

An Authenticated Passengers based on Dynamic QR Code for Bandung Smart Transportation Systems

*Rafinno Aulya, **Hilwadi Hindersah, **Ary Setijadi Prihatmanto, and *Kyung Hyune Rhee

* Dept. of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea

** School of Electrical Engineering and Informatics, Bandung Institute of Technology, Indonesia

Abstract—Involving smartphone users in the smart transportation system is growing in this digital era. To encourage people to use public transportation, we develop a mobile application through gamification technique to support user involvement on public transportation in Indonesia. The system is called Bandung Smart Transportation Systems (BSTS), and reward system is adopted to give users more benefits. The passengers who want to get benefit they are requested to scan QR code which is generated randomly, so every passenger can contribute to the system. Moreover, we develop an authentication scheme to avoid users' cheat of getting reward. The authentication protocol is developed on the location-based server which handles data request from user/client.

Keywords—authentication, gamification, QR code, transportation, security.

I. INTRODUCTION

In recent years, mobile social networking applications has been developing rapidly, many application provides location service interface for the user [1]. Most of the contents are using gamification techniques that can attract the user's attention. Gamification has raised a lot of interest both in industry [2] and also increasingly in academia [3] [4] [5] during the past few years [6]. An opportunity to develop smart transportation systems with location based service (LBS) in Bandung city to reduce traffic congestion by using gamification techniques. Gamification techniques implemented on public transport features to increase the number of public transport users i.e. bus. The system is named "Bandung Smart Transportation System (BSTS)".

The Concept of gamification on this feature is user can collect reward points every contribute to this system. The benefits of this applications is that user can see the position of multiple entities. Those entities might be friends of a user, public transport, police, ambulance, taxi, etc. While the benefits to the government would be the analysis of traffic density at certain hours, resulting in a system that can predict and anticipate traffic density [7]. One of the most serious security threats to a computing device is unauthorized use [8]. User authentication is the first line of defense againsts this threat [9]. Thus, it requires security techniques to prevent awarding points to users who are not authorized to get the points, or the user does not contribute properly. This study describes the development of the design of a user authentication using QR code. It would prevent malicious users or attackers who may take advantages from the system.

II. RELATED WORK

Authentication research this location has long done. Authentication location is very important to be developed, in order to add the security value of a system, in particular on systems that can be accessed publicly through the Internet. On certain location, there are authentication system which can only be accessed in the specified place. For example, the system on an office is only accessible if the user is inside the office building. Authentication site can also be implemented to check the users access the system if the user resides on other users trusted by the system. At this time, to use authentication this location there are several things to be aware of, such as GPS Accuracy, GPS Position and weather [10]. The author [10] describes the location of the authentication of users by making Location Signature that created by a location signature sensor (LSS) from the microwave signals transmitted by the 24 satellite constellation of the GPS.

The author [11] introduce location-based authentication technique that are especially address to use in buildings and the environment, which is not covered by GPS signal, an active infrastructure is used as a source of position information. The author [1] propose a location authentication scheme based on adjacent nodes, when verifying the authenticity of location provided by a user, some adjacent nodes with higher credits are selected as witnesses. The author [12] presents LINK (Location authentication through Immediate Neighbors Knowledge), a location authentication protocol working independent of wireless carriers, in which nearby users help authenticate each other's location claims using Bluetooth communication.

III. CURRENT WORK

In this section, we describes the current application, named BSTS version 1.0. BSTS Version 1.0 has a feature using the QR Code as a tool for passenger authentication. Bus that want to join the BSTS system must be registered. Registration can be done through an administrator interface by entering driver's data, license plate number, and the bus route. After registration, the bus driver will get a QR Code, and installed on the bus. Any passenger who want to contribute to the BSTS and to get the points, they are requested to scan QR Code through application interface. With the QR Code, information of the bus can be obtained, then user can give bus's rating.

QR code has been used in various applications since the QR code has the large capacity, the small printout size, the high speed scan, the damage resistance and the data robustness [13].

There are many advantages to use the QR code in mobile phones such as omni-direction readability and error correction capability. Therefore, mobile phones adopt the QRcode to support many services such as booking tickets, paying a fee and URL reading [14] [15] [16].

IV. SECURITY REQUIREMENT

In studies using QR Code authentication, there are some security needs to be applied to the system, including:

- **Physical**
QR Code displayed are expected not easily broken and not easy to be stolen by attackers.
- **Duplication**
QR Code displayed are expected not easy to be duplicated by an attacker. Attackers can take the QR code picture and print it easily.
- **Location**
QR Code is used as a means of authenticating a user's location, It is expected that QR Code can be used by users who are at an authorized location. In this feature, the authorized location is in the bus.
- **Usability**

QR Code is used expected to be one-time use, to prevent fake scanning

V. PROPOSED METHOD

In this study, the development of authentication location using QR Code dynamic based on time and location, where B and U moves in the same direction. Implementation of this system, B and U equipped with GPS and the Internet, in this study B and U are assumed to use the smartphone with Android operating system. The function of the GPS is to get the latitude and longitude position of clients that will be used in generating QR Code.

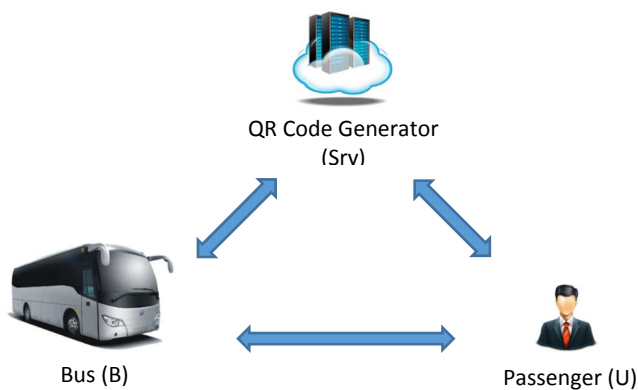


Figure 1. Relation of Entities

Figure 1 illustrates the relationship between the entities. Every entity has a direct relationship. Srv is the center of the relationship B and U, Srv is a media provider of B and U as well

as data storage of B and U. There are several entities that are used in this study:

Table 1. Notation

Notation	Description
<i>Srv (Server)</i>	The server part consists of an API (Application Programming Interface) is used for data processing. Programming language for this API is PHP.
<i>DB (Database)</i>	The database is data storage. This study uses MySQL as a database server.
<i>B</i>	Applications that will display the QR Code.
<i>U</i>	Applications used by the user to scan the QR Code / authentication location.

This research will be applied in public transport feature in the BSTS application. Therefore, it is assumed the B is Bus, and U is a passenger.

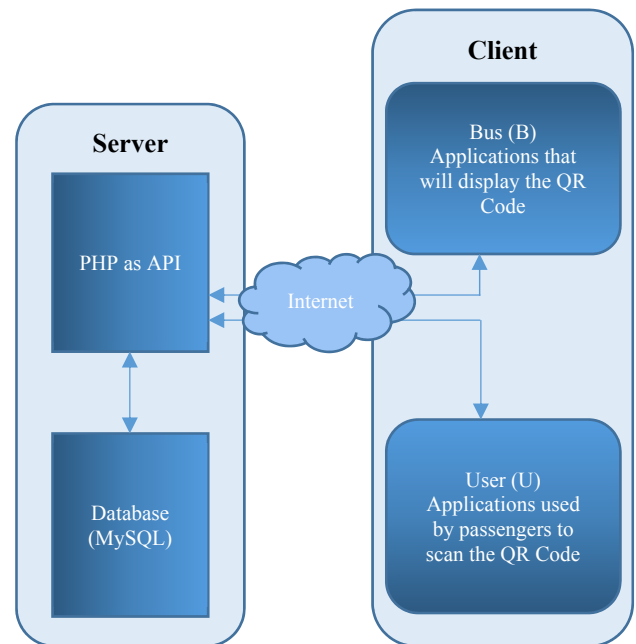


Figure 2. Hierarchy of Systems

Figure 2 illustrates the relationship between the server and the client. B and U are part of the client and on the server side there is a database that will store the data used in the system. API is part of the server which serves to connect the client to the server to receive, process and provide the data via Internet. Figure 3 illustrates the overall system. Among them:

1. B sends a bus id and the current position to Srv.

$B \rightarrow Srv : (Bus\ ID, Latitude, Longitude)$

2. Srv generates the encryption of the bus, the current position (latitude and longitude) and the current time, then send back to B.
Bus information :
 - ID
 - Bus ID
 - Latitude
 - Longitude
 - Timestamp

Srv → B: E(json(Bus Information))

3. After receiving the encrypted data from Srv, and B generate a QR Code image with data from Srv.
4. U who wants to contribute to the system is required to scan the QR code displayed by B.

B → U : Value of the QR Code

5. Results of scanning the QR code will be sent to Srv to be authenticated.

U → Srv : Result of Scanning QR Code

6. Srv will authenticate user with compare between result of scanning QR Code and data from database.
7. U gets reward points and allowed to give an assessment of the bus if the response from Srv is accepted. Otherwise, U is denied to access the page assessment of the bus.

Srv → U : Authentication Result

VI. DISCUSSION

In this section, we discuss about the security and performance of this systems.

• SECURITY ANALYSIS

In this section, we describe about security analysis, we compare between previous version and this version.

Table 2. Comparison Version

Variable	Previus Version	This Version
QR Code easy to be broken	Yes	No
QR Code easy to stolen	Yes	No
QR Code easy to duplicated	Yes	No

Table 2 we compare this version uses a dynamic QR Code with previous version uses a static QR Code. Every U makes an authentication on the B, U should scan the QR Code. After U is successfully authenticated, the QR Code is considered to be expired or has been used by Srv. QR Code is considered to have been used by fill in the value of the “User ID” that is on the database QR Code, thus if the QR Code is taken or recorded, the attacker would not be able to authenticate by the QR Code is repeatedly. Figure 4 describes about previous versions, the QR code displayed using the stickers are very easy to steal. QR Code can be taken and printed by the attacker, thus the attacker

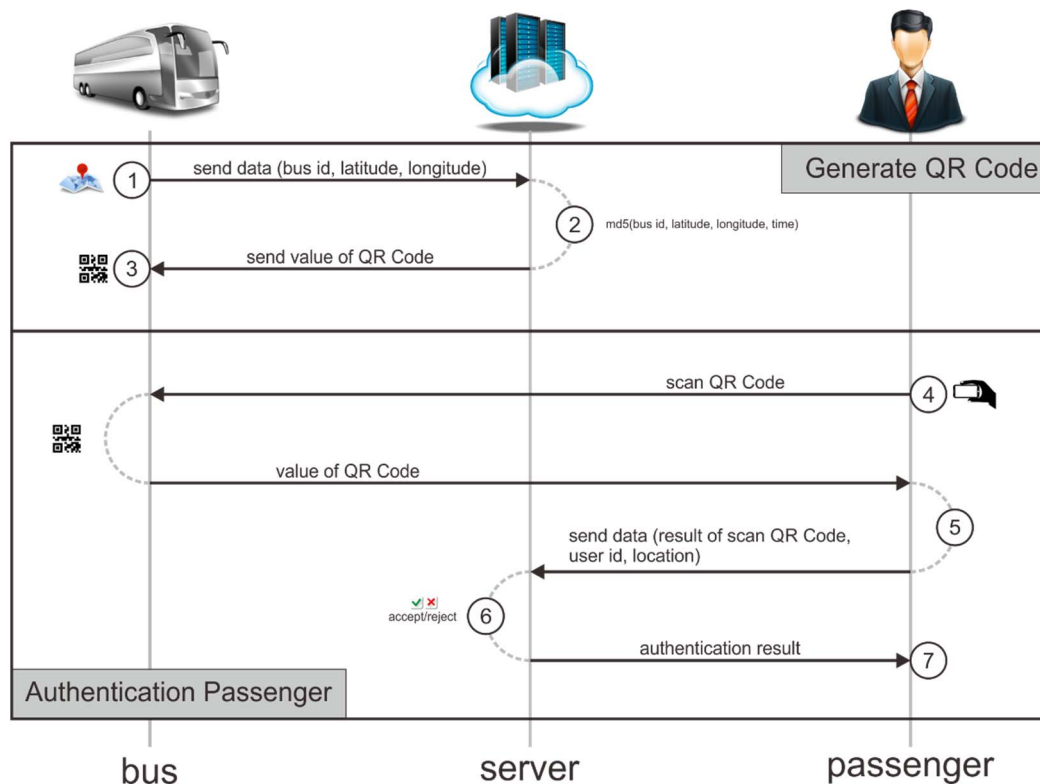


Figure 3. Overall System

will easily earn points by doing a scan of a QR Code anywhere and anytime.

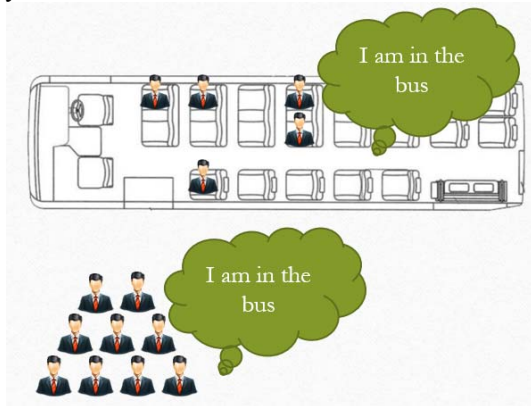


Figure 4. Analyze for Current System

Figure 5 describes the enhancement of the security of the system. By implementing this system, only the passengers of a bus that can be authenticated and gives an assessment of the bus, therefore the system can give points to users who had been a passenger on the bus.

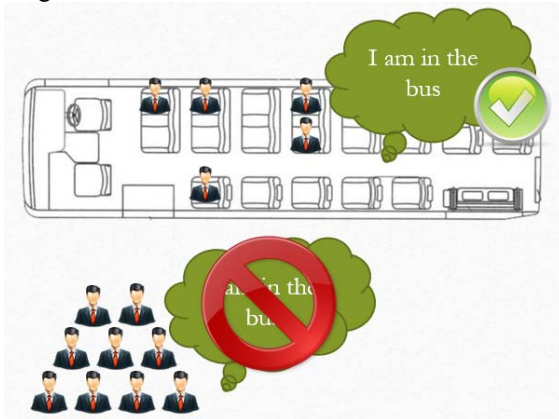


Figure 5. Analyze for New System

- **PERFORMANCE**

In this section, we describe about performance of server to authenticate and provide data to clients.

Many factors affect communication between server and client over internet network, such as : speed, traffic, bandwidth, etc. The graph shows the performance of the server to perform QR Code Generation and authentication. This data is taken by simulation, with a sample of the data 1 to 500 buses accessing the server at the same time to generate a QR Code, after that server receive authentication request from passenger. The graph (Figure 6) illustrates, the server will take a long time to handle a lot of clients.

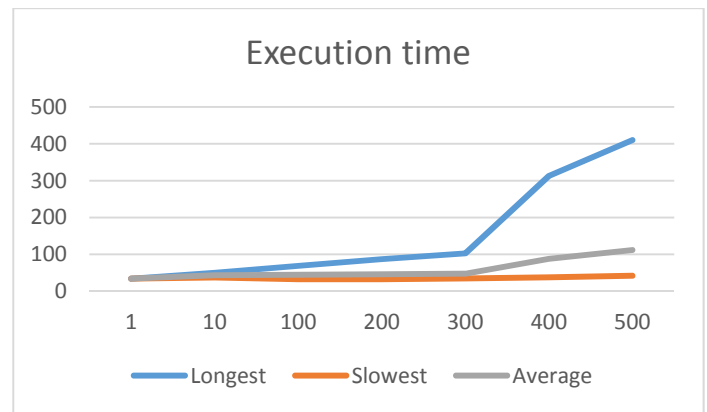


Figure 6. Graph of execution time for QR Code generation and authentication passenger

VII. CONCLUSION & FUTURE WORK

Design of this system based on current environment in Bandung City, and adopt gamification technique to improve number of users the public transport to reduce traffic density. Authentication techniques are needed for security system. Authentication can be a user authentication, authentication location, and other authentications. In the developed transportation system is needed authentication location of user to prevent fake passenger. Using dynamic QR Code which is made changeable based on the location and the current time, can be prevented from damage and theft of a QR Code which is as identity and authentication tools to users in the bus.

Improvement of the system, is expected to feature public transport is to function properly and appropriately on purpose, so as to provide rewards to users who actually use public transport. On experiments with a user authentication process takes 33.9875 ms, when there are 10 processes user authentication simultaneously, each process has a different process time, the fastest is 37.0238 ms, and the longest is 50.113 ms, and the average time is 43.06447 ms. Compared with the single authentication process time, the authentication processing time has increased 126.71%. The data obtained indicate weakness servers when there are many authentication requests. For future research, this feature could be developed on the techniques of encryption and authentication schemes on the QR Code. For future research, this feature will apply "Distributed Database Systems" to solve the problem traffic data on the server.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2014R1A2A1A11052981).

REFERENCES

- [1] L. Hua and J. Dai, "A location authentication scheme based on adjacent users," in Progress in Informatics and Computing (PIC), 2014 International Conference on, 2014.
- [2] G. W. Architects, Putting the Fun in Functional - applying game mechanics to functional software, 2009.
- [3] S. Deterding, D. Dixon, R. Khaled and L. Nacke, From game design elements to gamefulness: defining gamification, ACM, 2011.
- [4] J. McGonigal, Reality is broken: Why games make us better and how they can change the world, Penguin, 2011.
- [5] I. Bogost, Persuasive games: The expressive power of videogames, Mit Press, 2007.
- [6] K. Huotari and J. Hamari, "Defining Gamification - A Service Marketing Perspective," in ACM, 2012.
- [7] R. Aulya and K.-H. Rhee, "Location Based-Services Over Gamification Approach," in Korea Multimedia Society, Andong, 2015.
- [8] B. A. Tama and K. -H. Rhee, "Performance Analysis of Multiple Classifier System in DoS Attack Detection," in International Workshop on Information Security Applications, pp. 339-347, 2015.
- [9] W. Jansen and V. Korolev, "A location-based mechanism for mobile device security," Computer Science and Information Engineering, 2009 WRI World Congress on, vol. 1, pp. 99-104, 2009.
- [10] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," Computer Fraud & Security, no. 2, pp. 12-16, 1996.
- [11] D. Jaros, R. Kuchta and R. Vrba, The Sixth International Conference on Internet and Web Applications and Services (ICIW 2011), vol. 6, pp. 20-25, 2011.
- [12] M. Talasila, R. Curtmola and C. Borcea, "Collaborative Bluetooth-based location authentication on smart phone," Pervasive and Mobile Computing, vol. 17, pp. 43-62, 2015.
- [13] DENSO WAVE INCORPORATED, [Online]. Available: <http://www.qrcode.com/en/>.
- [14] T. S. Parikh and E. D. Lazowska, "Designing an architecture for delivering mobile information services to the rural developing world," in Proceedings of the 15th international conference on World Wide Web, 2006.
- [15] J. Rekimoto and M. Saitoh, "A Spatially Continuous Workspace for Hybrid Computing Environment," in Proceedings of CHI'99, 1999.
- [16] G. Yu, Z. Wang, L. Yi and L. He, "An application and implementation of two-dimensional symbols for circuit board quality control system," in Industrial Informatics, 2004. INDIN'04. 2004 2nd IEEE International Conference on, 2004.