Single Access Key for Activities in Smart City

Dany Eka Saputra
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
dany.e.saputra@students.itb.ac.id

Suhono Harso Supangkat
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
suhono@itb.ac.id

***Abstract*—Smart city is a new concept for developing and managing a modern city. It involve the usage of technology, especially information and communication technology, to monitor and understand the condition of a city then to act accordingly. Researches about the architecture of smart city, although the subject is relatively new, has taken the interest of many researcher and big technology company. However, every research mainly focus on the architecture and flow of information in a smart city. The researches left a hole in how the citizen interact and prove their identity in a smart city. This paper over a solution for citizen's identity authentication. The usage of single access key in form of physicalmetrics is proposed. The solution enables a citizen to access multiple services within smart city with a single device or identity.**

***Index Terms*—authentication, smart city, digital identity**

I. Introduction

The majority of population in the world is concentrated in many big cities. This condition will continue and it is estimated that 60% of world's population will be living in cities by 2030 [1]. This condition will create many problems in city's activities. The supply of energy, transportation of people and goods, citizen health, including government bureaucracy has its own challenge to meet the citizen needs.

Smart city is the most used concept for managing and building future cities. But, the concept itself is not strictly defined. IBM [2] has their on concept of smarter planet and it has been deployed in couple of cities around the world. IEEE [3] also already started to promote the research and implementation of smart city among its member.

Aside of the difference in concepts, there are silver line that connect each concept. The usage of information and communication technology is a prime requirement in a smart city. It is a general requirement that define the basic structure of smart city despite the concept. What is smart city, how information is distributed, what is the best technology suited to support smart city, and so on. Those are the mainstream focus on research on smart city. The big architercture and technology of smart city.

The citizen is rarely become the subjet of research on smart city. They tend to be passive object in every research. In smart city, some of citizen's activity will be transferred in digital world. For doing so, there must be a technology or methodology to ensure the integrity and security of citizen identity in smart city.

This paper will address citizen identity management in smart city as our main focus. A single access key is proposed as a method for citizen to access smart city services. This method will lessen the citizen burden to bring multiple type of access key, like identity card or payment card, but still can access multiple service in smart city.

II. Smart City

In this section, we will be discussing smart city. Some research about smart city will be presented here to give a better understanding about what is smart city. The discussion also meant to give clear reason behind the importance of single access in smart city.

A city can be viewed as a system which goal is to give its citizen a opportunity to live their life fully. This goal is reached by providing and managing energy, transportation, education, and any other field of activities. As number of citizen increases, those field of activities becomes more complex and can be viewed as an independent system. Thus the city becomes a system of systems. Managing the city cannot be done with conventional methods or paradigms.

Smart city come to fill the hole. Smart city is a concept where all activities in a city is managed with the support of technology. Stanford Program on Regions of Innovation and Entrepreneurship (SPRIE) launched Smart Green City [4] in 2008. It is an initiative that focused in promoting innovation of combined fields of technology, business, and policy at urban scale. The initiative offer a method to manage city as system of systems. The solution consist of 4 (four) primary area: smart green, smart living (community), smart media, and smart business. According to SPRIE, those 4 areas are the main activities in a city.

SPRIE solution is based on the deployment of smart system service. The goal of this deployment is : [5]

> *"to enable the capacity to dynamically configure the processes to adapt to the rapid changing market, as well as an ability to quickly develop/adapt applications to support the execution of these changes"*

The architecture itself is a platform where any other smart system solution will work and operate. It rely on the usage of ICT to distribute data and information quickly from the city to the city's manager and back to the city again.

IBM [2] define smart city as the usage of information technology to sense, analyze, and integrate the key systems

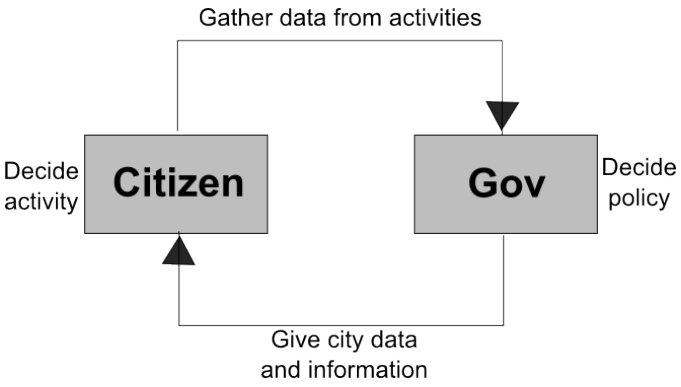

Fig. 1. Relationship of Citizen and Government in Smart City

within a city operation. Intelligent response and adaptation is the main forte of IBM's concept of smart city. The concept itself comes from IBM greater concept of Smarter Planet [6].

The IBM's architecture of smarter city focus on effort to monitor city conditions. This is achieved by employing a series of smart sensor and citizen participation. Citizen can actively help city monitoring process by submitting a condition they encounter. This collaboration of citizen and government ensure that a condition which cannot be sensed by technology (such as damaged road) still can be monitored.

From IBM Smarter City concept, we can conclude that there are a mutual relationship between the government and it citizen. The citizen gathering data from its citizen's activities. The data is used to make quick and correct decision to enhance the city's life. In return, the citizen can used the big data collected by government to make decision for their activity. Fig. 1. summarize this relationship.

Kehua et. al. [7] has different yet unique approach in viewing smart city. In this paper, the writer state that a smart city is developed in the basis of a digital city. Remote sensing, position tracking, and other spatial information become the main means to build the smart city. Although it has different approach than the concept from IBM or SPREE, it still emphasize the usage of ICT to gather and propagate data in smart city.

The work of Kehua et. al. also contain an approach to building smart city. Their approach divide the development of smart city into two big building block, the core platform and application system. The application system is a system of systems that provide services to the city. The application itself is divided based on its purpose, such as health care, environmental, and so on. This approach ensure that each system can be built independent from each other. This is means that every city can choose its own application and implement it gradually. Each application must be built upon the core platform to ensure fluid data exchange between applications.

From all the researches that have been discussed, we can conclude that ICT is the core backbone of a smart city. Furthermore, we can divide a smart city into 2 (two) different sides, physical city and digital city. Physical city is the real city where the citizen do their physical activities. It harbor the citizen and provide all the infrastructure needed by citizen (e.g. road, electricity, and gas). While digital city is where all the digital activities of a city is held, such as city's sensor or electronic services.

Each citizen on smart city will have their activities conducted on these two sides. For example, a citizen that wants to go to their workplace from home is checking the schedule and posisiton of a public transport he/she want to take by accessing public transport website through his/her smart phone. The act of checking public transport schedules is done in digital side, which populated by data generated from physical city. While the actual activity of riding a public transport is done in physical side.

Although each concept has a very detailed description of a smart city, every one of them still have a hole left that can impede the implementation of smart city. As we have discussed before, in smart city a citizen activity can be held in physical side or digital side. The problem lies in digital side where each data must be validated so it will give correct information. The identity of every citizen in digital side also must be validated. This can be done by providing each citizen a digital identifier, such as user name and password.

The usage of user name and password has their own problem. As [7] pointed out, there were a numerous services in a smart city. For each service, a citizen is required to have an user name and password. Using single user name and password for all the service is not visible because there will be security risk issues. If an unauthorized person can get his/her hands on a citizen user name and password, he/she can act as that citizen in digital side. To overcome this problem, we propose a solution of single access key consisted of several data that can be used as digital identifier or access key to services in smart city.

III. Access Key for Smart City

The solution of aforementioned problem is divided to two parts. The first part is the shape of digital identifier that can represent a person identity in digital world with high integrity. The second part is the back-end system which allow the digital identifier used in multiple service within smart city without any duplication of identifier.

A. The Digital Identifier

Our first step for developing the solution is considering the type of authentication method that best suited to represent identity in digital world. This problem plays a vital part in our solution because of internet/digital attribute of anonymity. The attribute means that no one can be entirely sure that someone is someone they claim to be.

According to [8], [9], [10], there are 3 authentication type that can be used for this purpose:

1) Pseudometrics: It is an authentication based on knowledge known only to the person entitled. This type can be in form of Personal Identification Number (PIN) or password.

2) Physicalmetrics: This authentication relies on an object possessed by a person that can represent his/her identity. Passport or identity card are the perfect example for this case.

3) Biometrics: This form of authentication is using something that uniquely attached to a person. Voice identification, face recognition, and fingerprints pattern are perfect example of this authentication type.

Among those three types of authentication, the biometrics type is the strongest kind to represent someone identity. This is due to the fact that biometrics data for each individual is unique and cannot be reproduced by anyone. But the usage of biometrics have some weakness in term of implementation cost. The device used to read biometrics data is quite expensive.

The pseudometrics on the other hand are quite simple and cheap to implement. This is why many of service in the internet uses username and password as means of user identity authentication. In exchange of its simplicity, pseudometric has the lowest rating in term of security than the others.

The problem of using pseudometrics, such as password, is people tend to use obvious words as their password (e.g. name, sequence, birth date). The cause of this tendency is the easiness to remember those words. The usage of meaningless word as password, although more secure, is hard to remember because nothing can be associated with those words. The work of [11] show the vulnerability of using obvious words as password. It show that almost 25% of password in their experiment can be cracked via direct cracking.

The physicalmetrics has higher security than a pseudometrics. With some kind of engineering, countermeasure can be installed to the object used to prevent any forgery of identifier object. However, this trait can only works in physical world.

Physicalmetric, as its name imply, uses physical object that belong to a person. For example, a passport is a book which contains identity of its holder. For physicalmetrics to works on digital world, it need to be injected by digital data. The example of this usage is a password in RFID tags or identity card built from smart card.

Based on the knowledge of each authentication strength and weakness, we conclude that the best solution is to combine pseduometrics and physicalmetrics. The data for authentication is made from a string of identifier which stored in an object, such as smart card or smart phone. The benefit of using this method is we can store password derived from illegible words without the risk of user forgetting it. Also by using a string of meaningless words, the strength of a password can be doubled and make any brute force type of cracking infeasible.

Our work on identity authentication does not stop here. As we have discussed before, using a single identity credentials possess a security risk in case someone get their hands on a person identity. To prevent this, we develop a number of credentials that can represent someone identity. Those credentials are stored in an object a person have. This is the concept of our single access key, by using a physicalmetrics someone could access multiple services in a smart city.

In [5] and [7], it shown that there are multiple services that can be grouped into some clusters. These clusters have their own business process and requirement. However, from much closer study we conclude that there are 4 (four) type of services that required authentication of user identity. These four types of services are described in Fig. 2.

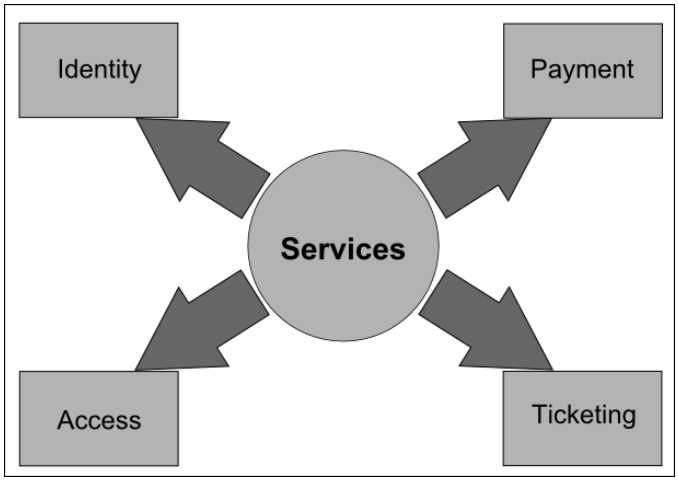

Fig. 2. Type of service which requires authentication

Our single access key is consisted of several tokens data to represent a person identity credentials in each of services. The data architecture of single access scheme is described as follow:

- *Identity*. The token for this service is a single unique ID number that represent user's identity. This token will serve as authentication of user identity for multiple services that require identity of user. To improve the integrity of user's identity we also attached a digital signature private key that belong to user.
- *Payment*. There are many type of electronic payment we can use nowadays. The token used for this service consist of several data which each data represent an authentication for specific type of electronic payment, such as credit card or electronic cash.
- *Access*. Access services requires credentials that prove a person have the right permission to access a service. It does not require user identity. For this reason, the token used in this service is a data that represent access level of a user.
- *Ticket*. Parking and public transport ticket are accurate example. This service require different data than other services. It require some timestamp and monetary data. In our concept, we define ticket as a data used for proving a time-limited membership or access, such as subscriber train ticket.

As a security measure, to access the token of each service we employ separate access key. This is meant to limit the ability of each service to access token that only matter to it. With this scheme if one of the token or access key is broken, the integrity of other data still remain intact. The data arrangement or our single access key can be viewed in Table 1.

TABLE I
DATA OF SINGLE ACCESS KEY

Services	Data	Data Type
Identity	ID Number	String
	Private key	String
Payment	e-cash data	String/Value
	Credit card account	String
	PIN	String (hash)
Access	Key	String
Ticket	Service ID	String
	Timestamp	String
	Service Signature	String

B. Access Management System

The solution we describe before cannot properly function as itself. It need support at back-end so every service can use the single access key easily without any major changes on its system. Access Management System (AMS) is the back-end solution which manage the database of each access key.

The system records and manages each access key holder's identity and mapping all the services it subscribe. The services itself is not necessary part of the system. It could be a service that any other vendor in smart city develops. AMS will bridge the single access key with the services.

This arrangement has another benefit. In case of losing the physicalmetric which user store his/her access key, the user only need to contact the AMS administrator to block or replace his/her credentials. Instead of user contacting each service to process his/her loss, the access management system will spread the loss notice to all service which the user enlisted.

In our design, the AMS consist of 2 (two) sub-system. These two sub-systems, payment gateway and access database, will works cooperatively to bridge the user with services in smart city. The payment gateway is a sub-system that manage financial transaction between user and services. With the usage of payment gateway, user and service provider is not needed to connect to their bank to settle a transaction. This way, user can use any method of electronic payment he/she had regardless the services.

Access database records all user primary data, such as name, address, and birth date. The mapping of users and their service also recorded in this database. This arrangement will increase the data management on service provider side. Service provider does not need to have user primary data in their database, they can access the user data via access database. The architecture of this system is shown by Fig. 3.

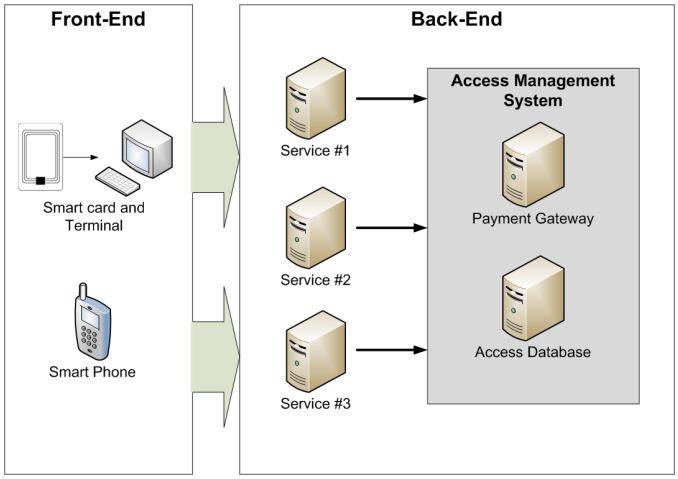

Fig. 3. Architecture of Access Management System

IV. CONCLUSION

On previous section, we have shown our work on providing a solution on citizens identity authentication in a smart city. The solution increasing the easiness of accessing services in a smart city. Each citizen only needs to have one single object (a computing device) instead multiple passwords to access services.

We also have shown that the solution is supported by a back-end system to ensure all service can use it without any data redundancy. This solution can enhance any implementation of smart city without increasing the implementation cost greatly. It is a comprehensive solution that considering the ability of smart city management.

However, there is some weakness in our solution. The implementation of this solution will require a massive database of public-private key pairs that each citizen have. Current Public Key Infrastructure (PKI) is not suited to manage key pairs of this magnitude. An efficient PKI need to be developed to fill this hole.

REFERENCES

[1] "World urbanization prospects, the 2011 revision," Apr. 2012. [Online]. Available: http://esa.un.org/unup/CD-ROM/Urban-Rural-Population.htm

[2] "Smarter cities," 2014. [Online]. Available: http://www.ibm.com/smarterplanet/

[3] "Smart cities," Jul. 2014. [Online]. Available: http://smartcities.ieee.org/

[4] "Smart green cities," Jul. 2008. [Online]. Available: http://sprie.stanford.edu/

[5] K.-Y. Wang. (2012) Enabling smart system services in smart cities. presentation. [Online]. Available: http://iis-db.stanford.edu/evnts/7239/SPRIE_SmartGreenCities_-Ko-Yang_Wang_June_2012.pdf

[6] "Smarter planets," 2014. [Online]. Available: http://www.ibm.com/smarterplanet/

[7] K. Su, J. Li, and H. Fu, "Smart city and the application," in *2011 International Conference on Electronics, Communications and Control*, 2011, pp. 1028–1031.

[8] N. Mastali and J. I. Agbinya, "Authentication of subjects and devices using biometrics and identity management system for persuasive mobile computing: A survey paper," pp. 1–6, 2010.

[9] D. Bala, "Biometrics and information security," pp. 64–66, 2008.

[10] J. Wayman, "Biometrics in identity management systems," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 30–37, Apr. 2008.

[11] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," pp. 5–14, 1990.