CYBERSECURITY STRATEGY FOR SMART CITY IMPLEMENTATION

RG Guntur Alam [1,2] , Huda Ibrahim [2]

[1] Sistem Informasi, Fakultas Teknik, Universitas Muhammadiyah Bengkulu, Indonesia - datuak73@yahoo.com
[2] School of Computing, Universiti Utara Malaysia, Malaysia - huda753@uum.edu.my

KEY WORDS: Smart City, Smart City Security, Cybersecurity, Cybersecurity Strategy

ABSTRACT:

The development of information and communication technology has spread throughout the world. Many benefits can be obtained, but the risks cannot be avoided. Communication grows massively in cyberspace and thus poses a security threat to smart city services. This threat can be overcome through national spectrum by implementing cyberspace security strategies in developing smart cities. This paper describes cybersecurity strategies performed in supporting the development of smart cities. Security strategies are developed based on factors related to the perspective of three pillars of smart city implementation models, namely technology, people, and institutions. Factors related to cybersecurity from these three pillars are explored from the experience of policy makers, actors, and users of smart city services, and evaluated using the opinions of cybersecurity experts and smart cities. This strategy will be a standard document that will be used as a reference in carrying out all processes related to information security in supporting the development of smart cities.

1. INTRODUCTION

The development of information and communication technology has brought about significant influence to change the lives of people in urban areas. The city as the center of human civilization cannot be separated from the problem of excess capacity and comfort, because the more people move from village to city, the newer problems will occur in the city (Purnomo et al., 2016). Technological progress is a choice that must be used by the city to provide the best service to its citizens (Widyaningsih, 2013). This condition triggered the development of various service innovations that led to the development of smart city concepts so that the city faces many challenges and opportunities. By using ICT in planning and building urban cities, traditional regional cities will transform into smart cities, which enable sustainable urban development in the future and make the environment smarter for all its citizens.

Smart city conceptual relationships are classified into dimensions based on characteristics that are often exhibited; the dimensions are technology, people, and institutions (Nam et al., 2011). The technological dimension specifies technology as the key to making cities smarter (Nam et al., 2011). ICT and its applications are fully used to facilitate the involvement of all parties in developing smart cities (Lindskog, 2004). The dimensions of people highlight creativity, social learning, and education, as smart city labels from the dimensions of people show smart solutions by creative people (Nam et al., 2011). From this perspective, the problems associated with urban agglomeration can be solved by creativity, human capital, cooperation between relevant stakeholders and their scientific ideas (Nam et al., 2011) for which Caragliu et al. (2011) called smart solutions. In the institutional dimension, support and policies for institutions are fundamental to the design and implementation of smart city initiatives (Nam et al., 2011). More than other components, smart cities with an institutional focus is seen from a user-centered perspective with more emphasis on citizens and other stakeholders (Meijer et al., 2015).

In developing smart cities, it is difficult to separate it from technology including cloud computing technology as a centralized source of information. The cloud platform is a huge IT resource for smart cities that includes the center of large-scale computing, storage, data, and users, which promotes resource sharing and increases the flexibility of resources, at the same time, will also carry a considerable potential security risk (Piro et al., 2014). Security risks can occur in various forms and cause by many factors, including technological factors and non-technological factors.

Therefore, this paper aims to explore cybersecurity factors in the development of smart cities that are related to technological, people and institutional factors, which are expected to propose cybersecurity strategies that can be accepted by all people and internet users in developing smart cities.

2. LACK OF CYBERSECURITY IN SMART CITY

Cybersecurity refers to internet security, computer networks, electronic systems, and other devices (Olayemi, 2014). In its implementation, there is no doubt that smart cities face various cybersecurity attacks, threats, and criminal violations. The vulnerability of smart cities when exposed by organized groups of individuals or groups can endanger the entire city (Khatoun et al., 2017). Cyber-attacks have increased dramatically since the early 1980s with operations suspected of being 'Logic Bomb' which blew up the Trans-Siberian Pipeline (Wells et al., 2014). When the number of attacks increases, their visibility decreases, and crime increases as shown in Figure 1.

The barriers of preventing cybercrime are the lack of collaboration between industry and the defense environment, the legal capacity to understand the complexity of the virtual environment and to make decisions based on a thorough understanding of facts, collaboration between countries, lack of cooperation between foreign ministries on cyber war and cyber crime (Grobler et al., 2013). Opportunities for attacks increase with the Internet of Things (IoT) (Wells et al., 2014), where the number of network devices is growing rapidly in each sector.

Companies that provide IoT devices for a smart city usually do not include cybersecurity as a priority, mainly because consumers today are more concerned with affordability and often do not realize the security threats posed by unsecured network devices (Allen, 2016). At present the security regulations for the standardization of telecommunications equipment are still inadequate, especially those intended for information system service needs have not been a priority (Sabana, 2017).

An example of problems caused by cybersecurity violations has happened in Atlanta Smart City, the capital of the State of Georgia in the US. In March 2018 it was paralyzed by SamSam, a "ransomware" bug that lasted almost two weeks and affected 30% of "mission-critical" software applications. As a result of this incident, a decade of dashboard legal documents and evidence of dash cameras removed from public officials' computers. Losses due to this attack reached $ 9.5 million (Freed., 2018). Baltimore, a bustling smart city in the US, was also the target of a ransomware attack intended at city emergency services (CAD), occurring in March 2018. In this attack, respondents were unable to access Computer Aided Dispatch (CAD) for 17 hours, so emergency assistance was not implemented efficiently (Kan., 2018).

Cybersecurity in supporting smart cities in Indonesia has received less attention from the government and public service providers, this can be seen from the application of web-based public services often built in haste without the concept of data security and lack of care and privacy protection (Wibowo, 2018a).

From the above cases, it can be concluded that there are weaknesses in cybersecurity in developing smart cities in Indonesia. Therefore, this study aims to explore cybersecurity factors in developing smart cities in Indonesia to propose cybersecurity strategies that can be accepted by all people and internet users in the development of successful smart cities in Indonesia.

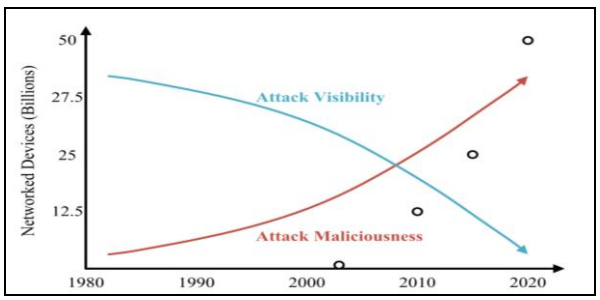

Figure 1. Growth of Networked Devices and Cyber-Attack Visibility and Maliciousness Trends, adopted from Wells et al., (2014)

Cybersecurity in supporting smart cities in Indonesia received less attention from the government and public service providers. Web-based public service applications are often built hastily without data security concept with minimal care and privacy protection (Wibowo, 2018a). This weakness can be seen from a cyber-attack on the Director General of Tax's website on June 11, 2018, an attack on the health promotion website at the Ministry of Health, attacks on the city domain tulungagung.go.id and cyber-attacks on the kpu.go.id domain during Election Provinces and Cities dated June 27, 2018 (Wibowo, 2018b). Table 1 displays data on the security level of web-based smart city applications in Indonesia.

Table 1. The security level of web-based smart city applications in Indonesia

Smart City	Secure	Less	Total
Surabaya	5	12	17
Bandung	2	2	4
Semarang	3	1	4
Yogyakarta	1	7	8
	11	22	33

Source: Adapted from (Wibowo, 2018a)

Of the 33 samples taken from the smart cities of Surabaya, Bandung, Semarang, and Yogyakarta, 22 web-based smart city service applications use insecure links which means that cybersecurity in smart cities in Indonesia is considered very weak, especially talking about the security of personal and institutional data. Cybersecurity in Indonesia is considered less important and not a top priority (Nugroho et al., 2016). Therefore, a policy strategy that regulates various elements related to cybersecurity needs to be made (Ardiyanti, 2014; Danuri et al., 2018). This strategy will be a standard document that will used as a reference in carrying out all processes related to information security in supporting the development of smart cities.

3. THE PROPOSED STRATEGY

This study aims to propose the design of cybersecurity strategies that can be accepted by all levels of society and internet users to support the development of smart cities. Therefore, this study begins by determining the factors that facilitate or hinder the handling of cybercrime based on the implementation of smart city development and cyber security from technological, human, and institutional perspectives. To achieve this goal, factors that might facilitate or hinder the handling of cybercrime from supporting smart cities will be explored from the Three Pillars Smart City Implementation Model adapted from Anindra (2018).

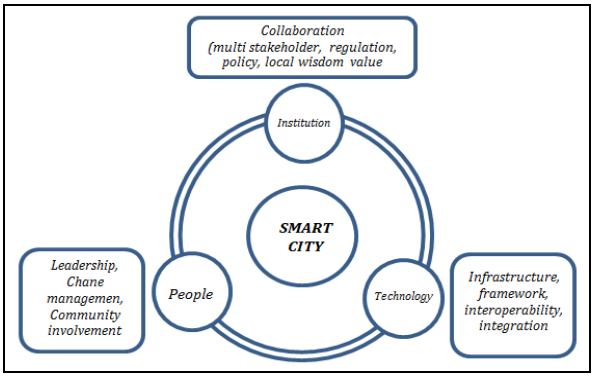

Figure 2. Three Pillars Smart City Implementation Model, adapted from Anindra (2018)

The relationship between the three pillars of the implementation of smart cities according to (Anindra, 2018) is as follows:

The first pillar that supports the formation of smart cities is technology. The rapid development of IoT, Big Data, Cyber-Physical and Cloud Computing Systems also encouraged the

emergence of innovation in solving community problems within the framework of Smart City. Cellular, virtual and wireless technology is the key to the evolution of smart applications that connect the two pillars above so that people and processes become more effective, efficient and firm because the ease, speed, and security of stored data are safe.

The second pillar is people who have the character of high learning spirit, religion and ethnicity, creative problem solving, flexibility to change, accept social pluralism, open-mindedness, and the desire to participate in public life. In implementing smart cities, these people play a strategic role as a determinant of the success of this program so that the term smart people emerge as actors in the application of smart cities. People are also an integration platform approach that connects all government agencies, industries/businesses, schools/ universities, non-profit organisations and individual citizens to make smart city initiatives successful. The output is expected to emerge from this collaboration, which is a pillar of the establishment of strong smart cities such as human cities, learning cities, creative cities, and knowledge cities.

The third pillar is institutional, as smart institutions act as the foundation of smart cities by involving various stakeholders, especially citizens in public/social decision-making and services. Smarter institutions must do more than regulate the output of the economic and social systems, but must interact dynamically with citizens, communities and businesses in real time to trigger growth, innovation, and progress.

This study attempts to fill in the gaps in the literature, proposes a framework for collecting essential data that allows emphasis on areas where the main barriers lie and how they can be resolved at the level of policymakers at the central, provincial and city levels to support smart city development.

4. RESEARCH METHOD

This study will use qualitative research methods based on the conceptual framework of Actor-Network Theory (ANT). The research will be divided into three phases:
1. Theoretical phase
2. Practical phase
3. Evaluation phase.

The research will be carried out in Surabaya involving Surabaya Smart City with three components of the institution that will participate in this study, namely, Surabaya City Government, Policy Makers in Surabaya Smart City Technical Implementation Unit and Surabaya Smart City technical implementation staff. At present, the research is still in the theoretical stage to gather information from secondary sources through literature reviews from journals, books, documents, proceedings, and other academic research.

5. CONCLUSION

Opportunities for cybercrime increase with the development of information and communication technology. Smart city cannot separate from the use of information and communication technology devices. Therefore, a policy strategy that regulates various elements related to cybersecurity needs to be made. This strategy will be a standard document that will used as a reference in carrying out all processes related to information security in supporting the development of smart cities.

This study will identify the barriers of human and non-human factors that are observed from three dimensions, namely people, technology and institutions. The data produced will provide a comprehensive picture of the current implementation of cybersecurity on smart cities in Indonesia. Accordingly, cybersecurity will become a more central issue in smart cities, especially in Indonesia. The proposed cybersecurity strategy will highlight the importance of involving technical implementers, planners and policymakers in the process of problems related to cybersecurity in a smart city to guide them in planning and implementing smart city projects. The proposed strategy can be used in all cities in Indonesia and smart cities in developing countries that have similar problems.

REFERENCES

Allen, N., 2016. Cybersecurity weaknesses threaten to make smart cities morecostly and dangerous than their analog predecessors, London School of Economics, London.

Anindra, F., Warnars, H. S. H. L., Min, D. M., 2018. Smart city implementation modelling in Indonesia with integration platform approach, Bina Nusantara University, Jakarta, Indonesia.

Ardiyanti, H., 2014. Cybersecurity dan tantangan pengembangannya di Indonesia. *Politica*, 5(1), 95–110.

Caragliu, A., del Bo, C., Nijkamp, P., 2011. Smart cities in Europe. *Journal of Urban Technology*, 18(2), 65–82.

Danuri, M., Suharnawi., 2018. Trend cyber crime dan teknologi informasi di indonesia. *INFOKAM*, 2(0), 55–64.

Freed, B., 2018. Atlanta ransomware attack was worse than originally thought. https://statescoop.com/atlanta-ransomware-attack-was-worse-than-originally-thought. accessed 30/07/2019

Grobler, M., Vuuren, J. J. van, Zaaiman, J., 2013. Preparing South Africa for Cyber Crime and Cyber Defense. *Systemics, Cybernetics and Informatics*, 11(7), 32–41.

Kan, M., 2018. Ransomware Strikes Baltimore's 911 Dispatch System. https://sea.pcmag.com/news/20374/ransomware-strikes-baltimores-911-dispatch-system. accessed 30/07/2019

Khatoun, R., Zeadally, S., 2017. Cybersecurity and privacy solutions in smart cities. *IEEE*, 55(3), 51–59.

Lindskog, H., 2004. Smart communities initiatives, University of Linköping, Sweden.

Meijer, A., Bolivar, M. P. R., 2015. Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences*, 0(0),1–17.

Nam, T., Pardo, T. A., 2011. Conceptualizing smart city with dimensions of technology, people, and institutions. Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times, Center for Technology in Government, University at Albany, State University of New York, U.S.

Nugroho, R. A., Santoso, E. B., 2016. Satisfactory analysis about free internet access in public space in Surabaya, Brawijaya University, Malang, Indonesia.

Olayemi, O. J., 2014. A socio technological analy sis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), 116–125.

Piro, G., Cianci, I., Grieco, L. A., Boggia, G., Camarda, P., 2014. Information centric services in smart cities. *Journal of Systems and Software*, 88(1), 169–188.

Purnomo, F., Meyliana, Prabowo, H., 2016. Smart City Indicators: A Systematic Literature Review. *Journal of Telecommunication, Electronic and Computer Engineering*, 8(3), 161–164.

Sabana, M. S., 2017. The Threat Perspective Analysis of Information Crime in Government in the Digital Age. Mercu Buana University Jakarta, Indonesia.

Wells, L. J., Camelio, J. A., Williams, C. B., White, J., 2014. Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, 2(2), 74-77.

Wibowo, S., 2018a. Enriching Digital Government Readiness Indicators of RKCI Assessment with Advance Https Assessment Method to Promote Cyber Security Awareness Among Smart Cities in Indonesia. Indonesia.

Wibowo, S., 2018b. Using the Visual Method of Https Checking for Measuring the Level of Data Transport Security on Web-Based Smart Cities Applications in Indonesia. In *2018 International Conference on ICT for Smart Society (ICISS)*.

Widyaningsih, D., 2013. Surabaya city towards smart city. Gajah Mada University, Yogyakarta, Indonesia.