INTERNATIONAL CONFERENCE ON CLIMATE CHANGE AND SUSTAINABILITY ENGINEERING IN ASEAN

International Conference on
Climate Change and Sustainability Engineering in ASEAN
(CCSE-ASEAN)2019
University of Jember, Indonesia, 13-14 November 2019
Jalan Kalimantan 37, Jember, Jawa Timur, Indonesia 68121
Website: https://ccse-asean.org email: info@ccse-asean.org

27 September 2019

Dedy Wahyu Herdiyanto
University of Jember

Subject: **Letter of Acceptance and Invitation to CCSE-ASEAN 2019**

Dear Dedy Wahyu Herdiyanto

We are pleased to inform you that your paper entitled *Electronic Transaction System For User Authentication And E-Payment Application Based On Rfid Smart Card* has been accepted for oral presentation by the International Conference on Climate Change and Sustainable Engineering in ASEAN (CCSE ASEAN) 2019.

We hereby cordially invite you to participate as a presenter at CCSE-ASEAN 2019, which will be held at the Auditorium of University of Jember, Jember City, Indonesia on 13-14 November 2019. Details on the registration are herewith attached.

We would be thrilled to have you present your research at this conference. We would also love to hear your thoughts and opinions about how to enhance the role of engineering in dealing with concerns about climate change and sustainability in Southeast Asia.

We are looking forward to welcoming you at CCSE-ASEAN 2019.

Yours faithfully,

Dr. Eng. Triwahju Hardianto
General Chair of CCSE-ASEAN 2019
Email: triwahju@ccse-asean.org

Hosts:
Faculty of Engineering, University of Jember
School of Engineering, University of San Carlos

UNIVERSITY OF SAN CARLOS
SCHOOL OF ENGINEERING

Electronic Transaction System for User Authentication and E-Payment Application Based on RFID Smart Card

Dedy Wahyu Herdiyanto [1,a)], Dodi Setiabudi [2,b)], Ali Rizal Chaidir [3, c)]

[1,2,3)] *Electrical Engineering Department, University Of Jember, Kalimantan Street No. 37 Jember 68121*

[a)] dedy.wahyu@unej.ac.id.
[b)] dodi@unej.ac.id.
[c)] ali.rizal@unej.ac.id.

Abstract. In this digital era, everything various aspects in life needs to be done fast, practical, and reliable. All these demands encourage people to consider adopting technology in life that includes microtransaction. Until this day, most of the microtransactions still carried by using conventional cash transactions. Although some people already use a debit card when as the times progressed, people began to switch to cashless transactions. Another similar system that has been implemented has each different design, but always prioritizes the principle of robustness, scalability, and flexibility. This paper proposes a cashless transaction system for the small-scale organization such as school, college, office, and other organization by designing an RFID terminal device and database server. This system aimed to be more user-friendly and straightforward. The designed system consists of an RFID card as e-money, terminal transaction device, and database server. RFID serves as a unique ID owned by the user to identify themselves to authorize their transactions. The user will be able to make a payment on the terminal device installed in the vendor shop by using the smart card. The device will access the database connected by a local network using wireless communication. The server will receive data from the terminal device that consists of user ID, vendor ID code, transaction type code, and transaction nominal. The results of the connectivity test show that at a distance of 1-6 m TD (Terminal Device) does not experience connection failure and delivery. However, starting at a distance of 7 m, TD indicates a failure of 18% of all experiments. TD can connect when separated from access points at a distance of 10 m but has a low success rate at distances of 9 and 10 m. TD always restarts connections after multiple shipments (5-6 shipments for a distance of 9 m, and 3-4 shipments at a distance of 10 m). In testing the connection delay, access time at a distance of 1-6 meters is quite stable with a range of 3-4s. The time needed for TD to connect can be said to be quite stable between 3-4 seconds. It will increase when separated from access points at a distance of 6 m even though the success rate remains stable up to a distance of 8m. For the next development, it is planned to use a single board computer hardware.
Keywords: wireless, communication, RFID, database, smart card

1. INTRODUCTION

The high community needs for easy and fast access to information have led to a paradigm shift towards information technology. The community as users began to adopt various technologies that were appropriate to their individual needs. One of the most widely applied technologies is cashless / e-payment systems. the world of electronic payments is evolving quickly with mobile payments emerging as an alternative to the credit card/debit card ecosystem [1]. It comes alongside crime reduction, reducing excess stocks and work in progress and also other benefits that directly impact costs [4]. However, in part of its application, many of these payment systems are still not stable enough, including due to hardware errors and long server processes. So, if sorted the improvements that need to be done are on the algorithm in the system. The algorithm must be made as simple as possible to reduce the excessive load on the system. In general, electronic payment requires three points, robustness, scalability, and flexibility [2,3].

In this study, a cashless payment system will be designed that is suitable for everyday use. The system is designed using a 13.56 MHz RFID-based smart card method. This payment system will be run with a server on the local network, to simulate the state of the application in stores, vending machines, cooperatives, and canteens in offices, shopping centers, schools, campuses, and other places. The purpose of this research is to produce a prototype early from an e-payment system with high average success.

The device used to read RFID card called terminal device, which is a portable identification and payment hardware that installed on the vendor. On the security point of view, RFID already has a feature that can prevent forgery because each RFID card has a unique ID that always different from each other [4].The primary purpose of the device is to identify user card and send it through a dedicated server. The server will manage all the data of users such as identity, balance, and transaction record by matching received data. The server will do all the calculating process to determine the cost that the user needs to pay.

After Introduction in Section I, the remaining of this paper written as follows: Section II presents some literature survey and research method. Section III presents process, design, and architecture that needed for this system. Section IV presents the result of the evaluation from this system. Also, the last section, Section V, presents the conclusion from this system and future work that need to be applied.

2. CONCEPT AND PROPOSED METHOD

Payment systems have undergone an incredible evolution, in only a few ten years, passing from a physical transfer of cash for goods or services to transactions exchanging money as digital data. Electronic Payment refers to payment system that to any type of electronic transaction, operated under financial regulation, involving funds transfer from a buyer to a seller of goods or services, and completed through an electronic network [5]. To ensure the security of these transactions, startups that are intermediaries will work with a number of banking institutions to start facilitating e-payment safely, quickly and practically. Currently, many startups facilitate sellers and buyers by providing security guarantees for e-commerce transactions.

In the system presented in this paper, the user can make payment or transaction on vendors or merchants that use this system. The terminal device will attempt to connect to the server when it scanned recognized access point on location. After it connected in standby mode, the user can make a transaction by putting card near RFID reader on the device. It will forward UID data from RFID through a network to the server. UID is a unique ID registered on RFID card. Each of the RFID cards always has different UID. The server checks the database if there is matched UID and its balance. If the balance meets bill requirements, the server sends success feedback to the terminal device and passenger able to enter. When the balance does not reach the minimum fare, the user will get the notification that their payment failed and needs a top-up their balance first. The previous procedure will be repeated for each transaction.

The server calculates by deducing user balance that stored on a database with their bill. The server will overwrite the user's balance after the payment. The server sends success feedback again to the device to finish their transaction. The following figure will show the design of the system, especially at the terminal device and database server so it can fill those requirements. Moreover, the resulting framework system will be used in the small-scale organization, store, merchant, or vendor. System design is shown in Figure 1.

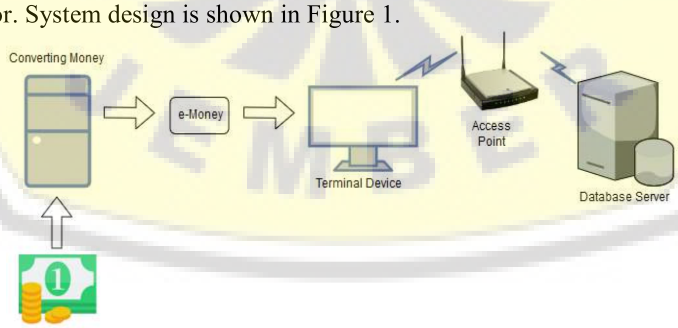


FIGURE 1. The process of designed system

3. AUTHENTICATION AND PAYMENT SYSTEM DESIGN

Authentication is the process in order to validate the user at the time of entering the system, the name and password of a user in check through the list of those granted the right to enter the system. Authentication used to confirm that someone (or something) is authentic or genuine. To authenticate the person usually is to verify their identity. In a ticketing system, authentication usually occurs when passenger request access to enter and leave vehicle. One of methods used to authenticate passenger is using RFID card as e-ticket.

RFID uses electromagnetic fields to identify and track tags attached to objects. The tags contain electronically stored information. RFID also has applied for many purposes, including airport and aviation service alongside IoT application to mark passenger luggage and cargo [6]. Typical requirements for RFID already depicted in Figure 2, which contains tag, reader, middle ware, and application system software.

FIGURE 2. Typical RFID System Design

3.1. Design of Terminal Transaction Device

The Board Unit was designed using microcontroller as base hardware. The design consist of five (5) main component, including 1 main processor board, 2 shield modules, keypad, and DC power input. The hardware used on terminal device shown in Figure 3 below.

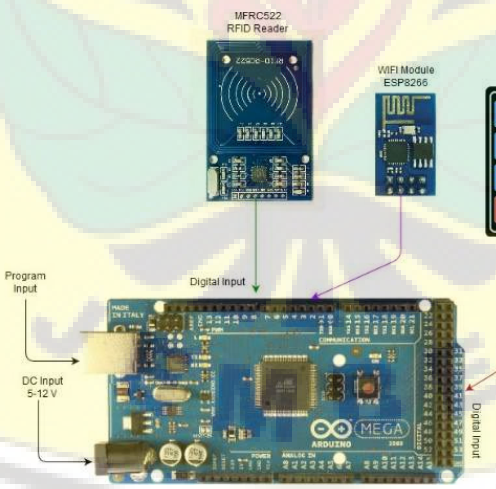
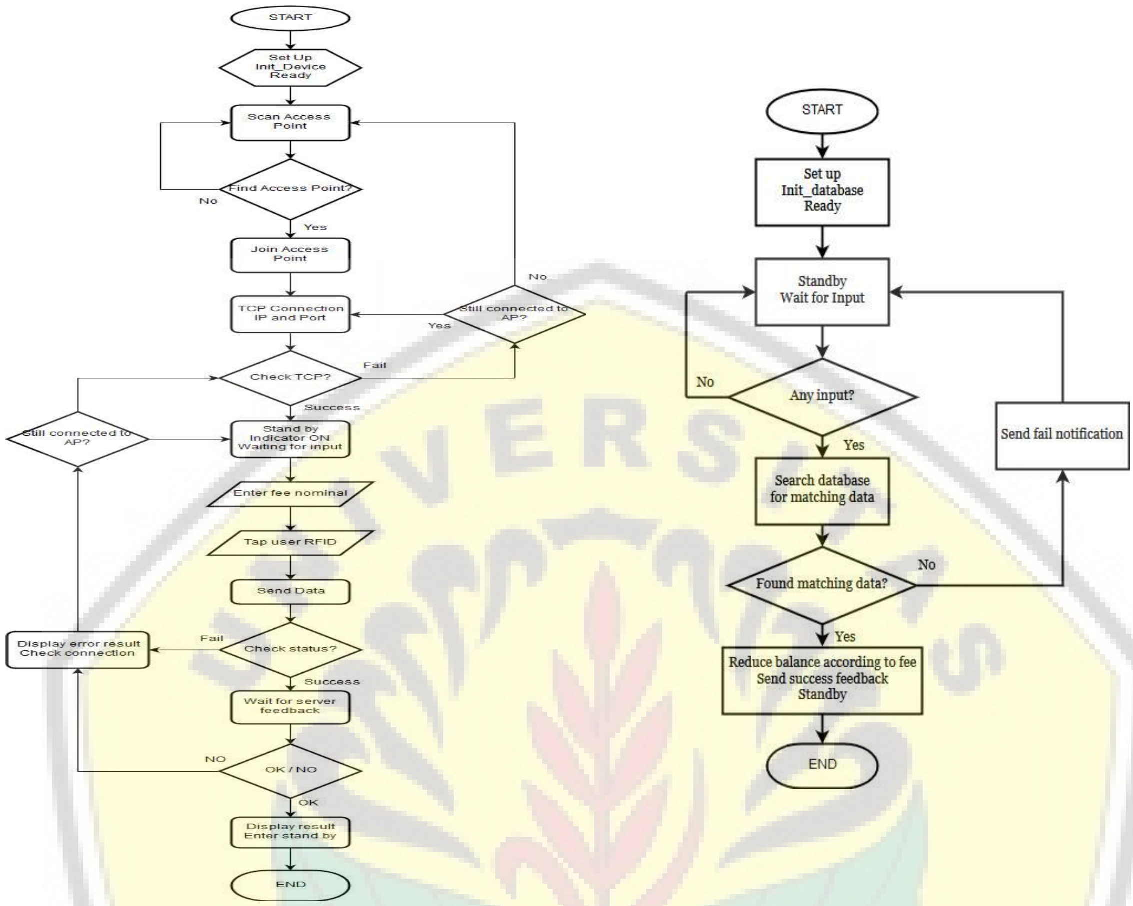


FIGURE 3. Terminal Device Board Diagram

Arduino Mega serve as main processor. The shield used for Wi-Fi connection is ESP8266. ESP8266 is open source Wi-Fi shield module board that becomes popular for Internet of Things application in the recent years [7]. ESP8266 already proved having great RSSI (Received Signal Strength Indicator) in room size area, whether in NLOS (Non Line of Sight) or LOS (Line of Sight) condition [8]. RFID shield module used in our project is MFRC-552. This module operates for RFID tag at frequency 13.56 MHz. MFRC-552 is RFID reader and writer that already commonly used in many RFID projects.



(a) (b)

FIGURE 4. (a) Flowchart of Terminal Device Operation, (b) Server payment operation

Figure 4.a shows the process in the device when it makes a connection and sends data. IP address lets in blank because it can be filled with any IP address as long it never changes when a connection is made. As for the port number, it is better to use Dynamically Assigned Port (1024-65536) to prevent connection crash. The data that sent to the server will have a format such as "YY#A#IDIDIDID#Nominal". "YY" is a code to identify merchant, vendor, or store. "A" is transaction type code. There will be two types of transaction, balance top up and balance deduce, so it needs to be differentiated. IDIDIDID represent eight unique characters known as a UID. UID, as mentioned before, will serve as a password and contain eight characters. UID used to find passenger ID, which is the primary key in the server. The last variable is nominal, which is inputted manually based on each payment. When the condition is set, the terminal device will send data using TCP connections. The terminal device needs to know the server IP address and port o send the data. Indicator for success and fail also has been added using LED and buzzer tone.

3.2. Server Process and Configuration

The other side of this system will be at the server. The server will keep the record of all data traffic and user data. The server provides communication socket because TCP connection cannot directly connect to PHP database. The server will open a socket to receive the data stream from the device. The process that occurs on the server while the user makes payment shown in Figure 5.b. When the user makes a payment, the server will check if the user has a minimum balance on their account. The minimum limit for balance also added to server algorithm. The system can prevent minus count on user balance by checking the minimum limit. After making sure the user's balance, the server will process the incoming message from the terminal device. The server will do the calculation by deducing current balance with bill nominal. It also sends feedback to the terminal device to let user that the payment has been completed.

4. DISCUSSION AND RESULTS

This section explain the conducted tests to evaluate performance of the system. The evaluation divided into two section, that is terminal device evaluation and system overall evaluation.

4.1. Terminal Device Evaluation

This part shows the result of the test to determine the limitation of the designed terminal transaction device. In an attempt to send data, the hardware or terminal device (TD) will read the RFID card and send information to the USR-TCP Test application. Observation is divided into two parts, namely when TD sends data and when receiving feedback. The results displayed when TD sends data to the application are shown in the following figure 5.

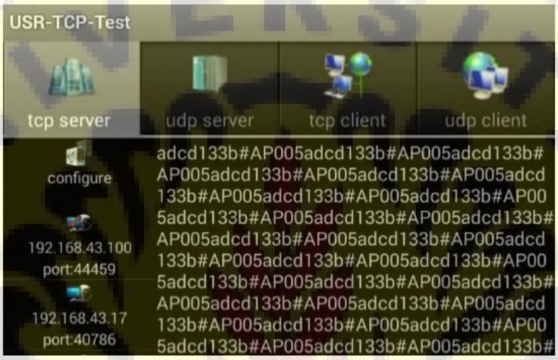


FIGURE 5. Sending data over to virtual server

In the picture above you can see the data sent by TD. The format of the data sent for testing the functionality is not the format that will be used later. This format is used to simplify checking the test. On the side, the IP address and port used by TD are also displayed. After the TD function for sending data can be executed, the test is continued by observing the effect of distance on the function. The following results are shown in the Figure 6 below.

FIGURE 6. Connectivity result obtained from various distance

In the graph above, it is shown that at a distance of 1-6 m TD does not experience connection and delivery failures. However, starting at a distance of 7 m, TD indicates a failure of 18% of all experiments. Even at distances of 9 and 10 m, TD always restarts connections after multiple shipments (5-6 data transfers for a distance of 9 m, and 3-4 transfers at a distance of 10 m).

After testing TD connectivity, the next observation is for the access time of the test. Every time at a specified distance, 100 attempts have been made on connectivity testing. Then the results of the time are drawn on average based on the test distance. The following is a graph of the average access time for each distance in Figure 7 and Table 1.

TABLE 1. Average Connection Time against Distance Change

No.	TD-AP Distance	Average Connection Time
1	1 m	3,2 s
2	2 m	3,1 s
3	3 m	3,4 s
4	4 m	3,5 s
5	5 m	3,6 s
6	6 m	4,0 s
7	7 m	4,6 s
8	8 m	5,0 s
9	9 m	5,4 s
10	10 m	5,6 s

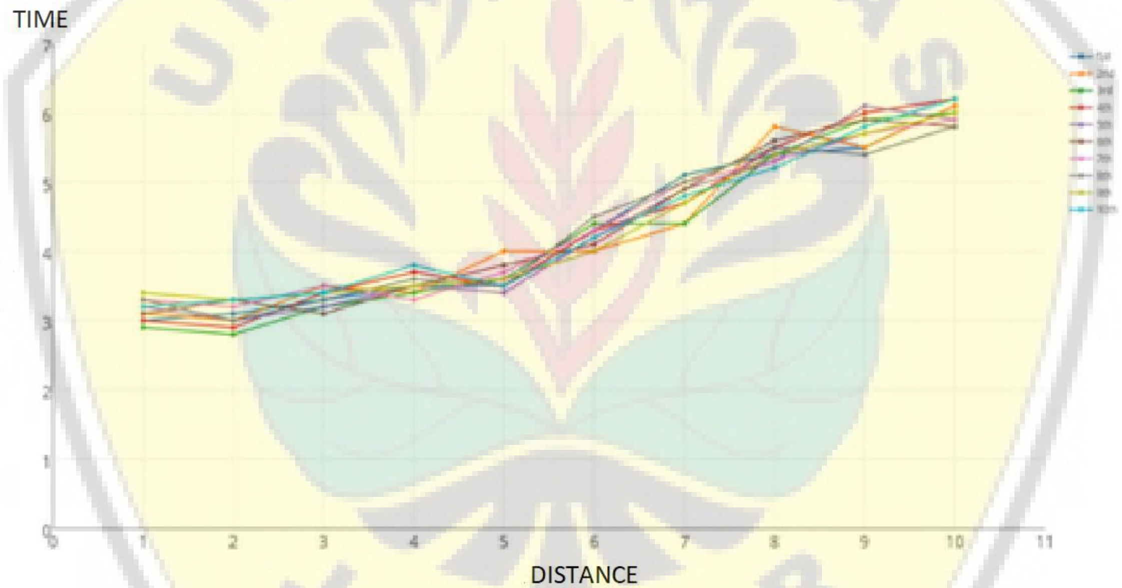


FIGURE 7. Average Connection Time Against Distance Change

In the graph above, access time at a distance of 1-6 meters is quite stable with a range of 3-4s. Even though at a distance of 6 meters, it is still said to be stable, at that distance, the access time begins to experience a significant increase. Also, after reaching 7, 8, 9, and 10 meters, the time needed is getting bigger. If it is associated with the results of connectivity testing, the last four variables from a distance also decrease the quality of the connection, especially at a distance of 9 and 10 meters. The decrease in quality is indicated by the more frequent restarting connections on TD.

4.2. Database Synchonization

After checking TD can work as expected and also its limitation, the next step is to check if TD can work with the rest of the system. The test condition created based on the result of TD evaluation. TD will be tested using a simple server that has been designed. The primary purpose of this test is to ensure the success of TD synchronization with the server. It is also can determine whether the transfer made by TD can be recorded by the server and the user who made the transaction successfully entered the payment query. The test results are shown in the following figure 8.

iduser	uid	saldo	ssid	status	queue
170	1	8000	AP002	0	0
172	2	989000	AP5	0	0
181	adcd133b	71000	AP005	0	0
190	abcdefg1	5000	AP006	0	0
192	83269075	19000	AP004	0	0

FIGURE 8. Display of the database on the server

For this test, the user ID is registered in advance with the nominal balance in various nominal amounts. Users are assumed to make transactions continuously. SSID changes or access points are conditioned if the user moves the transaction area. The results obtained from the test are very satisfying. All tests received positive results without any transaction error. In this test, it has also been proven that there were no problems when the transaction location was changed. This result also proves that the system is ready to be integrated more broadly.

The last test done on the system is testing the success rate if there is more than one data sent to the server at the same time. TD that is used as a comparison is a virtual TD using a smartphone. The server used is the USR-TCP application, because if the test uses a database server, it is difficult to know the speed of arrival. The test is carried out by sending data from the three TD simultaneously at the specified distances. There are two intervals used in this test, namely with a random interval for each data transfer. The result will be shown in figure 9 below.

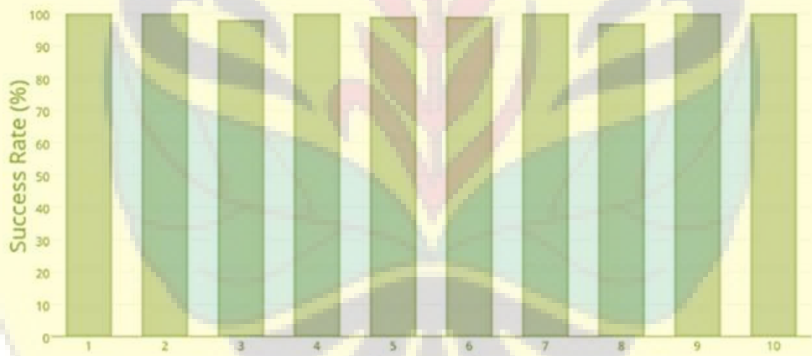


FIGURE 9. The results of sending data from multiple TD at random intervals

When testing the random intervals, the results obtained are not too much different from the results obtained from regular interval testing. TD can send data without experiencing errors that can disrupt the system. However, minor errors such as reading errors still appear in some tests.

From these results, it can be said that there are no problems for the transmission of three TDs at the same time. That is because the TCP connection process will ensure that the connection is connected between the TD and the server. Also, the port connection is confirmed once more is truly synchronized the TD and the server before sending data. For the success rate itself, it can be said that there are no problems when sending simultaneously.

5. CONCLUSION

From the evaluation and test that has been conducted in various way, several conclusion can be taken from the results. TD is able to connect when separated from access points at a distance of 10 m, but has a low success rate. The time needed for TD to connect can be said to be quite stable between 3-4 seconds, but it will increase when separated from access points at a distance of 6 m, even though the success rate remains stable up to a distance of 8m.

The success rate of data transmission has dropped dramatically to around 50% in testing with a distance of 9 m. The connection will experience a reset when the delivery success rate decreases. When there are more than 1 TD that makes a transfer, the server is still able to receive data with a very good success rate. An error on the port connection can be avoided because after the connection is received by the server, the server will move the connection to another port within the DAP (Dynamically Assigned Port) range.

The next step for this research is creating a better interface for the operator. As can be seen, the server still operated from computer system and not user friendly. There are also rooms for improvement to use hardware for OBU using better specification from Raspberry board or other mini computer. In addition, it could improved by adding an interactive monitor that can show transaction. Although it also needs to keep the concept of compactness for hardware design.

REFERENCES

1. Preuveneers, Davy et al. *Feature-Based Variability Management for Scalable Enterprise Applications: Experiences with an E-Payment Case*. 2016 49th Hawaii International Conference on System Sciences (HICSS). January 2016.
2. Herdiyanto, Dedy Wahyu et al. *Passenger Authentication and Payment System Using RFID Based On-Board Unit for Surabaya Mass Rapid Transportation*. 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA).
3. Chang, Pintsang. "A Distributed Integrated Fare Collection and Accounting System in Metropolitan Railway Transit," 9th International Conference on Ubiquitos Intelegence and Computing and 9th International Conference on Autonomic and Trusted Computing, 2012, pp. 797 - 802
4. Vishwanat, Arun et al. "Personalised Public Transportation : A New Mobility Model for Urban and Suburban Transportation," 2014 17th International IEEE Conference on Intelegent Transportation System, Qingdao, China. October 8-11 2014, pp. 1831 - 1836.
5. Alessandro Vizzarri and Francesco Vatalaro. *m-Payment systems: Technologies and business models*. 2014 Euro Med Telco Conference (EMTC). Naples, Italy
6. Dietmar P.F. Möller and Hamid Vakilzadian. "Wireless Communication in Aviation Through the Internet of Things and RFID," Electro/Information Technology (EIT), 2014, pp. 602 –607.
7. Kolban, Neil. "Kolban's Book on ESP8266". 2015. Texas, United States of America. Pp. 27.
8. Yoppy ; R. Harry Arjadi ; Henry Candra ; Haryo Dwi Prananto ; Tyas Ari Wahyu Wijanarko. *RSSI Comparison of ESP8266 Modules*. 2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS). Batu, East Java, Indonesia, Indonesia.