreover, according to [20] the general purpose of ICN is to achieve efficient distribution and content that can be relied upon to provide a common platform for communication services which are currently available in a special system such as peer-to-peer (P2P) overlay and exclusive content distribution network.

The basic concept of ICN communication from the client perpesctive according to 20] is illustrated in **Figure 1**.

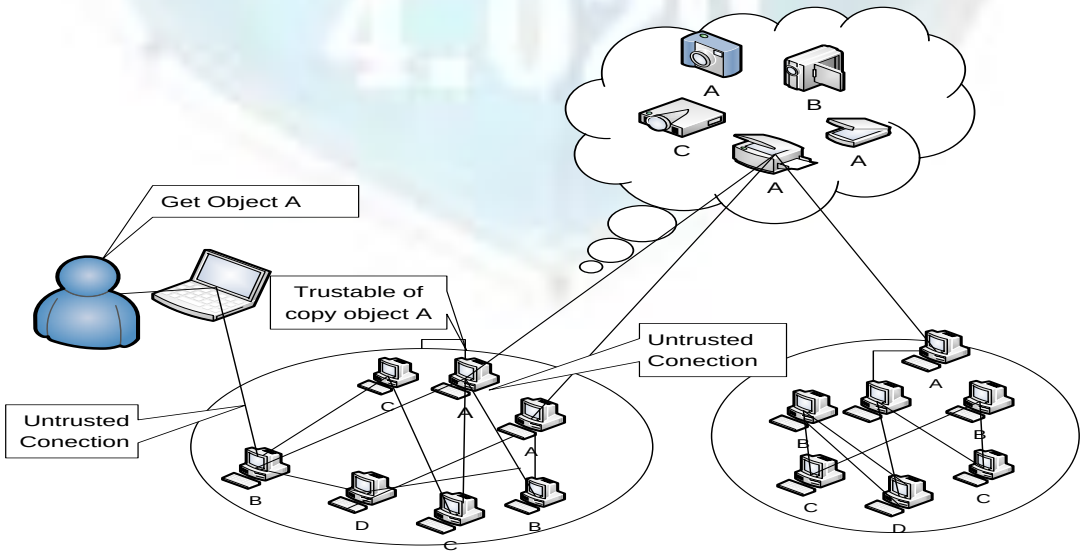

Figure 1. Model of ICN Communication: the client perspective

Picture 1, is an illustration of a network that was formed to fulfill the entire demand of clients in all formed network, whereby the data obtained are from sources wanted by the client, so that it can make efficient caching streamline and applications used as part of the service on the network. Therefore, the integrity of the data provided freely by request from the host considered as trusted.

IV. PROPOSED MODEL OF APPLYING ICN IN EGOVERNMENT

Approach to ICN according to [21] resulted in content taking from the network of other elements of the server locating, security model cannot be taken based on where the packet coming from or to find a server. On the contrary, the design of ICN must secure the content than the path / way, as suggested by [22] and [23] which is considered as better security due to the use of digital signatures and secure package. To ensure a trust of the certified safety package, the package is authenticated by using digital signatures, also securing lines of communication between users and providers, and provides encryption / decryption in each package to secure the package and give confidence.The customers who request resources or content must know the name of the contents, and also the customer must know the content provider's public key, so that the customers can verify the authenticity and integrity of the content. Therefore, the model of ICN itself must bind the object name with the public key of the content provider.

According to [24], there are four key strategies that can be used as a reference for eGovernment information security, the four strategies are:

1. **Aspects of Data Types and Services :**
   a. Sorting / classifying the types of data / information that will be used in eGovernment services.
   b. If the data / information to be displayed / exchanged lead on data privacy and confidential nature, it must be ensured that there is infrastructure which could guarantee the security both in terms of eGovernment service provider and from the user community services.
2. **Policy Aspects :**
   a. It requires establishing integrated policies such as the concept of single sign on for all eGovernment services.
   b. It needs a clear policy regarding to the application on the concept of security system and control toward every level of the user.
   c. The application of the concept of General security policy that in the current status as security measures and contingency plans.
3. **Aspects of Infrastructure and Technology :**
   a. It needs support and commitment to the implementation of a number of security standards such as ISO 27001: 2009 for computer security and the ISO 14443 standard for interoperability.
   b. It requires a deeper study on the adoption of the latest security technologies such as context awareness to improve the comfort in the security aspect.
   c. It needs a policy to control the quality of security that is applied to various types of technology device which is used widely in the community.
4. **Human Aspect :**
   a. It needs continually education to educate about the importance of keeping the privacy of personal identity that is stored in the Smartphone.
   b. Need an education in choosing the various type of computer device that technologically supports security system implemented in eGovernment.

According to [25], human factor will construct a group and eventually becomes a culture of organization. Therefore, the human factor in security is a complex issue and dynamic because it can be associated with various aspects of human being. Meanwhile, [26] stated that efforts to improve security must be followed by increasing feedback from the human factor. Feedback can be obtained through various methods, such as through modeling to determine the characteristics of the human factor in security systems.

Considering the basic principles of ICN and the most important thing of eGovernment security, the issues on eGovernment security can be solved by ICN approach with the proposed solution in securing the contents which are contained in eGovernment by altering host to host security concepts into the concept of content security.

Besides implementing the ICN, the application using another approach also becomes one of the alternatives. The alternatives may include the use of encryption on

each data or information and also the application of captcha as authentication

V. CONCLUSION

Information security is an important aspect to support secure eGovernment services. It really depends on the readiness of the government in providing infrastructure security guarantees as control toward the crucial data. Host to host security approach that has been widely applied to eGovernment can be increased with the approach of the security model that focuses on content, called Information centric network (ICN). ICN model approach focuses on the search content from the network, regardless of storage location or the physical representation of the content. In ICN architecture, the user obtains the content regardless of location or the host server, and it allows the users to share content and data anywhere and anytime. ICN model approach provides better security due to the use of digital signatures and security of data packets. The proposed model in this paper is still conceptual, and it is necessary to step through the next stages of research, in order to examine the extent to which performance of the actual implementation of the ICN in eGovernment implementation.

REFERENCES

[1] F. Hadi, F.T. Muhaya, "Essentials for the eGovernment Security," In : International Conference on Information Society (i-Society), 2011, pp.237-240

[2] Y. Prayudi, T.K. Priyambodo, " Secure and Trusted Environment as a Strategy to Maintain the Integrity and Authenticity of Digital Evidence,"" International Journal of Security and Its Applications, Vol. 9, No. 6, 2015, pp. 299-314.

[3] E. Fraga, "Trends in e-Government: How to Plan, Design, and Measure e-Government," Government Management Information Sciences (GMIS) Conference, June 17, Santa Fe, New Mexico, U.S.A. 2002

[4] C. Leitner, "eGovernment in Europe: The State of Affairs," European Institute of Public Administration, Maastricht, the Netherlands, 2003.

[5] J.S. Djumadal, "Implementasi E-Government Sebuah Harapan Penuh Tantangan Di Provinsi Daerah Istimewa Yogyakarta," e-Indonesia Initiative 2008 (eII2008), Konferensi dan Temu Nasional Teknologi Informasi dan Komunikasi untuk Indonesia, Jakarta 21-23, Mei, 2008,

[6] T.K. Priyambodo, Y. Prayudi, "A Proposed Strategy for Secure and Trusted Environment in e-Government," Springer International Publishing, Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering 362, Switzerland, 2016 DOI 10.1007/978-3-319-24584-3_38, 2016, pp. 449-459.

[7] Moen, N. Klingsheim, K. Inge, F. Simonsen, & K.J. Hole, "Vulnerabilities in E-Government Web portals," International Journal of Electronic Security and Digital Forensics, 1(1), 2007, pp. 89–100. Retrieved from http://www.nowires.org/Papers-PDF/ICGeS_egov.pdf

[8] M. Alshehri and S. Drew, "eGovernment Fundamentals," (2010), 35–42.

[9] A. Akbulut, "An investigation of the factors that influence electronic information sharing between state and local agencies," Louisiana State University. 2003.

[10] M. Sami and M. Mohd, "Best Practices in E-government: A review of Some Innovative Models Proposed in Different Countries," International Journal of Electrical & Computer Sciences IJECS-IJENS, Vol. 12 No. 01, Februari 2012.

[11] A.B. Setiawan, "Implementasi Tata Kelola Keamanan Informasi Nasional Dalam Keranka eGovernment," Jakarta, 2011.

[12] S. H. Bakry and F. B. Muhaya, "Assessing the Benefits of Egovernment," Second Kuwait Conference on e-Services and eSystems, 2011.

[13] W. Seifert, "A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance," Congressional Research Service: The Library of Congress. 2003.

[14] OECD, OECD eGovernment Flagship Report "The eGovernment Imperative," Public Management Committee, Paris:OECD. 2003.

[15] M. Wimmer and B. Bredow, "A Holistic Approach for Providing Security Solutions in e-Government," Proceedings of the 35th Hawaii International Conference on System Sciences. 2002

[16] L. Feng, "Implementing E-government Strategy is Scotland: Current Situation and Emerging Issues," Journalof Electronic Commerce in Organizations 1(2), 44-6. 2003.

[17] M. Wimmer, C. Codagnone, and M. Janssen, "Future e-Government Research: 13 Research Themes Identified in the eGovRTD2020 Project," In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 223–223). Ieee. doi:10.1109/HICSS.2008.179

[18] Abdallah, Hassanein, and Zulkernine, "A Survey of Security Attacks in Information-Centric Networking," 1553-877X (c) 2015 IEEE.

[19] A. Mahfouth, "Security Aspects of the Information Centric Networks Model," International Journal of Computer Science and Security (IJCSS), Volume (7) : Issue (2) : 2013.

[20] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," IEEE Communications Magazine,. 0163-6804/12/ © 2012 IEEE.
[21] A. Ghodsi, T. Koponen, Raghavan., S. Shenker, A. Singla, and J. Wilcox, "Information-Centric Networking: Seeing the Forest for the Trees," ACM 978-1-4503-1059-8/11/11. 2011
[22] M. Walfish, H. Balakrishnan, and S. Shenker, Untangling the Web from DNS. In Proc. of NSDI, 2004.
[23] D. Wendlandt, I. Avramopoulos, D. Andersen and J. Rexford, "Don't Secure Routing Protocols, Secure Data Delivery," In Proc. of HotNets, 2006.
[24] T.K. Priyambodo and Y. Prayudi, "Information Security Strategy On Mobile Device Based Egovernment," ARPN Journal of Engineering and Applied Sciences. Vol. 10, No. 2, February 2015.
[25] K. Parsons, A. Mccormac, M. Butavicius and L. Ferguson, "Human Factors and Information Security : Individual, Culture and Security Environment," Edinburgh, 2010.
[26] J.J. Gonzalez and A. Sawicka, "A framework for human factors in information security," In:WSEAS International Conference on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks, 2002, pp. 1871–1877.

ABOUT THE AUTHORS

Tri K. Priyambodo (M'2012). He became a Member (M) of IEEE in 2012. Since 2008, he has been an Associate Professor with the Department of Computers and Electronics, Universitas Gadjah Mada, Indonesia. From 2010 to 2013 he was responsible for the development of Indonesia Inter-University Student Satellite Project as National Project Leader. He is the author of five books, more than 20 articles. His research interests include intelligent control systems, autonomous unmanned systems, satellite and aerospace electronics, computer networks security and eGovernment related issues.

Didit Suprihanto, Currently he is a PhD Student at Department of Computer Science and Electronics Gadjah Mada University and lecturer at Department of Electrical Engineering, Mulawarman University, Samarinda, Indonesia.

