Advances in Intelligent Systems Research, volume 172
Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)

Cyber Threats Analysis on Jakarta Smart City

Amiruddin AMIRUDDIN[1*], Bio AKRAM[2], and Fitri Hana DINI[3]

[1,2,3] *Sekolah Tinggi Sandi Negara, Bogor, Indonesia*
**Corresponding author: amir@stsn-nci.ac.id*

ABSTRACT
Jakarta Smart City (JSC) is the concept of a modern city utilizing the Internet of Things to enhance and guarantee public services that are fast, inexpensive and environmentally friendly. Various programs were designed, offered and integrated to make it easier for citizens to meet their needs. However, this innovation also raises risks, especially those related to cyber threats. Denial of Service and phishing are some of the threats that might occur in JSC programs. Cyber threats to JSC have not been found much discussed in the literature even though the information is very important for the people of Jakarta to know in order to increase awareness and make early prevention of such cyber threats. In this study, a theoretical cyber threats analysis was conducted to identify cyber threats that might occur in the programs contained in each pillar of JSC, accompanied by alternative security solutions. This study identified several cyber threats to JSC including cyber-fraud, social engineering, eavesdropping, phishing, and DoS. Preventive actions that can be taken include public information security awareness and education, the application of authentication, secure communication channel, and the use of firewalls.
Keywords: *cyber threats, Jakarta, smart city, smart economy, smart environment, smart mobility*

I INTRODUCTION

Smart city is a concept of a city that allows investment in human and social resources, and traditional and modern communication infrastructure promotes sustainable economic growth and high quality of life, with wise natural resource management, through participatory governance [1]. In smart cities, all types of user data are stored on electronic devices, for example on smartphones, to make everything smart. However, sometimes these devices are not competent to manage sensitive user data. Thus, users are facing privacy leaks caused by excessive data collection which means the device application collects user data more than its original function. This is quickly becoming one of the most serious potential safety hazards in smart cities [2]. Researchers have proposed several methods for privacy protection in smart cities such as the use of cryptography, biometrics and ontology, machine learning data mining, game theory, and blockchain [3].

The first and most successful example of smart city concept implementation is Barcelona. The purpose of Barcelona'Smart City (BSC) is connecting people, information, and city elements using new technologies to create a sustainable city, competitive and innovative commerce, and a better life quality with an accountable administration and good maintenance system. The main strategies carried out by Barcelona to realize smart city, inter alia, are establishment of the smart city strategy team, increase of government transparency, presence of political desire, partnership with other key stakeholders, and the use of open data. BSC has at least 22 programs that can be said to be complete reaching various major interests to realize the goals of smart city. The whole program are: telecommunication networks, urban platforms, smart data, smart light, energy self-sufficiency, smart water, smart mobility, renaturation, urban transformation, smart furnishings, urban resilience, citizenship, open government, Barcelona in the pocket, smart garbage collection, smart regulation, health and social services, education, smart tourist destinations, infrastructure and logistics, leisure and culture [4].

The concept of smart cities continues to grow and penetrates various cities in the world including Jakarta. Through the Jakarta Smart City [5], Jakarta applies the concept of the modern city based on the Internet of Things to improve and guarantee public services that are fast, inexpensive, and environmentally friendly for their citizens. Various programs are designed, offered, and integrated to make it easier for people to meet their daily needs such as the ease of getting transportation equipment, finding place for internship, and conducting environmental monitoring. However, smart city innovation not only brings benefits, but also brings with it a variety of risks [6] especially those related to cyber threats. Cyber-fraud, data forgery, Denial of Service (DoS), phishing, and social engineering are some cyber threats that might occur in programs within JSC. If these threats are not watched out and anticipated or prevented early, they can cause a variety of losses.

To the best of our knowledge, cyber threats to JSC have not been found to be discussed in-depth in the literature even though such information is very important for the people of Jakarta to know in order to form and increase awareness and make early prevention. In this study, a theoretical cyber threats analysis was conducted to identify possible cyber-attacks on programs contained in each pillar of JSC. This study identified several cyber threats to JSC including cyber-fraud, social engineering, eavesdropping, phishing, and DoS.

This paper is organized as follows. Section 1 describes the introduction or the research background. Section 2 describes the research method. In Section 3 we describe the programs in Jakarta Smart City, while in Section 4 we

present cyber threats to JSC and identified prevention techniques, and Section 5 concludes the paper.

RESEARCH METHOD

In this study, data collection was done by reviewing the programs of Jakarta Smart City and several related literature on Smart City cyber-threats. Data analysis was conducted using qualitative method, by linking the obtained data about the programs in Jakarta Smart City and cyber threats found in the literature studied. Each program in Jakarta Smart City was studied on its characteristics to look for various vulnerabilities that might be affected by cyber-attacks. Various types of cyber threats or attacks were extracted from the reviewed literature. Furthermore, preventive measures that can be carried out according to the relevant cyber threats were also identified.

JAKARTA SMART CITY

Jakarta Smart City (JSC) is a concept of modern city that utilizes the latest technological advances of Internet of Things (IoT) to connect various programs with users via online channels. The JSC concept is intended as an effort to guarantee and improve the quality of Jakarta's public services in accordance with the general principles of government, through active involvement of the citizens as recipients of these public service benefits. Based on observations and literature, JSC has several infrastructures which are categorized into several pillars i.e. smart mobility, smart economy, smart living, smart people, smart governance, and smart environment [5]. A more detailed explanation of the programs in each pillar is explained in the following section.

A. Smart Mobility

Smart mobility is a pillar to overcome the problems of chaos and traffic congestion in Jakarta and encourage people to choose mass transportation modes that are fast, inexpensive, and environmentally friendly [7]. Programs contained in the pillar of smart mobility in JSC [5] are as following.

Ridesharing

This is a program to reduce the number of vehicles on the road by driving together with people whose destination or direction are the same.

OK-OTRIP

This is a program to change the routes of a number of public transport which are considered ineffective. Later all public transport routes will be integrated with Transjakarta, the main public transport in Jakarta. With the program of public transport users only need to pay Rp. 5,000 for one trip.

Mass Rapid Transit (MRT)

This is a railroad-based public transportation which, according to plan, will extend to approximately 110.8 km and is equipped with CCTV which is integrated with the Jakarta Smart City portal.

Jakprogas Converter Kit Utilization Program (Jackup)

Jackup is a program that supports the conversion of oil fuel to gas fuel by installing a converter to a vehicle. This program aims to succeed in the 'blue sky' program which is a government policy to control air pollution. This program uses technology from a kit type that can synergize with a gasoline engine.

Ganjil Genap

This program aims to reduce the number of vehicles passing certain routes by allowing the operation of even-number-plate vehicles only on even dates or odd-number-plate vehicles only on odd dates. This program is expected to decrease the use of private transportation and consequently increase the use of public transportation.

B. Smart Economy

Smart economy aims to increase regional/global economic competitiveness, ease access for all residents and business people, and realize digitalization of business processes with electronic business programs [7]. Following are several programs in smart economy in Jakarta Smart City [5].

Kaki Lima Online

The program aims to improve the digital presence of street vendors assisted by the KUMKMP Agency and is expected to help increase street vendors' income, and provide a sense of security to the community because only BPOM-certified street vendors will be involved in this program.

Info Pangan Jakarta

This is a program that provides food information in Jakarta. This is one part of strengthening the food security program to achieve the ultimate goal of equitable distribution and improvement of social welfare.

C. Smart Living

Smart living aims to improve security, comfort, health, and culture to be encouraged and happy for all residents in the city [7]. Here are some smart living programs available at Jakarta Smart City [5].

Face Recognition CCTV

Installation of surveillance cameras that have features to detect faces and are integrated with the Jakarta Smart City portal to improve security.

Cekrekening.id

Portal to check problems on account numbers that are likely to be involved in criminal act. Thus, it can help citizens to make cashless transactions more safely.

Rumah Susun (Rusun)

Multi-storey buildings that each part can be owned and used separately, especially for residential areas with certain categories.

Geographic Information System (GIS)

Information system that combines graphical data (spatial) with text data from geographical objects that are useful for urban planning, especially in terms of graphical presentation of information.

D. Smart People

Smart people aim to create a qualified, creative, educated population, able to utilize ICT-based services, and provide a more consistent educational experience [7]. The following are some smart people programs in Jakarta Smart City [5].

I-Jakarta

Digital library application that is useful for simplifying the search for information or books.

Edutrip

Educational tourism program for residents of Jakarta and those outside of Jakarta to gain insight into the use of technology to overcome various problems of the capital.

Co-working Space

Internship program for new graduates, professionals, or final year students to provide hands-on experience or participate in programs related to the Jakarta Smart City concept according to their expertise, interest, and respective disciplines.

E. Smart Governance

Smart governance aims to provide transparency, improve public and social services, integrate organizations with government, and improve community access to services [7]. Some of the smart governance programs in Jakarta Smart City are as follows [5].

E-Musrenbang

Musrenbang is a forum of **stakeholders** in order to develop regional development plans in Jakarta. E Musrenbang is a website and mobile based planning application to support the implementation of community aspirations through Musrenbang in the framework of drafting Local Government Work Plans. E-Musrenbang is a form of transparency in the Jakarta development plan that informs the proposed programs and allows Jakarta residents to directly submit proposals.

Jakarta Smart City (JSC) Lounge

This program utilizes technology by promoting collaboration and transparency to manage the resources to be more efficient in solving problems in Jakarta.

Jaringan Dokumentasi dan Informasi Hukum / Legal Information and Documentation Network (JDIH)

The Legal Information and Documentation Network (JDIH) website contains various legal products in various categories to facilitate access to various data.

Dishub DKI On-time System (DDOTS)

The DDOTS application primarily functions as an attendance recorder that is useful for facilitating the employees of the Dishub (Transportation Agency) so that they no longer need to come to the office when they have to work in the field.

Citizen Relation Management (CIRM)

CIRM is an application that is used by government officials in the DKI Jakarta province to accommodate and follow up on citizen reports that are integrated with the Qlue application (an application intended for Jakarta residents to submit complaints or criticisms related to the city of Jakarta).

F. Smart Environment

Smart environment aims to create an ideal environment with the use of energy and buildings that are environmentally friendly, and free of pollution [7]. The following are some of the smart environment programs that exist in Jakarta Smart City [5].

Truck Compactor

Replacement of conventional garbage trucks with compactor type with closed body design that allows rubbish to be odor-free and safer to transport waste since it minimizes the possibility of garbage scattered all the way to the landfill.

PJU LED Smart System.

Installation of Smart System LED lights that have better and longer-lasting lighting and equipped with a communication gateway system that is connected with a smartphone application so that officers can monitor lights in real-time.

Smart Parking

Information system that provides information about empty parking spaces obtained from detectors in parking locations and the data is sent to the control center which will then be communicated to parking users.

Automatic Weather Station

This automatic weather monitor is equipped with various sensors to record and inform some vital components.

Disaster Warning System.

The Disaster Warning System consists of units of disaster early warning devices, which are equipped with loudspeakers to inform the condition of river water discharge.

Automatic Water Level Recorder

Environmentally friendly water level gauges installed in six river locations and integrated with the BPBD DKI Jakarta website monitoring.

Modern Garbage Bin

This "Wheelie bin" trash bin with German brand Weber has a capacity of 660 liters that can accommodate loads up to 207 kg and is compatible with truck compactors.

CYBER THREATS ANALYSIS

A. Cyber Threats

In this section, the results of the cyber threats analysis as summarized in Table 1 are presented. The description of the cyber threats is following the pillars in JSC.

Table 1 Cyber threats on Jakarta Smart City programs

Pillars	Programs	Threats
Smart Mobility	Ridesharing	Social Engineering
	OK-OTRIP	-
	MRT	-
	Jackup	-
	Ganjil Genap	-
Smart Economy	Kaki Lima Online	Cyber-fraud, phishing
	Info Pangan Jakarta	Phishing, DoS
Smart Living	Face Recog. CCTV	Eavesdropping
	Cekrekening.id	DoS
	Rusun	-
	GIS	DoS
Smart People	I-Jakarta	DoS
	Edutrip	Eavesdropping, social engineering
	Co-working space	Eavesdropping, social engineering
	E-Musrenbang	DoS

Smart Governance	JSC Lounge	Eavesdropping, social engineering
	JDIH	DoS, phishing
	DDOTS	DoS
	CIRM	DoS
Smart Environ-ment	PJU LED Smart Sys.	DoS
	Truk Compactor	-
	Modern Garbage Bin	-
	Smart Parking	DoS
	Disaster Warning Sys.	DoS
	Automatic Weather Station	DoS
	Automatic Water Level Recorder	DoS

1. Smart Mobility

In this category, only RideSharing program was identified vulnerable to a cyber threat called social engineering. The RideSharing allows attackers to socialize [12] passengers through a communicative approach to obtain important information about or from passengers.

2. Smart Economy

In the Smart Economy category, the two programs i.e. Kaki Lima Online and Info Pangan Jakarta were identified vulnerable to cyber threats.

Kaki Lima Online can be exposed to the threat of cyber-fraud and phishing attacks [8] [9]. This is, the street vendors can order their own merchandise, then cancel that order when ordered items have been received. Another threat to this program is that buyers can get phishing [10] through discounts or promotions on behalf of Kaki Lima Online that are not actually from that party.

Info Pangan Jakarta can be exposed to Phishing and Denial of Service (DoS) attacks. The attacker can do phishing [10] in the form of deface on website of the Info Pangan Jakarta or send an email in the name of Info Pangan Jakarta to attract the target. In addition, attackers can carry out DoS attacks [11] [12] on the availability of the website by sending packets repeatedly which can make the server not work.

3. Smart Living

In the Smart Living pillar, three programs, i.e. Face Recognition CCTV, CekRekening.id, and Geographic Information System (GIS) can be exposed to cyber-attacks in the form of eavesdropping and DoS described as follows.

Face Recognition CCTV, attackers can do eavesdropping [13] [8] [14] in the form of gathering information from databases on CCTV or directly monitoring data obtained in real-time.

Cekrekening.id

The attacker can do DoS [11] [12] to turn off the website service of cekrekening.id by sending packets repeatedly until the server does not work so that users cannot use the service.

Geographic Information System

Attackers can turn off GIS services by performing a DoS [13] [8] [11] [12] attack i.e. sending packets repeatedly until the server does not work.

4. Smart People

In the Smart People category, all programs i.e. I-Jakarta, EduTrip, and Co-working Space can be exposed to cyber-attacks in the form of DoS, Eavesdropping, and Social engineering.

I-Jakarta

The attacker can turn off I-Jakarta services through a DoS attack [11] [12] by sending packets repeatedly until the server does not work.

EduTrip

Attackers can do eavesdropping [14] to collect information by disguising themselves as tourists and collecting important information contained in the Edutrip facility. In addition, attackers can get important information by conducting social engineering [15] to employees at the Edutrip location.

Co-working Space

Attackers can gather information [14] by disguising themselves as apprentices and collecting important information contained in the Co-working space facility. Attackers can do social engineering [15] to get important information by conducting social approaches to employees at the apprenticeship location.

5. Smart Governance

In this pillar, all programs i.e. E-Musrenbang, JSC Lounge, JDIH, DKI Dishub System (DDOS), CIRM, can be exposed to cyber-attacks in the form of DoS, Eavesdropping, Social Engineering, Phishing.

E-Musrenbang. Attackers can carry out DoS attacks [11] [12] by turning off the E-Musrenbang website service so that users cannot use the service by sending packets repeatedly until the server does not work

JSC Lounge. Attackers can eavesdropping [13] [8] [14] to collect information by visiting the JSC Lounge that can be visited by common people and collecting important information contained in this facility. Attackers can also get important information by conducting social approaches [15] to employees at this location.

JDIH. The attacker does a DoS [11] [12] to turn off the JDIH service by sending packets repeatedly until the server does not work so that the user cannot use the service. The attacker can also deface the website [10] JDIH or send an email on behalf of JDIH to attract the target.

DDOTS. Attackers can turn off DDOTS services through a Dos attack [11] [12] by sending packets repeatedly until the server does not function so that the employee's time record becomes not the same as the original data.

CIRM. The attacker can do a DoS attack [11] [12] to turn off the CIRM service by sending packets repeatedly until the server does not work.

6. Smart Environment

In this pillar, several programs i.e. PJU LED Smart System, Smart Parking, Disaster Warning System, Automatic Weather Station, and Automatic Water Level Recorder, can be exposed to DoS attacks.

PJU LED Smart System

Attackers can turn off this service through a DoS attack [13] [8] [11] [12] so that the lights do not function properly and road users can be disrupted and the possibility of an accident at night will increase.

Smart Parking

Attackers can turn off this service through DoS attacks [13] [8] [11] [12] so that motorized vehicle users find it difficult to find parking spaces and congestion will increase.

Disaster Warning System

This service can be attacked with DoS [13] [8] [11] [12] so that warnings of disasters do not work when the disaster indicator gives a signal.

Automatic Weather Station

Attackers can turn off this service through a DoS attack [13] [8] [11] [12] so that this device will report incorrect data on the server.

Automatic Water Level Recorder

Attackers can carry out DoS attacks [13] [8] [11] [12] to turn off this service so that the information center does not get an appropriate report if the water level should be anticipated.

B. Defense Techniques

In the previous section, several threats that identified might have arisen in JSC programs are Social Engineering, Cyber-fraud, Phishing, DoS, and Eavesdropping. In this section we discuss several security measures or techniques for cyber threats as summarized in Table 2, including: providing education or socializing information security awareness to the user community; ensuring the communication path or channel used is secure and the website to be targeted is not a fake website; applying authentication techniques; redirecting communication routes if necessary; using firewalls, and encrypting data or randomizing signals.

Provide information security awareness or education to the users or community

To prevent the threat of social engineering or phishing, the public needs to be educated and to increase their awareness not to share important information or credentials, especially to unknown people. Especially if sharing information is done through the Internet or social media, don't be easily fooled by various lure. In addition, users need to be educated and careful not to receive any discounts and always check the correctness of the information received.

Ensure that the communication channel is secure and the destination website is not a fake one

Users of JSC programs must ensure that the communication lines used are truly secure. Likewise, the targeted website must be ensured to use the correct URL address with the https method.

Implement authentication techniques

For the threat of cyber-fraud, preventive measures that can be taken are ensuring that payment has been made before the shipment of goods, and in addition, the use of authentication can also be applied to detect cyber-fraud perpetrators.

Use firewall

Actually it is very difficult to prevent DoS attacks, especially the distributed DoS because such attacks can be carried out by many nodes from various places. Efforts that can be done or prevention are using a firewall and tracking incoming TCP connections by applying SYN cookies to the browser so that SYN floods can be reduced. For HTTP flooding, reverse proxies can be deployed at several points to filter access in a distributed manner so that it can prevent or reduce system overload.

Implement data encryption or signal randomization

The threat of eavesdropping can be prevented by randomizing both the signals used to communicate and the data or information transmitted. Eavesdropping by visitors such as tourists or apprentices can be anticipated by monitoring access through visitors' registration.

Redirect route

An effort that can be done to stop the DoS attacks is to contact Internet service providers to divert the DoS route to the trash. However, even though this effort is effective in preventing DoS, it also closes access from all users. Therefore, users need to be told to be patient for some time while making repairs for stopping such attacks.

Table 2 Defense Techniques

No.	Defenses	Targeted Threats
1	Information security awareness and education	Social engineering, phishing, cyber-fraud
2	Secure communication channel	Social engineering, phishing
3	Authentication	Cyber-fraud
4	Firewall	DoS
5	Encryption or scrambling	Eavesdropping
6	Redirection	DoS

CONCLUSION

In this study, cyber threat analysis was carried out on Jakarta Smart City based on a literature review. Various programs in the six pillars of JSC were investigated to identify cyber threats that might occur in the program. Based on the results of identification, JSC programs are vulnerable to cyber threats in the form of cyber-fraud, social engineering, phishing, eavesdropping, and DoS. Some precautions that can be taken in connection with these threats are conducting regular security education or awareness for users, monitoring access and applying authentication mechanism, and using firewalls to filter packets that enter the network so that dangerous packages can be restricted.

REFERENCES

[1] A. Caragliu, C. Del Bo, and P. Nijkamp, Smart Cities in Europe, Journal of Urban Technology, vol. 18, No. 2, 2011, Page(s): 65-82

[2] Yibin Li ; Wenyun Dai ; Zhong Ming ; Meikang Qiu , Privacy Protection for Preventing Data Over-Collection in Smart City, IEEE Transactions on Computers, Volume: 65 , Issue: 5 , May 1 2016, Page(s): 1339 – 1350.

[3] Lei Cui; Gang Xie; Youyang Qu; Longxiang Gao; Yunyun Yang, Security and Privacy in Smart Cities: Challenges and Opportunities, IEEE Access, Volume: 6, 2018, Page(s): 46134 – 46145

[4] Josep-Ramon Ferrer, Barcelona's Smart City vision: an opportunity for transformation, Special Issue: Smart Cities at the Crossroads, Journal of Field Actions, vol. 16, 2017, Page(s): 70-75

[5] Jakarta Smart City. Accessed 20 April 2019 http://smartcity.jakarta.go.id/.

[6] Anatoliy N. Kazak and Nelli Shamayeva, "Separate Aspects of Smart Cities Security", 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), 2018, Page(s): 216-218.

[7] United Nation Commission on Science and Technology for Development, “Smart Cities and Infrastructure”. Budapest, 2016.

[8] Beale, S. S., & Berris, P. (2018). Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses. Digitization and the Law, Page(s): 21-40.

[9] Sharma, Ushamary & Ghisingh, Seema & Ramdinmawii, Esther. (2014). A study on the Cyber - Crime and Cyber Criminals: A Global Problem. International Journal of Web Technology. 3. Page(s):172-179.

[10] Suganya, V., A Review on Phishing Attacks and Various Anti Phishing Techniques. International Journal of Computer Applications, 139(1), 2016, Page(s): 20-23.

[11] Ijaz, S., Ali, M., Khan, A., & Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. International Journal of Advanced Computer Science and Applications, 7(2).

[12] Piskozub, A. (n.d.). Denial of service and distributed denial of service attacks. Modern Problems of Radio Engineering, Telecommunications and Computer Science (IEEE Cat. No.02EX542).

[13] R. Mirza, Q. Muhammad, G. Sajid, and U. Saleem, “Security Issues in the Internet of Things (IoT): A Comprehensive Study” International Journal of Advanced Computer Science and Application. vol. 8, No. 6, 2017.

[14] Li, X., Dai, H., Wang, Y., & Wang, H. (2015). Eavesdropping activities in wireless networks: Impact of channel randomness. TENCON 2015 - 2015 IEEE Region 10 Conference.

[15] Kher, T. A., & Kariya, S. L. (2016). A Survey on Social Engineering: Techniques and Countermeasures. IJSRD - International Journal for Scientific Research & Development, Vol. 4(Issue 07), Page(s): 258-260.