# INFORMATION SECURITY STRATEGY ON MOBILE DEVICE BASED eGOVERNMENT

Tri Kuntoro Priyambodo[1] and Yudi Prayudi[2]
[1]Department of Computer Science and Electronics, Gadjah Mada University, Indonesia
[2]Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
E-Mail: mastri@ugm.ac.id

## ABSTRACT

Mobile devices today are an important equipment to support daily activities. Nowadays, people generally tend to use mobile devices as it has several advantages, namely: universality, usability, high efficiency, economy and individuation. Mobile devices will become a major channel for eGovernment implementation in the future. In line with the increasing number of information presented as well as the services offered by the government, the greater the challenges of information security are. The exchange of information that happens should be supported by a good security mechanism. However, when discussing on security issues, the opposite matters are matters related to convenience. This paper discusses some aspects of eGovernment as well as solutions to the challenges of information security issues when implementing a mobile device as a communication channel. There are four things that are offered as a solution to information security strategy to keep a balance between security and convenience, namely: selection of data and services, the appropriate policy, adoption of technology and the human education aspect.

**Keywords:** egovernment, information security, mobile devices, strategy.

## INTRODUCTION

The globalization era have changed the way people view the service of the government bureaucracy. The easiness given with ICT support has become the new standard of the government bureaucracy itself. Through the use of ICT, the public demands that government performance is fast, cheap, and process-oriented. According to Indrajit (2013) the use of digital technology has given rise to a new mechanism of government bureaucracy which is then known as the Electronic Government (eGovernment), that is the use of ICT for the exchange of information and services between government agencies with the public and other units that require it.

Indonesia is the largest archipelago in the world with a number of islands reached 17,508. This geographic condition becomes one of the reasons the government to immediately implement eGovernment. In this case, Djoko in Dahlan (2008), argued that based on the geographical challenges it faces, then there are 5 reasons why the Indonesian government needs to immediately implement eGovernment are: to support the government changes towards democratic governance, to support the application of balances authority between central and local Governments, to facilitate commnunication between central and local government, to gain openness, to facilitate the transformation towards an information society era.

Furthermore, according to Rokhman (2011), the initiation of eGovernment by the Indonesian government has been started since 2003. Until now, the index and evaluation of e-government implementation provided by some of the parties have not shown satisfactory results. According to Rokhman (2011), Indonesia is still in the low ranks among other countries in Southeast Asia. Based on data released by the UN (United Nations, 2014), Indonesia currently is ranked 106th out of 193 countries assessed by the UN. EGDI (eGov Development Index) for Indonesia is 0.4487, the index is still below the average value EGDI for all countries assessed is 0.4712.

One problem is that there are a number of obstacles and challenges in implementing eGovernment in Indonesia. In this case according to the survey of several cities in Indonesia by Priyambodo (2007) in a previous study concluded that there are five challenges in the development of eGovernment in Indonesia, namely: human resources, eLeadership, regulation, organization and infrastructure.

Firman as a Director of eGovernment of Ministry of Communication and Information of Indonesia (Kominfo) said, in line with the increasing number of information presented by the government as part of the service, the greater the challenges of information security are. Information security usually involves confidentiality, integrity, and availability. In this case Kominfo concludes that based on the study of the application of ISO 27001: 2009 on the information security, the information security in eGovernment in Indonesia is still relatively vulnerable (Hukum Online 2014). It encourages a number of vendors, such as Microsoft to help strengthen the information security on eGovernment in Indonesia. The assistance is conducted in the form of technical assistance to the government web portal security, payment transaction security and the consolidation between units of eGovernment services.

Agency for Assessment and Application of Technology (BPPT) itself as a government agency that has a strategic function for the assessment and application of technology has implemented six strategies to support the development of eGovernment in Indonesia, one of which is to utilize information and communication technology optimally to improve the quality of eGovernment services to the community. In this case, one of the most prospect technology choices to support such a strategy is the mobile phone. It is because of considering so many users and the extent of mobile phone services in Indonesia (BPPT, 2010).

According to Anestia (2014), average growth of data packet customers for the three major operators in Indonesia (Telkom, Indosat, XL) has reached 40%. Today, with a population of Indonesia alone reaching 237 million, it proves that the number of mobile phone users has reached 270 million with the data packet users reaching 123 million. With this consideration, then in the future, the implementation of eGovernment will shift to the use of mobile devices as a channel of communication. It is then known as mGovernment. Kumar and Sinha (2008) state that mGovernment itself is a subset of eGovernment, that is the application of the concept of anytime, anywhere where information and services provided by the government can be utilized by the community through the availability of mobile devices. There are three things that become the triggers of the emergence of mGovernment services, the penetration of mobile devices in various circles of society, the convergence of telecommunication technologies, and the emergence of 3G data transfer services (Kushchu, 2003).

Related to the issue of eGovernment, according to Kumar and Sinha (2008); there are two things that become critical factors of implementation of eGovernment, that is privacy/security and accessibility issues. Privacy/security issues are important matters given the use of data access via the Internet is vulnerable to interception whether conducted directly by individuals or through the help of tools. While the accessibility issues concern how to provide access to information and services so that people at various levels and conditions can enjoy all the convenience provided by the eGovernment services.

When discussing security, the problems that occur are related to the convenience. Security and convenience are issues faced the most by each institution that implements a security system. In this case, according to Mente (2000) there is a security paradox, "The more convenient we tend to make things, the less secure they are; conversely, the more secure we make things, the more inconvenient it becomes". It certainly applies as well in the implementation of eGovernment application. At the time when eGovernment security solutions are applied to the maximum, it will certainly reduce the sense of comfort in using the service. And vice versa. Therefore, it needs an appropriate strategy to implement security and convenient issues within the scope of the application and eGovernment services. This strategy is necessary so that the function and purpose of eGovernment services are in accordance with the expectations of the government and the society.

This paper is intended to provide an idea of how information security strategy is on the mobile device-based eGovernment. The article will be divided into four sections. In the first section, it will discuss the basic principles of eGovernment/mGovernment, the second part will discuss the basic principles for information security. After discussing the basic aspects, the third part will discuss a few thoughts on the information security on eGovernment and the use of mobile devices as an alternative solution.

## eGOVERNMENT AND MOBILE DEVICE

The definition of electronic government (eGovernment) in general is the system used by the government to perform information management and public service based on information and communication technology. There are various opinions on the definition of eGovernment as follows:

- Shailendra Singh and Karaulia (2011) said, until now there is no standard definition of eGovernment, however, the generally accepted definition is: the application of information and communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges with in government, between government and government agencies of National, State, Municipal and Local levels, citizen & businesses and to empower citizens through access and use of information.
- According to the UNDP cited by Alshehri and Drew (2010), eGovernment is: "the application of information and communication technology (ICT) by government agencies".
- Meanwhile, World Bank definition cited by Alshehri and Drew (2010), eGovernment is: "the use by government agencies of information technologies (such as wide area networks, the internet and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government".

The difference in the definition according to Indrajit (2013) is due to several factors, namely: different scenarios and implementation of the spectrum, the internal condition both macro and micro of countries which implement it, as well as the vision, mission and strategy of development of the country.

Smith and Jamieson (2005) said, all eGovernment activities are intended to fulfill three main objectives, namely:

- Improving service delivery, which directly improves service and satisfaction of the society, business, and community by redirecting resources to priority services.
- Getting value for money from the public purse - that is how the service units on the government can run its service activities in accordance with the budget that has been established, in efficient manner in accordance with the existing rules.
- Aligning supporting government agendas - The government hopes to ensure that the planning, investment and management in the public sector are

oriented to support the achievement of the agendas of the government.

The main objective of eGovernment, according to Smith and Jamieson (2005) is used to encourage the emergence of the service through various possible channels which can be easily accessed by the public, the business environment and the community. The mobile device is a potential communication channel that can be used to implement eGovernment. Kumar and Sinha (2008) said, the advantages of mobile applications compared to web-based applications are on the speed and the ability to data access. Countries with a condition in which the speed of Internet access is relatively slow, but the penetration and the growth of mobile devices are very fast, the use of mobile devices as a communication channel in eGovernment is very appropriate.

According to NXP (2012), the development of mobile devices into the smartphone with the ability not only as a communication tool but also has other abilities equivalent to the functionality of the computer has made smartphones as a technology that adheres in human life. Cloud technology and 3G/4G communication technology support create the comfort of human in conducting their activities with the help of a smartphone. Report from PwC (2011) itself states that currently 38% of mobile phone consumers in the America are smartphone users and most of it is in tablet form. Refers to a survey made by Gartner that the smartphone users always show an increasing trend every year.

The importance of the smartphone as a tool to support their daily activities, according to NXP (2012), is a common thing if someone leaves the wallet, which contains various identity cards and money, but it would be a problem if someone left the smartphone device. This is because all the important data that is typically stored in a wallet, such as identity cards, ATM/credit cards, business cards and money right now could be easily replaced its function through a number of smartphone-based applications.

The use of mobile devices in the implementation of eGovernment has improved the quality of interaction in order to achieve real-time information interaction. In addition, according to Su and Pei (2010), the implementation of mobile devices in eGovernment services provide five virtues, namely: (1) Universality, (2) Usability, (3) High Efficiency (4) Economy and (5) Individuation.

Su and Pei (2010) elaborate on the virtues that the rapid penetration of mobile devices allows the chances of the faster spread of information and services in the community. The use of mobile devices is easier than with computers, eGovernment implementation relies heavily on the topology and the network setting while the use of mobile devices is much more efficient and simple implementation. Economically the use of mobile devices for eGovernment does not require investment as the use of the computer does in eGovernment in general. The use of mobile devices will allow the direct benefit obtained by the user community because the service is direct according to their respective needs.

## INFORMATION SECURITY

The concept of information security is more concentrated on the confidentiality of documents stored electronically. In association with government organizations, the information security means protection against records and data held by that agency. Security information is also related to the monitoring of the recording policy, administration and actions of the government agencies to the documents that are important (Wang, 2008).

There are some definitions of security information:

- According to Smith and Jamieson (2005), Information Security is "the effective implementation of policies to ensure the confidentiality, availability and integrity of information and assets is protected from theft, tampering, manipulation or corruption".
- According NSTISSC cited in Smith and Jamieson (2005), Information Security is "the protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit, and against denial of service to authorized users, including those measures necessary to detect, document, and counter such threats ".

Meanwhile, according to Bell, cited by Smith and Jamieson (2005), the purpose of information security is to protect an organization's information assets and to protect the business processes of the organization as well as the preservation of the CIA principles, namely:

- **Confidentiality:** ensure that the information is only received by those who have authorization to receive it. Information can be confidential for reasons of privacy, commercial or political.
- **Integrity:** ensure that the information can only be changed by the system or those who have authorization to do so.
- **Availability:** ensure that the information and processing systems are always available when the information is required. According to Alshboul (2012), the vulnerability of a system can occur in one of the following four areas, namely: programs, peripherals, communications, input and output.

Furthermore, according to Alshboul (2012), the causes of vulnerability of a system are divided into six factors, namely:

- **Technical and Technology factors:** Application of the proper security system and the availability of many security tools that are either pro or anti become a challenge for the emergence of system vulnerability.
- **Human factors:** Users at various levels of users often

become a gap in the emergence of system vulnerability, both because of the emergence of human error or because the appropriate user behavior supports efforts to strengthen the security of the system.

- **Social factors:** The emergence of various communities is a medium for the dissemination of information. It is not infrequently that the strength of a community becomes the gap for the distribution of sensitive security information on a computer system.
- **Political factors:** The existence of political and business interests becomes the encouragement for the efforts to deliberately find a vulnerability gap of a system.
- **Economic factors:** The selection of a particular technology which is cheaper and easier for a system security can be a loophole for the existence of vulnerability. The cost factor in choosing technology can be exploited by certain parties because of the limited capabilities of these technologies.
- **Networking factors Espionage, and interferences mistransmissions:** Network quality and data transmission media can be a factor in the vulnerability of the integrity and availability of information.

In relation to the implementation of information security within an institutional environment, according to Wang (2008), there are four aspects that have to be concerned, namely:

- Security, which is the support and readiness of the infrastructure and the application of appropriate security policy strategy including in terms of access control.
- Convenient, is the ease of distribution and use by the client on all possible platforms.
- Transparency, is that the system does not require excessive user intervention.
- Scalability, is that the implemented system is quite relevant to be implemented and does not require a large investment.

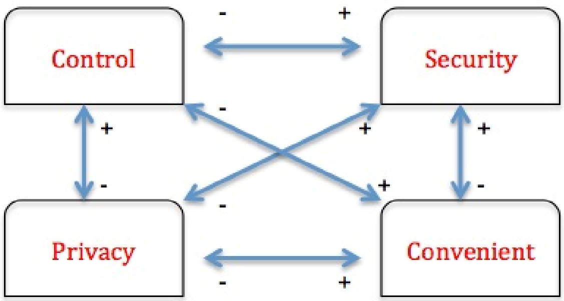

**Figure-1.** Relation of 4 security and convenient dimensions illustration is adapted from the paper of (Montano *et al.* 1988).

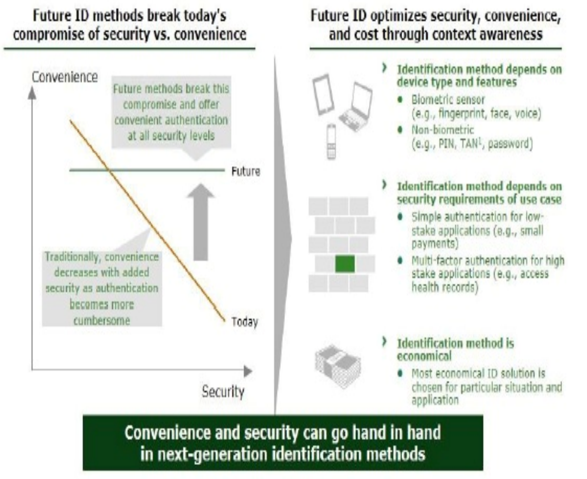
Future ID methods break today's compromise of security vs. convenience
Convenience
Future methods break this compromise and offer convenient authentication at all security levels
Future
Traditionally, convenience decreases with added security as authentication becomes more cumbersome
Today
Security
Future ID optimizes security, convenience, and cost through context awareness
Identification method depends on device type and features
Biometric sensor (e.g., fingerprint, face, voice)
Non-biometric (e.g., PIN, TAN1, password)
Identification method depends on security requirements of use case
Simple authentication for low-stake applications (e.g., small payments)
Multi-factor authentication for high stake applications (e.g., access health records)
Identification method is economical
Most economical ID solution is chosen for particular situation and application
Convenience and security can go hand in hand in next-generation identification methods

**Figure-2.** Context awareness technologies as a solution to get the optimum value between security and convenience. (Security Document World, 2014).

Furthermore, according to Montano *et al*. (1988), security and convenient are the two of the four security dimensions other than control and privacy. In providing a solution to the design of a smart home, then Montano *et al*. (1988) mention four dimensions as the main factor for the relation as illustrated in Figure-1. Illustration provided by Montano *et al*. (1988) can be used as a strategic reference for building eGovernment application service policy. It means that an eGovernment application should be designed in such a way by considering the application of the four dimensions.

Meanwhile, despite the fact that the current security factor is inversely proportional to the convenience, but the development of security technology will be more advanced so that the optimum position between security and convenience will be achieved. Studies in the field of context-aware security will be one of the solutions to overcome this problem (Security Document World 2014; Macdonald, 2010). Context aware in principle is the use of additional information to improve security decision so that more accurate security decisions are obtained and able to support the more dynamic business.

## INFORMATION SECURITY ON eGOVERNMENT

According to Wimmer *et al*. (2008), in an effort to provide strategic direction for the development of eGovernment in the European Union countries, starting in January 2007 the eGovRTD2020 program in the form of a strategic plan for the eGovernment development through 13 research areas is launched. From the thirteenth of the research area, there are at least four same area can be grouped into information security areas, namely:

- Trust in eGovernment with one of the problem is about how to build and enhance the concept of trust in eGovernment environments.

- Information quality: there are some problems in this topic, one of which is about how the framework can be established to ensure the information quality and trustworthy certification mechanism, then how to ensure the information quality that will be used for the purposes of decision making.
- Cyber Infrastructures for eGovernment. In line with the development of technology, the technology platform for eGovernment will involve the involvement of many platforms so that its reliability must be maintained. Agreed standard, prepared modules and services must have interoperability with each other and support the growth of the industry that supports the field of eGovernment.
- Data privacy and personal identity. Personal data, if it is used properly, will improve the quality of eGovernment services, but, on the other hand, there is also the potential for abuse. Therefore, issues related to policy, security protocols and data management will be very important matters to maintain a balance between the use of personal data for the benefit of eGovernment services and protection from potential abuse.

According to Puyosa (2012), the main challenge of implementing eGovernment not only improves the efficiency of public services, but also strengthens the trust and openness among the government administrators with their society through the exchange of relevant information. Unfortunately, this is not supported by a secure infrastructure. In this case, Moen *et al*. (2007) state that most of the countries that implement eGovernment are not built in a safety mechanism that supports authentication, confidentiality, and integrity. In his research, Moen *et al*. (2007) mentioned that most of the implementation of eGovernment is utilizing a web-based application, and it turns out 80% of web-based eGovernment applications were found to have vulnerabilities against web application attack especially Cross Site Scripting and SQL injection.

Furthermore, according to Istiyanto (2005) there are 7 business risks that must be anticipated from the implementation of eGovernment, namely: fraud, error, delay, the publication of the Confidential Information, Intellectual Property theft and Safety-Critical Dependence. The problems that arise in the implementation of eGovernment is the number of e-provided government services, but it turns out that there is no interoperability between services. Each eGovernment service implements a separate security system so that the user is faced with a lot of security systems that require the user to pass authentication. Therefore, according to Wang (2008), the SSO (*Single Sign-On*) mechanism is important to implement for the implementation of eGovernment services. If the system is not implemented, it will have an impact on the reduction of the user's convenience in the use of eGovernment services because they have to authenticate multiple times each time they enter into different eGovernment services.

According to Smith and Jamieson (2005), in a public perspective, eGovernment is viewed as a whole, so if there is a security problem in one of the services, it will be regarded as a fail on the whole process of eGovernment. Thus, efforts to improve the information security on all eGovernment services are regarded as something very important. The level of community participation in the eGovernment is strongly influenced by the fulfillment of the expectations of the society itself, on the quality of services provided, the completeness of information obtained, the speed and flexibility of the information transaction and the important thing is security through an infrastructure which is widely accessible by the society (Alshboul, 2012).

Moreover, according to Kushchu (2003) there are a number of challenges to be faced by the government generally applying mobile application in eGoverment services, namely: Infrastructure development, Payment Infrastructures, Privacy and Security, Accessibility, Legal Issues and Compatibility. It is a challenge for e-government professionals, practitioners, and researchers to demonstrate its contribution, solutions and support to help realize a good eGovernment.

## STRATEGY FOR INFORMATION SECURITY

One example of the implementation of eGovernment applications with a level of very good data security is at handling the passport. There are a number of very strict regulations and standards to ensure that the data stored in a passport are completely secure like (ISO/IEC 15408) for computer security, the ISO 14443 for interoperability standards between devices and services (NXP, 2012).

Mobile device solutions for eGovernment through the use of smartphones should be supported by a secure communication process between servers of eGovernment and the smartphone devices. At least there should be two sides of security to be considered properly. The first is from the server side of eGovernment services, and the second is on the side of smartphone device used.

According to NXP (2012), the implementation of the Trusted Execution Environment (TTE) on a smartphone would be a guarantee of security for data handling in this scope. The thing to note is that if the provided eGovernment services are concerned the identity of personal data. NXP (2012) said, on the application of eGovernment the most fundamental matter is to control the access to personal data information. Therefore, PwC (2011) mentions that there should be an appropriate strategy related to where important personal data is stored. Data is stored on the device, the network, the cloud service or a combination of all three. In addition, no less important matter is to classify the types of data and information that can be accessed/exchanged between the service provider to its users.

There are a number of constraints on the implementation of security in eGovernment mobile, namely:

- User acceptance that is when a number of important data can eventually be accessed or stored on the smartphone devices so how the users treat the technology will be one of the important keys in the application of information security.
- Human factors associated with loss or broken tools can be a loophole for the emergence of security system vulnerabilities in eGovernment services.
- Some smartphone vendors are known to have excellent security support. The diversity of smartphone users in the community will be a constraint for providing security assurance from the aspects of smartphone technology. In this case, of course it is not possible that eGovernment service providers limit their services only in the smartphone user community of a particular vendor.
- Implementation of a secure eGovernment should upgrade the infrastructures that support it. It is a constraint on the funding aspect. It is necessary to have a good vision of eGovernment service providers on the impacts and benefits of upgrading infrastructure and technology for national security as a whole so that funding is not a constraint.

Considering the various constraints, then according to NXP (2012) anyhow the advancement of smartphone technology is but in principle this technology should not be targeted as a total replacement for all government services. eGovernment in general and mobile technology in eGovernment in particular should still be regarded as a complement of the actual government services. In this case, the rapid development of mobile technologies that affect the lifestyle of the community at large should be considered as a challenge to build a new model of communication between the government and society. But according to Security Document World (2014) transfer of government services in accordance with the progress of these technologies is dependent on the ability of the government itself in preparing the trusted transaction services and policies in the handling of the lifecycle of digital identity. While the predictions of Security Document World (2014) state that if from now these two matters can be prepared well by the government, in 2020 saving cost amounting to 30-50 Billion US$ will be obtained.

Therefore, based on previous studies by Priyambodo (2007), the study of various topics related to the basic principles of eGovernment, the potential use of mobile devices moves as a communication channel that is widely distributed in the community, the viewpoint of security, the development of technology, then broadly there are four main strategies that can be used for a reference for mobile device-based eGovernment information security. The four strategies are the Types of Data and Services, Policy, and the Infrastructure and Technologies as well as human. An explanation of the four strategies are as follows:

**Types of data and services**

- Classifying types of data/information that will be used in eGovernment services.
- If the data/information to be displayed/exchanged leads to data private and confidential data, then it must be ensured that there is an infrastructure which can ensure the safety of both the eGovernment service provider or of the user community of its services.

**Policy aspects**

- Need to establish integrated policies such as the concept of single sign-on for all eGovernment services.
- Need a clear policy relating to the application of the security system and control concept to every level of user.
- Implement the concept of General security policy which includes the current status, security measures, as well as contingency plans.
- Law Policy aspects should be prepared to provide support of legislation to anticipate all possible protection and legal arrangements.

**Aspects of infrastructure and technology**

- The support and commitment to the implementation of a number of security standards such as ISO 27001: 2009 for computer security and ISO 14443 for interoperability standards.
- In-depth study for the adoption of the latest security technologies such as context awareness to improve comfort in terms of security.
- The policy to control the quality of security that applies to various types of mobile devices/smartphones that are used widely in the community.

**Human aspects**

- The continuous education about the importance of maintaining personal/private identity that is stored in the smartphone.
- The education to select the type of smartphone devices that support technologically support the security system which is applied in the eGovernment. General description of the four strategies is as seen in Figure-3 below.
- Including education on privacy and security issues.

In previous studies, Priyambodo (2007) delivered five key aspects as the eGovernment readiness. These five aspects are human resources, e-Leadership, regulation, organization and infrastructure. The fifth aspect of his point of view is the ability of the government itself in preparing themselves to implement eGovernment. The community as a user of the service eGoverment will see the successful implementation of eGovernment from the attainment of the objectives and functions of the eGovernment itself as well as the government's readiness to support the implementation. In this case the success of the implementation of eGovernment is when all of the aspects of readiness can be met properly.

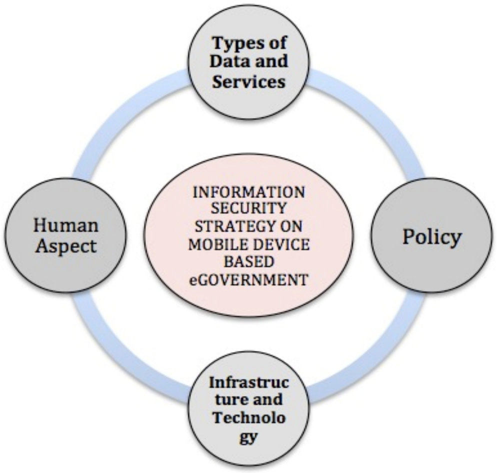
Types of Data and Services
Human Aspect
INFORMATION SECURITY STRATEGY ON MOBILE DEVICE BASED eGOVERNMENT
Policy
Infrastructure and Technology

**Figure-3.** Aspects of information security strategy in eGovernment.

In this study proposed an idea of the eGovernment strategy for securing data based on the mobile application. The strategy includes four aspects, namely the type of the data and service, policy, technology and human aspect. Two of the four aspects, namely the type of data and service as well as the policy entirely in the government domain. While aspects of the technology and infrastructure is the domain between the government and the actors in the technology market. Human aspect itself entirely at the user side. Thus, for the study of eGov security strategy based on the mobile, the government together with technology and society actors should jointly take a role in maintaining the security of the data. Security is not entirely the responsibility of the government as a provider of eGovernment services, but safety is also the responsibility of the owner of the technology as well as the citizens as owners and users of data.

Kushchu (2003) argues, there are three aspects that require the government to consider the mobile application as a communication channel eGovernment future. The three aspects are: the increasing penetration of mobile devices, the evolution of technology, standards and Internet protocol that enables faster data transfer as well as the increasing adoption of mobile applications services provided by individuals or businesses. In this case the four strategies presented in this paper would be a reference to the authority of eGovernment policy holders to consider and pay attention to certain things that the implementation of e-government at the mobile communication channel completely in accordance with the expectations of the government itself and the citizens.

## CONCLUSIONS

In principle, the use of mobile phone/smart phone to support eGovernment services are highly dependent on the readiness of the government itself in providing a secure infrastructure guarantee for the control of important data. If this still cannot be done, then the mobile device-based eGovernment services should be only as a backup of a conventionally similar mechanism.

The very broad characteristics of mobile device users are an alternative communication channel for the implementation of eGovernment. There are many virtues of mobile devices that support the objectives of eGovernment; one of which is large and rapid penetration in society. Therefore in the future, the mobile government will be the tendency of eGovernment implementation. One issue that must be addressed is the security issue, it cannot be separated from the use of public paths for data traffic. The implementation of security in a system is always inversely proportional to convenience. Therefore, it needs a strategy to implement a security system, but still continues to consider the aspect of comfort. There are four things that are offered as a solution to information security strategy in order to keep a balance between security and convenience, namely: selection of data and services, the appropriate policy, technology adoption and the aspect of human education.

The strategy proposed in the perspective of the region even though the Indonesian government, but in fact can be applied by any government. The problems and challenges faced by each country in the data security for eGovernment use mobile application in principle is the same so that the strategy proposed in this paper can also be used as a reference by other countries.

Further research on the issue of the application of these security strategies can be more focused on the technical deepening of each of these aspects, for example, is about mapping information and services that require a dedicated data security, the study of technology standards that can be applied to ensure the communication and data exchange on mobile devices as well as studies on the application of context-aware security for mGovernment implementation. Overall the study in this paper and a series of follow-up research will be a valuable input for the improvement of the quality of eGovernment implementation in the future.

## REFERENCES

Alshboul, R. 2012. Security and Vulnerability in the eGovernment Society. Contemporary Engineering Sciences. 5(5): 215-226.

Alshehri, M., and Drew, S. 2010. E-Government Fundamentals. In International Conference ICT, Society and Human Beings (IADIS). pp. 35–42.

Anestia, C. 2014. Pelanggan Data Tiga Operator Besar Naik Jadi 123,3 Juta Pengguna. Indonesian Finance Today. Available at: http://assets.ift.co.id/pdf/epaper/file/336/Telko_17_3_14.pdf.

BPPT. 2010. Arti Penting Pengamanan Informasi Pada Egovernment. bppt. Available at: http://www.bppt.go.id/index.php/teknologi-informasi-energi-dan-material/589-arti-penting-pengamanan-informasi-pada-eGovernment [Accessed October 15, 2014].

Dahlan. N. 2008. Development of e-Government in Indonesia: A Strategy Model and Its Achievements. Ritsumeikan Journal of Asia Pacific Studies. 24: 35–46. Retrieved from http://www.apu.ac.jp/rcaps/uploads/fckeditor/publications/journal/RJAPS_V24_Dahalan.pdf.

Hukum Online. 2014. Keamanan Informasi eGov Masih Rentan. Hukum Online. Available at: http://www.hukumonline.com/berita/baca/lt540fe9fedd278/keamanan-informasi-ieGov-i-masih-rentan [Accessed October 15, 2014].

Indrajit, R. E. 2013. Electronic Government: Strategi Pembangunan Dan Pengembangan Sistem Pelayanan Publik Berbasis Teknologi Digital. p. 194. Retrieved from http://www.mdp.ac.id/materi/2013-2014-1/SI437/052098/Si437-052098-893-14.pdf.

Istiyanto, J.E., 2005. Aspek-Aspek Keamanan pada Infrastuktur eGovernment. pp.1-12. Available at: http://jazi.staff.ugm.ac.id/gamatech-Jazi.pdf.

Kumar, M. and Sinha, O.P. 2008. mGovernment – Mobile Technology for eGovernment. In: J. Bhattacharya (Ed.). Towards Next Generation eGovernment. Secunderabad India: Computer Society of India. pp. 294-301. Available at: http://www.csi-sigegov.org/2/32_343_2.pdf.

Kushchu, I. 2003. From eGovernment to mGovernment : Facing the Inevitable. In: European Conference on eGovernment. Available at: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan045367.pdf.

Macdonald, N. 2010. The Future of Information Security Is Context Aware and Adaptive. Available at: http://www.bytes.co.uk/files/7313/4383/1104/Gartner_Reprint-_The_Future_of_Information_Security_is_Context_Aware_and_Adaptive.pdf.

Mente, R. 2000. Convenience Vs . Security. Neptune Consulting Group, Inc. Retrieved from http://www.neptune.net/White Papers/Convenience Vs Security.pdf.

Moen, V. *et al*., 2007. Vulnerabilities in eGovernment Web portals. International Journal of Electronic Security and Digital Forensics. 1(1): 89-100. Available at: http://www.nowires.org/Papers-PDF/ICGeS_egov.pdf.

Montano, C. F., Lundmark, M., and Mähr, W. 2006. Control vs Convenience : Critical Factors of Smart Homes. In: 2nd Scandinavian Student Interaction Design Research Conference. Gothenburg Sweden. Retrieved from http://www.cse.chalmers.se/research/group/idc/studentpapers/pdf/control_convenience.pdf

NXP, 2012. Secure and Convenient - Smartphones in eGovernment, Available at: http://www.nxp.com/documents/white_paper/75017422.pdf.

Priyambodo, T. K. 2007. Readiness of Information and Communication Technology Utilization in Indonesia. In International eLearning Workshop. Bandung.

Puyosa, H.D., 2012. eGovernment: Security Threats. IEEE Computer Society. Available at: http://stc-egov.ieee.net/blog/eGovernmentsecuritythreats [Accessed October 15, 2014].

PwC, 2011. Managing security in a mobile world, Available at: http://www.pwc.com/en_US/us/it-risk-security/assets/managing-security-in-a-mobile-world.pdf.

Rokhman, A. 2011. E-Government Adoption in Developing Countries ; the Case of Indonesia. Journal of Emerging Trends in Computing and Information Sciences. 2(5): 228-236. Retrieved from http://www.cisjournal.org/archive/vol2no5/vol2no5_4.pdf.

Security Document World. 2014. The role of trusted digital identity in enabling the eGovernment 2020 vision, Available at: http://www.securitydocumentworld.com/creo_files/upload/article-files/140206_-_digital_identity_in_2020_-_sia.pdf.

Shailendra Singh and Karaulia, D.S., 2011. eGovernance : Information Security Issues. In: International Conference on Computer Science and Information Technology (ICCSIT'2011). Pattaya. pp. 120-124.

Smith, S. and Jamieson, R. 2005. Key Factors in eGovernment Information System Security. In: 18th Bled eConference e-Integration in Action Bled. Bled Slovenia. pp. 1-15. Available at: https://domino.fov.uni-mb.si/proceedings.nsf/0/f648bd1d88db64bfc12570140048d02a/$file/08smith.pdf.

Su, C. and Pei, Z., 2010. Application Model of Mobile eGovernment in Wuhan Urban Circle. 2010 International Conference on Multimedia Information Networking and Security. pp.738-741. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5671352 [Accessed October 24, 2014].

United Nations. 2014. E-Government Survey 2014. p. 284. New York, USA. Retrieved from http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf.

Wang, J. 2008. Design of eGovernment Security System based on Information Security Model. International Conference on Information Management, Innovation Management and Industrial Engineering. (1): 359-362. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4737663 [Accessed October 21, 2014].

Wimmer M., Codagnone, C. and Janssen, M., 2008. Future eGovernment Research: 13 Research Themes Identified in the eGovRTD2020 Project. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008). IEEE. pp. 223-223. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4438927.