Thesis for the Degree of Master of Engineering

Design of Dynamic QR Code for Authenticated Passengers on Bandung Smart Transportation Systems

by

Rafinno Aulya

Interdiciplinary Program of Information Systems
Pukyong National University

February 2016

Design of Dynamic QR Code for Authenticated Passengers on Bandung Smart Transportation Systems

(반둥 스마트 교통 시스템에서 승객 인증을 위한 동적 QR 코드 설계)

Advisor: Prof. Kyung-Hyune Rhee

by

Rafinno Aulya

A thesis submitted in partial fulfillment of the requirements
for the degree of

Master of Engineering

in Interdiciplinary Program of Information Systems
The Graduate School,
Pukyong National University
February 2016

Design of Dynamic QR Code for Authenticated Passengers on Bandung Smart Transportation Systems

A thesis

by

Rafinno Aulya

Approved by:

_____

(Chairman) **Man-Gon Park**

_____

(Member) **Hilwadi Hindersah**

_____

(Member) **Kyung-Hyune Rhee**

26 February 2016

Table of Contents

List of Figures

List of Tables

List of Pseudocodes

반둥 스마트 교통 시스템에서 승객 인증을 위한 동적 QR 코드 설계

라핀노 아울리야

부경대학교 대학원 정보시스템협동과정

요 약

반둥 스마트 교통 시스템(Bandung Smart Transportation System, BSTS)은 인도네시아 반둥시의 일부 교통 문제를 해결하기 위해 개발 된 시스템이다. 사용자들은 BSTS 가 제공하는 스마트폰 어플리케이션을 이용하여 교통시스템을 사용할 수 있으며, 게임화(gamification)된 형식으로 사용자의 활용도나 기여도에 따라 보상을 제공할 수 있다. BSTS 어플리케이션의 핵심 기능 중 하나는 대중교통 기능으로, 사용자들은 대중교통 환경의 개선을 위한 평가 및 조언을 제공하고 이에 대한 보상을 받을 수 있다. 이때, 사용자의 대중교통 이용 평가에 대한 신뢰성 보장을 위한 방안이 필요하며, 본 논문은 대중교통을 이용하는 사용자의 위치를 버스에 설치된 QR 코드를 통해 인증함으로써 어떤 사용자가 실제로 해당 교통시스템을 이용했는지 여부를 검사하기 위한 시스템을 개발한다. 종이 또는 스티커 형태로 부착되는 QR 코드는 쉽게 손상되거나 정적인 특성으로 인해 악의적인 목적으로 중복 사용될 수 있으므로 본 논문에서는 동적으로 매번 갱신되는 QR 코드를 버스 내부에 설치된 스크린에 나타내도록 구현하였다. 동적 QR 코드는 버스의 이동 위치에 따라 주기적으로 갱신되고 일시적으로 사용되므로 중복된 QR 코드가 사용될 가능성을 줄일 수 있다. 또한 제안 시스템은 사용자 위치 인증 기법과 결합하여 동적 QR 코드의 기능성을 향상 시킬 수도 있다.

키워드 : 인증, 게임 화, QR 코드, 교통, 보안

Chapter 1. Introduction

1.1 Background

In recent years, mobile social networking applications has been developing rapidly, many application provides location service interface for the user [1]. Transportation planning has been done by the government to overcome traffic congestion problem in the city. Public transportation is one of the alternative to reduce traffic congestion, because it maximizes the number of passengers in a vehicle with the same destination. For example if there are eight people departing from point A to point B at the same time with each car, there will be eight cars moving from point A to point B at the same time. With the public transportation, eight people can use one vehicle only, thereby reducing a moving vehicle at the same time. Most public transportation in Indonesia are owned by a private company. Declining interest of people to use public transport becomes a major problem of transportation. Many people choose to use a private vehicle, and it is one of the causes of traffic congestion. There are many factors

that affect people less interested in using public transport, some of these factors will be discussed in the next chapter. The development of technology has now covered almost all daily activities. Especially smartphone,now is not a luxury product in the society. Almost everyone can have and enjoy the sophistication of smartphone technology. Many developers develop and publish applications in the application market for free or paid to be preferred by many users. Present has many smartphone users who download the application in the app market. With the occasion can be used to make the system a content that is useful to the general public.

The traffic system is becoming quite complicated due to the increasing of roads and vehicles. Many countries realized Intelligent Transport Systems to make better use of existing transport resources. As Intelligent Transport Systems has mass traffic information data, it is a worthy study problem that how to make efficient use of these data. Because vehicles, the Individual of the Intelligent Transport System, have characteristics such as needing personalized information, mobile, huge number which make it difficult to publish information to those potential users [2]. It makes an opportunity to create an intelligent transportation system using Location

Based Service (LBS). The system uses applications on mobile devices. In the first version it only covers Bandung City and available on the Android Operating System (OS). The system is named Bandung Smart Transportation System (BSTS). The application consists of several features associated with transportation in the city of Bandung. The feature was developed with the concept of gamification, which the user can collect reward points every contribute to this system. The benefits of this applications is that user can see the position of multiple enitities. 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 [3]. One of the most serious security threats to a computing device is unauthorized use. User authentication is the first line of defense againts this threat [4]. 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.

1.2 Objective

The general objective of this study is to apply security techniques to authenticate the location in the BSTS system. The specific objectives of this study are:

- Improve QR Code authentication scheme in existing system.
- Design authentication scheme using QR Code.
- Design authentication scheme for two different mobile devices are adjacent.
- Analyzing the ability of the system to authenticate the user.

1.3 Scope

The scope of this study is to design a scheme to authenticate the location of the user using the QR Code. This study discusses:

- QR Code displayed on the device that is being moved.
- How to get the latest position of the QR Code and users periodically

- How the value of the QR Code is can be generated.
- How the system can authenticate the user's location adjacent to the QR Code, where users and QR Code on the move.

1.4 Outline

The thesis has been divided into five chapters which are:

Chapter I, Introduction

Introduction consists of thesis background, problem statement, thesis objective, scope, and thesis outline.

Chapter 2, Literature Reviews

Literature reviews explains the theoretical supports and methods. It includes explanation about authentication location

Chapter 3, System Requirements and Design

Chapter 4, System Implementation for authentication of passenger

System Implementation contains the process of development using , Web service Programming, and smartphone application programming. It is also consists of the overall architecture of the system and database schema.

Chapter 5, Conclusion

Chapter 2. Literature Reviews

2.1 Preliminary Study

2.1.1 Transportation System

In Indonesia, the busway can only be found in some large city. Public transport in Indonesia there were using buses and most use the minibus, the so-called "Angkot". "Angkot" is an acronym for "Angkutan Kota" which means the city transportation. "Angkot" can stop and wait for passengers anywhere.

Some factors that could make a lack of public interest to use public transportation in Indonesia, among others :

- Schedule and Traveling Time

  The uncertainty of the arrival of public transport in the city makes people prefer to use their own vehicles. As a result, people can not predict their travel time when they go somewhere. There is a popular term when public transport is waiting for passengers,

namely "ngetem". “Ngetem” is public transportation stops for wait passangers for a long time.

- Tariff

  In Indonesia tariff of public transport is regulated by the organization under the department of transportation. There are three types of fare i.e. long-distance, short distance, and children. Long distance rates apply when passengers use public transport as far as more than half the distance of the route. Whilst short distance rates apply when passengers use public transport as far as less than half the distance of the route. Student rate is the rate that applies to children from elementary school to high school. The tariffs are informed in every public transport unit with a sticker attached to the info fare.

  With the long-distance rates and the rates at close range to make public transport fares do not have a clear benchmark. Some public transport drivers take high tariffs if passengers like not knowing tariffs, for example tourists or taking long distance rates when passengers only a distance close.

- Cleanliness

  Cleanness includes the conditions in public transport, for example seat, trash. It affects the level of public interest to use public transport.

- Convenience

  The convenience is one of the factors that affect the level of public interest to use public transport. Driving style of the driver is one that affects comfort. Sometimes a driver driving a vehicle very fast and make passengers fear, or also drivers drives too slow to make the passengers too long to arrive at the destination.

2.1.2 Current System

BSTS has developed an application called "Semut". The application is a social media-based applications. The application is also an application-based geolocation. The application can be found in Google Play : *https://play.google.com/store/apps/details?id=com.app.semut&hl=en*.

On the application, there are several features that are being developed, among them:

1. Profile Feature

   Every users who have registered will have a profile account. Accounts that profile consists of:

   a. Personal Data

      Personal data consists of name, address, date of birth, telephone number, and gender.

   b. Username and password

      Username and password are used to login to the application. Users can change and reset the password if the user forgets the password.

   c. Avatar

      Avatar is an icon that is used or displayed on the map as a marker. Avatars can be changed as the user desires. There are two kinds of avatars if the user wants to replace, there are free and paid.

2. Poin Rewards

   Every user contribute to this system will get points. In the current version, the accumulation of the points can be used to replace

avatar. In the future, there are will be a lot of awards that may be granted to the active users of the application i.e. by having *n*-points, users will get a free one-way use public transport.

3. Global Position Feature

   If the user has been logged-in on the application, application records the position of the user, and the data is sent to the server location. The data of the location of the user is used to calculate and to display the traffic density, assuming the majority of the people of Bandung use the application.

4. Map Feature

   The application comes with a map on the main page. On this map the user can see the position of other users. Marker of users will appear on the map based on the settings of the user account, this is to maintain the confidentiality of the user position.

5. Relation Feature

   This feature is commonly known as the friendship features on social media-based applications. Users can make friends with other users on the system by adding as a friend.

6. Group Feature

   After the user make friends with other users, users can create group.

7. Navigation Feature

   Users can create travel route with this application. Users simply specify the point of origin and point of destination, the system will provide the best path that can be used by users.

8. Taxi Feature

   Users can order a taxi and they can see the status of booking a taxi with this feature. Only registered taxi which can be used by the application. The taxi driver registers the taxi unit to the system, and the taxi driver uses the application to view and accept requests.

9. Public Transportation Feature

   In this study, we focus on this feature. Actually, this system will be implemented on "angkot", but to simplify the next be called a bus. In the current version, a bus that will contribute to this system must register first. The system requires data such as route, driver's name and license plate number. After registration, the system

generates a QR Code for the bus units and it is installed at the entrance of the bus. Users who want to contribute to provide an assessment to the bus must scan the QR Code, thus the applications used will know the details of the bus. After scanning the QR code, the user can make an assessment of the bus that is being used. By contributing to this system in providing an assessment of the bus, the user is given the points.

2.2 Mobile Platform

The operating system is software that is critical of a computer system, with this operating system the user can run an application program on a hardware device, such as smartphones. Currently there are several platforms for mobile devices are widely used such as Android, iOS, Windows Phone, etc.

- Android

  Android is a software stack for mobile devices that includes an operating system, middleware and key applications [5]. Android platform is the platform that currently dominate the market of

mobile devices, it takes almost 50% share of worldwide smartphone market [6]. Platform Android is an operating system based on Linux and open source. There are many applications available for this platform, and to develop the application, there are several IDEs such as Android Studio, and Eclipse.

- iOS

  iOS is the operating system developed and distributed by Apple. iOS operating system can only be found on devices manufactured by Apple. iOS becomes second largest smartphone platform [6].

- Windows Phone

  Windows Phone is an operating system developed by Microsoft, and is distributed through third parties.

- Others.

  There are several other operating systems, such as: Blackberry, Tizen, etc.

At the present time, the smartphone has generally been supported by multiple sensors such as a light sensor, a pressure sensor, a GPS (Global Positioning Service) that can be used to retrieve position data based on

altitude, latitude and longitude, and other advanced features. These devices can be used to develop a system to get a lot of contributions from users. For example with these devices can be used in transportation systems, tracking the position of the user and can produce data traffic density.

2.3 Gamification

Gamification has raised a lot of interest both in industry [7] and also increasingly in academia [8] [9] [10] during the past few years [11]. For example, the success of mobile services such as Foursquare and Nike+ are often attributed to gamification [8].

Gamification is not always related to the game. Gamification is a technique to increase the interest of users to use the provide application. If no gamification in an application, the user may feel bored or may not be interested to the application. Examples of gamification on an application or a system such as posting status on Facebook, users can like and comment on a post other users. This can increase the interest of users to

post a status, to get "likes" from other users, as well as other users are able to comment on the status.

2.4 QR Code

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 [12]. 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 [13] [14] [15].

QR code is a type of matrix codes or two-dimensional bar code developed by Denso Wave, a division of Denso Corporation is a Japanese company and published in 1994 with the main functionality is can be easily read by the scanner QR is short for quick response or a quick response, their purpose is to deliver information quickly and get a quick response. Unlike the bar code, which only store information horizontally, QR codes can

store information horizontally and vertically, and therefore QR code holds more information than a barcode.

QR code functions like a physical hyperlinks that can store addresses and URLs, phone numbers, text, and text that can be used in magazines, daily mail, advertising, on signs buses, business cards or other media. In other words as a liaison quickly content online and offline content. The presence of this code allows the user to interact with media attached to phone effectively and efficiently. Users can also generate and print their own QR codes for others by visiting one of several encyclopedias of QR code.

QR codes have a high capacity in a data encoding that capable of storing all types of data, such as numerical data, the data is alphabetical, kanji, kana, hiragana, symbols and binary code. Specifically, the QR code is capable of storing the data of up to 7,089 types of numeric characters, alphanumeric data of up to 4,296 characters, the binary code of up to 2,844 bytes, and kanji up to 1,817 characters [16]. Besides the QR code has a smaller screen than the barcode. This is because the QR code can accommodate the data horizontally and vertically, and therefore

automatically zoom the image size of the QR code can be only one-tenth of the size of a bar code. Not only that, the QR code is also resistant to damage, because the QR code is able to correct errors up to 30%. Therefore, although some symbols of the QR code is dirty or damaged, the data can still be stored and read. Three square-shaped marks in three corners has a function so that the symbols can be read with the same results from any angle throughout 360 degrees.

2.5 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 [17].

The author [17] 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 [18] 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 [19] 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.

2.6 Encryption Technique

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizeble by its attackers while stored and transmitted [20]. Due to the encryption was used to secure communications in various countries, only certain organizations and individuals who have an interest in very urgent confidentiality using encryption. In the mid-1970s, strong encryption is used for security by the secretariat of the United States government agencies in the public domain, and is currently on the system encryption has been used widely such as Internet e-commerce, mobile phone network and the bank's ATM. In this paper, we use MD5 algorithm for data encryption. MD5 algorithm is an authentication method used in a broad research field. The data encryption techniques are summarized in this paper. On the basis of anatomy of MD5 algorithm, combining of DES encryption algorithm, introducing time countermark and restricting of IP address, the method of one password at a time based on MD5 algorithm is used to give a security implementation of user password encryption [21].

2.7 Web Service

Web service is a software application or a piece of software that can be accessed remotely by various devices with a particular intermediary. In general, the web service can be identified by using such URL in a regular Web. But the difference the web service with general web is the interaction of a web service. Unlike the general web URL, the URL of the web service only contains a collection of information, commands, configurations or useful syntax construct a certain functions of the application. Web service composition lets developers create applications on top of service-oriented computing's native description, discovery, and communication capabilities [22].

Web services can be interpreted also a method of data exchange, regardless of database location and platforms used to process the data. Web service is capable support interoperability. Thus the web service is able to be a bridge to the various existing systems.

General web used to perform the response and requests made between the client and the server. For example, a particular web service users typing

the URL address of the web to make a request. Request will be up on the server, processed and then presented in a response. Thus there was a simple client-server communication.

On the web service, the relationship between the client and the server does not occur directly. The relationship between client and server is bridged by the web service file in a certain format. Thus access to the database will not be directly handled by the server, but through an intermediary known as a web service. The function of this web service facilitates the distribution and integration of databases to multiple servers.

2.7.1 XAMPP

XAMPP is a open source software, which supports many operating systems, is a compilation of some programs. The function is as a standalone server (localhost), which consists of a program the Apache HTTP Server, MySQL database, and translator written in the programming language PHP and Perl. XAMPP name is an acronym of X (four system), Apache, MySQL, PHP and Perl. The program is available inside the GNU General Public License and is free. XAMPP is a simple

web server, and can be used to serve dynamic web page display. To get XAMPP user can download directly from its official website. XAMPP is developed from a project called Apache Friends team, which consisted of a Core Team, the Development Team and Support Team.

2.7.2 Apache

Apache HTTP Server or Server Web / WWW Apache is a web server that can be run on many operating systems such as Unix, BSD, Linux, Microsoft Windows and Novell Netware and other platforms, which is useful to serve and the enable the the website. The protocol used for serving web www using HTTP. Apache has advanced features such as error messages that can be configured, authentication based on database and others. Apache is also supported by a number of graphical user interface (GUI) that allows the server handling becomes easy. Apache is an open source software developed by an open community comprised of developers under the Apache Software Foundation. Apache is an open source software for web server creation, deployment and management. Apache is one of the most commonly used applications for website hosting [23]. Apache is designed to create web servers which have the ability to

host one or more HTTP-based websites. Notable features include the ability to support multiple programming languages, server side scripting, an authentication mechanism and database support [24]. Apache can be extended via modules to add new useful functions such as `mod_rewrite`, which enables redirecting to control the visitor's options and shape traffic on the website. By using `mod_rewrite`, user can adjust the settings of the website traffic by editing the `httpd-xampp.conf` file which redirects all folder required to use in HTTPS connection [23].

2.7.3 PHP

PHP is an extension of Hypertext Preprocessor, PHP or Hypertext Preprocessor is a programming language in the form of code or script that can be added to the HTML programming language, PHP is also often used for the design, create and program a website. PHP can also be used to make the API (Application Programming Interface) that connect the mobile device to the server application.

2.7.4 My SQL

MySQL is an implementation of relational database management system (RDBMS) that is distributed for free under the GPL (General Public License). Every user can use MySQL for free, but with restrictions such software should not be used as a commercial product. MySQL is actually a derivative of one of the main concepts in the database that have been there before; SQL (Structured Query Language). SQL is a database operation concept, such as CRUD (Create, Read, Update, and Delete) which allows the operation of data is done with ease. The reliability of a database system (DBMS) can be known of how the optimizer in the process of SQL commands created by the user or other application programs. MySQL support database transactional operations and database non-transactional operations. In the non-transactional mode of operation, MySQL has good performance compared to other database providers. However, the non-transactional mode there is no guarantee of the reliability of the stored data, therefore non-transactional mode is only suitable for the type of applications that do not require reliability of data such as web-based blogging application i.e. wordpress, Content

Management System (CMS), and others. For business purpose is advisable to use a transactional database mode, only as a consequence the performance of MySQL in transactional mode is not as fast as the performance of the non-transactional mode.

2.7.5 JSON (JavaScript Object Notation)

JSON is a data exchange format on the computer. The format is text-based and human-readable and is used for representing simple data structures and associative arrays (called objects). JSON format is often used to transmit structured data through a network connection in a process called serialization. The main application is in the AJAX web application programming to serve as an alternative to the traditional use XML format.

Chapter 3. System Requirement and Design of Systems

3.1 Security Requirements

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

- Pysical

  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.

3.2 Entities of Systems

There are several entities that are used in this study.

Table 1. Notation

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

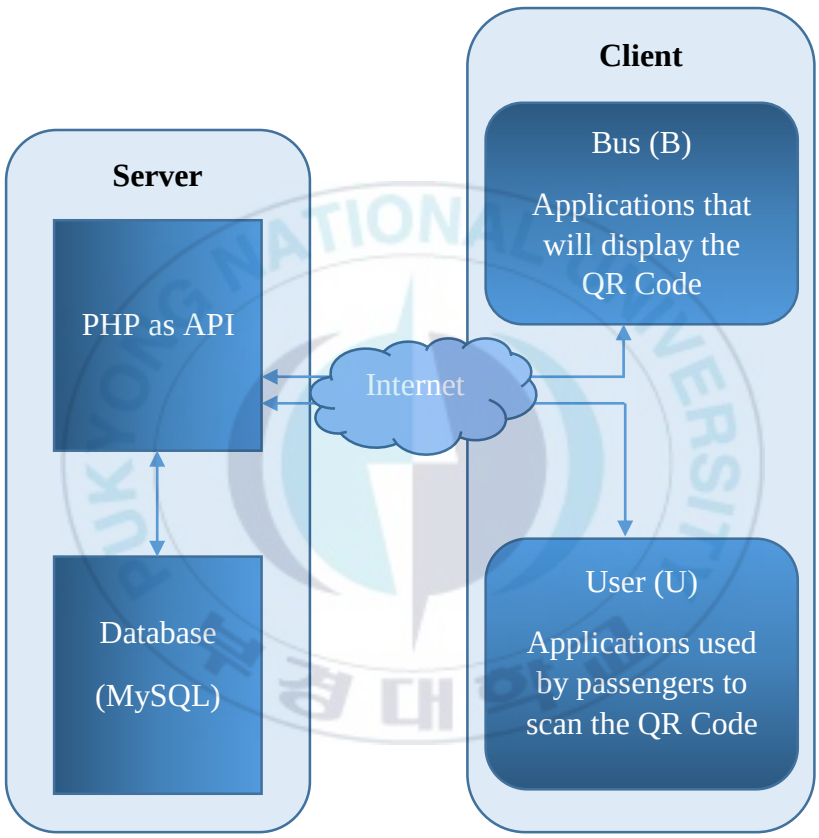


Figure 1. Hierarchy of Systems

Figure 1 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.

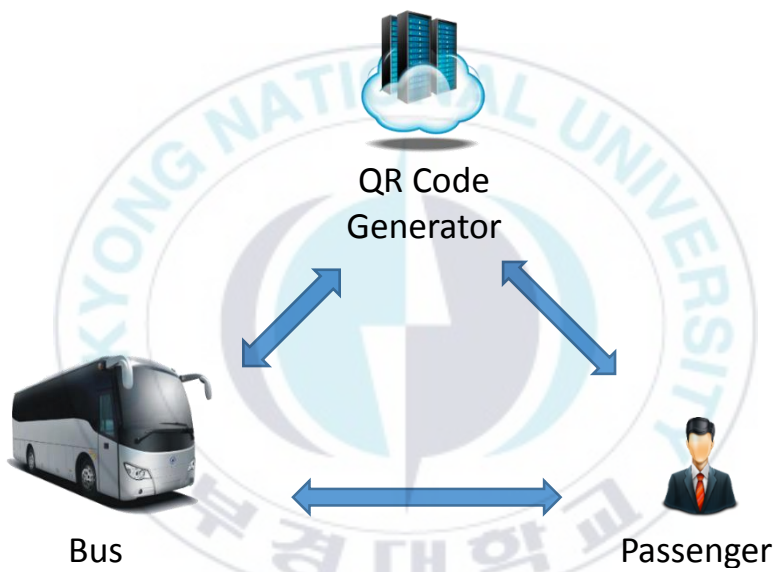


Figure 2. Relation of Entites

Figure 2 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.

3.3 Design of Authentication

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.

3.3.1 Overall System

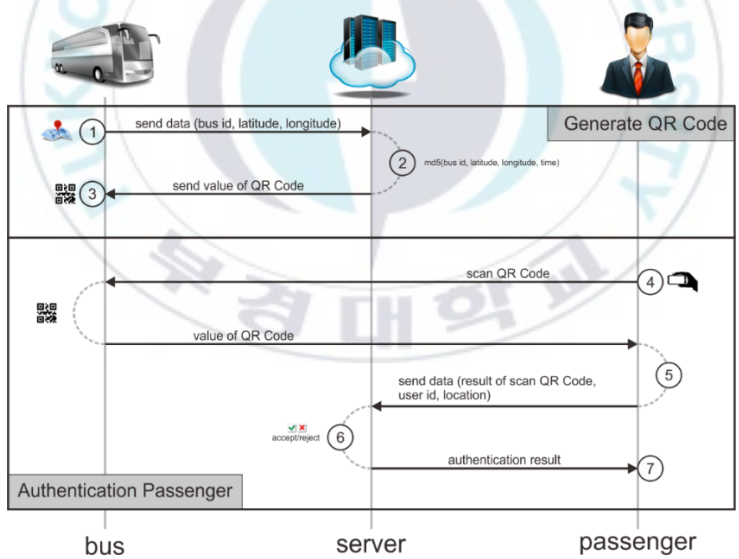


Figure 3. Overall System

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.

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

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.

$$B \rightarrow U: Value\ of\ the\ QR\ Code$$

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

$$U \rightarrow Srv: Result\ of\ Scanning\ QR\ Code$$

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.

$$Srv \rightarrow U : Authentication\ Result$$

3.3.2 Design of Database (DB)

In this study, the value of QR Code generated by Srv will be stored in the database. Table 2 is a database structure.

Table 2. QR Code Table in Database

Name	**Type**	**Description**
ID	Integer	ID of QR Code
UserID	Integer	Id of the user who scan the QR Code
BusUnitID	Integer	Id of the bus that displays the QR Code
Latitude	Double	Latitude position of the bus that displays this QR Code
Longitude	Double	Longitude position of the bus that displays this QR Code
Timestamp	Datetime	The time when the making this Code QR
Encryption	Text	E (JSON (ID, BusUnitID, Latitude, Longitude, and Timestamp))

3.3.3 Generate QR Code Process

Bus Application (B)

```
Params = (BusUnitID, Latitude, Longitude)
Send(Srv, Params)
Receive(Srv, ValueQRCode)
GenerateQRCode(ValueQRCode)
Show QR Code
```

Server (API for generate QR Code)

```
Receive(U, Params)
BusUnitID = Params[BusUnitID]
Latitude = Params[Latitude]
Longitude = Params[Longitude]

ArrayQRCode[BusUnitID] = BusUnitID
ArrayQRCode[Latitude] = Latitude
ArrayQRCode[Longitude] = Longitude
ArrayQRCode[Datetime] = DateNow("yyyy-MM-dd
HH:mm:ss")
TextQRCode = JSON_ENCODE(ArrayQRCode)
ValueQRCode = Encryption(md5, TextQRCode)

IsInsertNewQRCode = TRUE
PreviousQRCode = ReadDatabase("Select * `tb_qrcode`
WHERE `BusUnitID` = 'BusUnitID'")
if LastQRCode != NULL AND PreviousQRCode[UserID] ==
0, then
      IsInsertNewQRCode = FALSE
endIf

if IsInsertNewQRCode = TRUE, then
      QRCode[ID] = NULL
      QRCode[UserID] = 0
      QRCode[BusUnitID] = BusUnitID
      QRCode[Latitude] = Latitude
      QRCode[Longitude] = Longitude
```

```
      QRCode[Timestamp] = DateNow("yyyy-MM-dd
      HH:mm:ss")
      QRCode[Encryption] = ValueQRCode
      InsertDatabase(QRCode)
else
      QRCode = PreviousQRCode
      IntervalTimeInMinutes = DateNow -
LastQRCode[Timestamp]
      if IntervalTimeInMinutes < 1 minutes, then
            QRCode[Latitude] = Latitude
            QRCode[Longitude] = Longitude
            QRCode[Timestamp] = DateNow("yyyy-MM-dd
HH:mm:ss")
            QRCode[Encryption] = ValueQRCode
            UpdateDatabase(QRCode, "Update
`tb_qrcode` WHERE `ID`='QRCode[ID]'")
      else
            ValueQRCode = QRCode[Encryption]
      EndIf
EndIf
Send(B, ValueQRCode)
```

Pseudocode 1. Algorithms for Generate QR Code

Pseudocode 1 illustrates the algorithm for generating QR Code.

3.3.4 Authentication Process

Pseudocode 2 illustrates the algorithm to authenticate the results of scanning the QR Code.

```
User Application (U)

ScanResult = result of scan QR Code
Params = (UserID , Scan)
Send(Srv, Params)
Receive(Srv, AuthenticationResult)
```

```
If AuthenticationResult = ACCEPTED, then
      Go to next Page
else
      ShowMessage("Authentication is rejected")
endif

Server (API for authentication)

Receive(U, Params)
ScanResult = Params[ScanResult]
UserID = Params[UserID]

QRCode = ReadDatabase("Select * `tb_qrcode` WHERE
`Encryption` = 'ScanResult' AND `UserID` = '0'")

if QRCode != NULL, then
      QRCode[UserID] = UserID;
      UpdateDatabase(QRCode, "Update * `tb_qrcode`
WHERE `ID`='QRCode[ID]'")
      Send(U, ACCEPTED)
else
      Send(U, REJECTED)
endIf
```

Pseudocode 2. Algorithms for Authentication

3.4 Scenario of Public Transportation Features

Authentication using the QR Code will be implemented on public transport features in the BSTS Application. The purpose of the feature is to facilitate passenger to contribute an assessment of the bus used. The expectations of the assessment is that providers can improve their service

for passengers. Users who are on the bus is authorized user, and their can give the assessment. Otherwise, users who are not on the bus or users who are not passengers are not allowed to give an assessment.

This study is the development of one of the features that already exist on the BSTS application. Users can gives an assessment of the bus that was used by scan the QR code displayed on the bus. QR Code development is not shown by sticker paper, but using a screen that is attached in side the bus.

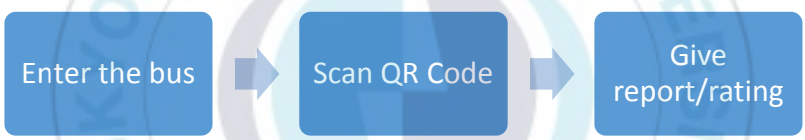


Figure 4. Scheme of Public Transportation Feature

Passenger can give assessment to bus who have registered on the BSTS System. Users will get points if the user uses the bus since scanning QR Code is required and give an assessment of the bus, because the user is considered to contribute to the BSTS System. The points can be collected and redeemed for prizes such as free tickets, shopping voucher, etc.

Chapter 4. System Implementation and Analysis

4.1 Simulation Setup

The simulation consists of three entities, namely: buses, passenger and server. To perform the simulation, we create 2000 users as the dummy data (1000 users as passengers and 1000 users as buses).

4.2 Simulation Result

4.2.1 Analysis Server

The results of the simulation is to analyze the speed of the server to serve a request for generate QR Code and QR Code authentication.

Table 3. Execution time for authentication

Number of Buses (unit)	Longest (ms)	Shortest (ms)	Average (ms)
1	33.9875	33.9875	33.9875
10	50.113	37.0238	43.06447
100	69.0481	32.5219	44.64067
200	87.0573	32.5219	46.06904
300	102.5682	34.5227	47.77344
400	312.7061	37.5244	87.90711
500	410.2716	42.0309	111.9492

Table 3 illustrates the execution time Srv for authentication of the U.

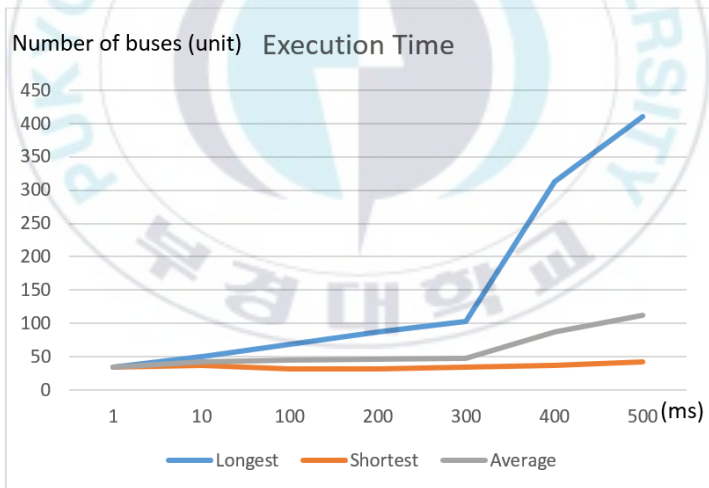


Figure 5. The graph of the average of execution time for authentication one passenger

Figure 5 depicts a graph of the execution time Srv to generate a QR Code and authentication for one user. 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 illustrates the server will take a long time to handle a lot of clients.

4.2.2 Analysis System

Table 4. Comparison Version

Variable	Previuos 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 4 we compare this version uses a dynamic QR Code with previous version uses a static QR Code. Every U makes a 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.

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

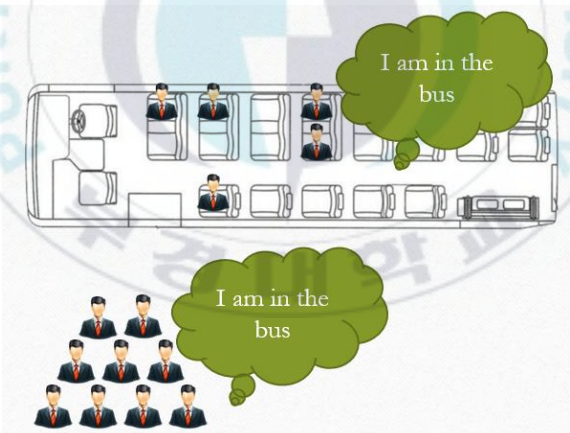


Figure 6. Analyze for Current System

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 gives points to users who had been a passenger on the bus.

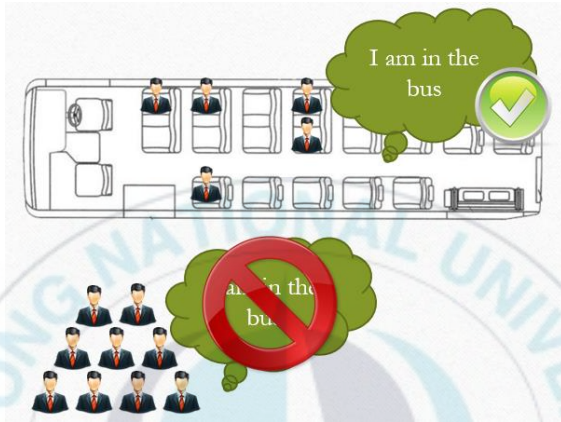


Figure 7. Analyze for New System

4.2.3 User Interfaces

- **Bus Application**

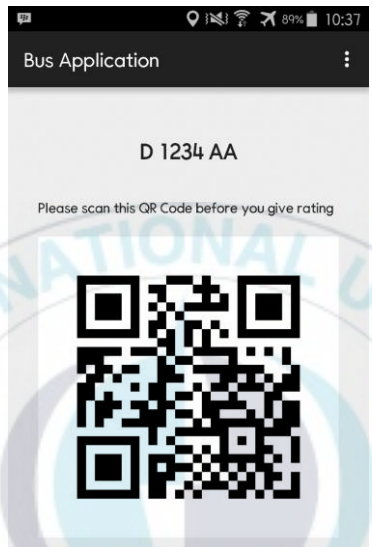
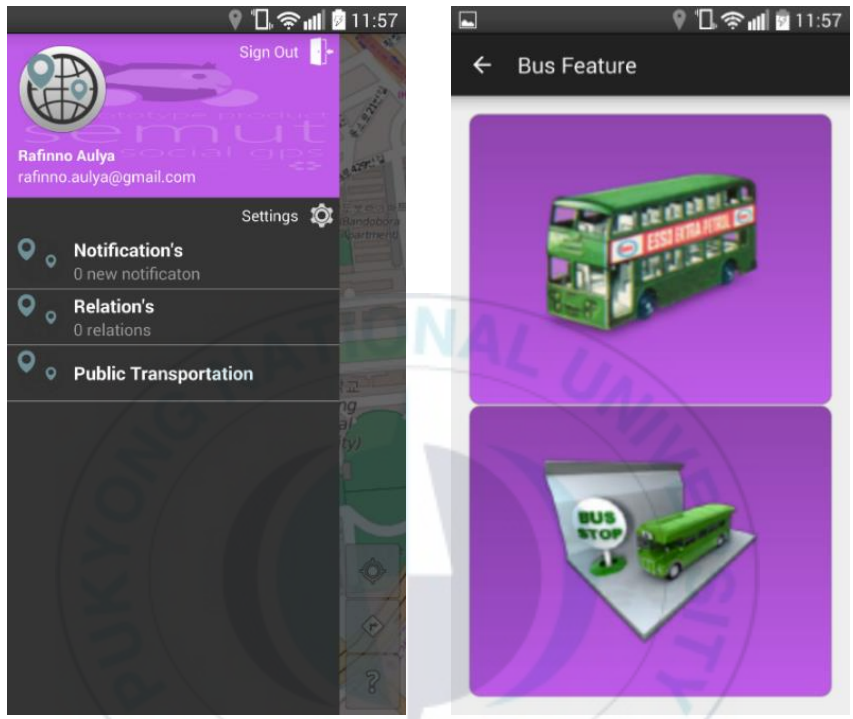


Figure 8. QR Code Display on Bus

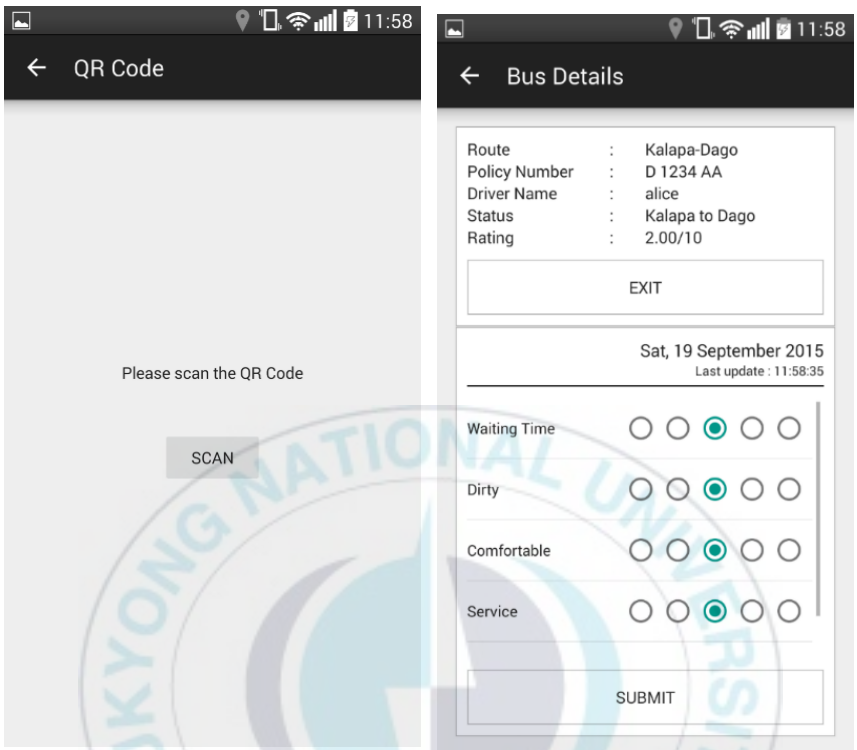
Applications on the bus will display a QR Code, and will be changed if it has been used or is not used within 5 minutes after the QR Code created.

- **Passanger Application**



(a) **(b)**

Figure 9. Menu Page of Public Transportation Feature (a) and Bus Feature Page (b).



(a) **(b)**

Figure 10. QR Code Scan Page (a) and Bus Report Page (b).

On this page, the user can select the menu "Public Transportation". There are two options on this page, to be able to contribute to giving judgment against the bus, the user can select the topmost button. Before a user can

give judgment against the bus, users should perform a scan against a QR Code that has been displayed on the bus.

Figure 11. QR Code Scanning Process

The application will instantly scan the QR Code when camera is directed to the QR Code, once the application gets results from QR Code, the application will send it to the server to be authenticated. After the result of scanning the QR Code is verified, and the response from the server is verified, then the application displays the assessment page.

Chapter 5. Conclusion and 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. We are able to authenticate devices that are adjacent to move in the same direction, properties that can be utilized is global position of the devices. We can authenticate the distance of the two devices, and we also need secure communications to authenticate i.e. Bluetooth, QR Code,

NFC, etc. By utilizing the devices, we can develop authentication scheme according to the environment is available on the devices.

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. For future research, this feature could be developed on the techniques of encryption and authentication schemes on the QR Code. And for future research , this feature will apply “Distributed Database Systems” to solve the problem traffic data on the server.

References

[1] L. Hua dan J. Dai, "A location authentication scheme based on adjacent users," dalam *Progress in Informatics and Computing (PIC), 2014 International Conference on*, 2014.

[2] W. Junhan, Q. Fei dan L. Jianfeng, "Research and application of the location information in the intelligent transportation," dalam *1st International Workshop on Cloud Computing and Information Security*, 2013.

[3] R. Aulya dan K.-H. Rhee, "Location Based-Services Over Gamification Approach," dalam *Korea Multimedia Society*, Andong, 2015.

[4] W. Jansen dan 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.

[5] A. Developers, What is android, Android Developers, http://developer. android. com/guide/basics/what-is-android.html, 2011.

[6] W. Enck, D. Octeau, P. McDaniel dan S. Chaudhuri, "A Study of Android Application Security," *USENIX security symposium,* vol. 2, p. 2, 2011.

[7] G. W. Architects, Putting the Fun in Functional - applying game mechanics to functional software, 2009.

[8] S. Deterding, D. Dixon, R. Khaled dan L. Nacke, From game design elements to gamefulness: defining gamification, ACM, 2011.

[9] J. McGonigal, Reality is broken: Why games make us better and how they can change the world, Penguin, 2011.

[10] I. Bogost, Persuasive games: The expressive power of videogames, Mit Press, 2007.

[11] K. Huotari dan J. Hamari, "Defining Gamification - A Service Marketing Perspective," dalam *ACM*, 2012.

[12] DENSO WAVE INCORPORATED, [Online]. Available: http://www.qrcode.com/en/.

[13] T. S. Parikh dan E. D. Lazowska, "Designing an architecture for delivering mobile information services to the rural developing world," dalam *Proceedings of the 15th international conference on World Wide Web*, 2006.

[14] J. Rekimoto dan M. Saitoh, "A Spatially Continuous Workspace for Hybrid Computing Environment," dalam *Proceedings of CHI'99*, 1999.

[15] G. Yu, Z. Wang, L. Yi dan L. He, "An application and implementation of two-dimensional symbols for circuit board quality control system," dalam *Industrial Informatics, 2004. INDIN'04. 2004 2nd IEEE International Conference on*, 2004.

[16] J.-C. Chuang, Y.-C. Hu dan H.-J. Ko, "A novel secret sharing technique using QR code," *International Journal of Image Processing (IJIP)*, vol. 4, no. 5, p. 468, 2010.

[17] D. E. Denning dan P. F. MacDoran, “Location-based authentication: Grounding cyberspace for better security,” *Computer Fraud & Security*, no. 2, pp. 12-16, 1996.

[18] D. Jaros, R. Kuchta dan R. Vrba, *The Sixth International Conference on Internet and Web Applications and Services (ICIW 2011)*, vol. 6, pp. 20-25, 2011.

[19] M. Talasila, R. Curtmola dan C. Borcea, “Collaborative Bluetooth-based location authentication on smart phone,” *Pervasive and Mobile Computing*, vol. 17, pp. 43-62, 2015.

[20] N. Gholap, S. Das dan L. D N, “Location And Authentication Based Encryption Scheme Application Design For Mobile Device,” *International Journal of Engineering Research and Technology*, vol. 2, no. 4, pp. 1619-1623, 2013.

[21] J. ZHANG, X. LI dan M. ZHANG, “Study and Realization of Authentication Technique Based on MD5 Algorithm,” *Computer Engineering*, vol. 4, p. 45, 2003.

[22] N. Milanovic dan M. Malek, “Current solutions for web service composition,” *IEEE Internet Computing*, no. 6, pp. 51-59, 2004.

[23] I. Ristic, Apache Security, O'Reilly, 2005.

[24] C. J. Lamprecht and A. V. Moorsel, "Adaptive SSL: Design, implementation and overhead analysis," in *Self-Adaptive and Self-Organizing Systems, 2007. SASO'07. First International Conference on* , 2007.

Acknowledgements

Al-hamdu lillahi rabbil 'alamin, all praises are belonging to Allah S.W.T who has given the writer the health and the strength to finish this thesis. My blessing and peace of Allah upon the messenger of Allah, Muhammad S.A.W, his family and companions.

I revere the patronage and moral support extended with love, by my parents and my families whose support and make me passionate to complete this thesis.

I would like to thank LISIA Member (Sam, Brian, Myeong, Kim, Wan) and especially for Professor Kyung-Hyune Rhee, Dr. Youngho-Park, Sunbae Bayu Aditama, Sunbae Lewis for the guidance in LISIA Lab.

I would like to thanks our Professor Bon-Ki Shin, Professor Chan-So Kim and especially for Professor Man-Gon Park for this program and for the guidance.

I would like to thanks for ITB, especially for ITB Rector Pak Prof. Dr. Ir. Kadarsah Suryadi DEA, Dean STEI Pak Dr. Ir. Jaka Sembiring, M.Eng, Pak Dr. Ir. Hilwadi Hindersah, M.Sc, and Pak Dr. Ir. Charmadi Mahbub as our supervisor for guide during study in ITB and PKNU and attend our final thesis presentation. And also thanks to DIKTI for the scholarship, and Pak Dr Gatot Hari Priowirjanto, Pak Dr. rer. nat. AB Susanto, MSc, Mbak Dipl.Ing (BA) Cahya Kusuma Ratih, M.T and PKNU Administrative Staff for the chance and your help.

Thanks also to friends Dual Degree ITB-PKNU 2015