# Performance Evaluation of Smart Security System Prototype based on Radio Frequency Identification (RFID) and Internet of Things (IoT)

Doan Perdana, Muhamad Ihsan, Rendy Munadi, Sussi, Nurwulan

*School of Electrical Engineering*, Telkom University, Indonesia.

Email: doanperdana@telkomuniversity.ac.id; muhamadihsan@student.telkomuniversity.ac.id; rendymunadi@telkomuniversity.ac.id; sussi@telkomuniversity.ac.id; nurwulanf@telkomuniversity.ac.id

***Abstract* - A home security system from the front door is very important. Unfortunately, most door access used at home is still using a conventional key. Where its use is still vulnerable to hacking. In this research, this home door security system is able to be a solution to maintain the security of all aspects which are placed in the house. The door security system is RFID-based as an access to unlock the door. There is also an Internet of Things system so the door lock can be opened remotely. Instead of a conventional key, the system uses an RFID card which is a smartcard in which there is a tag of different unique code in each card. So the key can only be opened by a recognized card only. The system will notify the homeowner if there is someone unknown attempts to unlock. Tests in this study yielded the smallest end-to-end delay data was 0.314s with throughput of 5116.35 Bytes / s. And also the average Availability system of 97.39% and Reliability system of 97.30%.**

***Keywords - Internet of Things, Radio Frequency Identification, Door Security System, Smartcard***

## I. INTRODUCTION

Home security systems in general still use conventional keys that are vulnerable to break-ins. Other than that, in terms of efficiency, the use of conventional keys is very inefficient, because with the many doors in a house can imagine the number of keys that we must carry. Therefore an integrated system is needed that can replace the conventional door lock

One way to overcome the above problems is to use an RFID system. RFID (Radio Frequency Identification) is one of the superior and fast technologies in identifying an object. The advantage of this technology is the ability to identify wirelessly, and can contain other than just barcodes. RFID can read in any condition compared to other technologies such as barcodes or optical card readers that can only read when certain conditions. RFID is generally attached to a card. In this research the card used is an RFID card, which is a card in which there is a chip that will be induced by the RFID reader so that both can communicate. RFID tags in the RFID card can be used as authentication to open access from a door. So that only the listed cards can access.

RFID is widely used in terms of security, especially for the authentication feature of the access rights of an object. As in [1] where researchers implement the RFID function to authenticate access rights from the house door. With RFID, we no longer need to carry a key because we only need an RFID card that we can store in our wallet or pocket. The use of RFID can also avoid the drawbacks of conventional keys that are easy to duplicate.

To anticipate if anyone wants to access the door but does not have a card, researchers add the Internet of Things feature to the system so that the door can be opened through the device carried by the homeowner. The Internet of Things is a concept where an object can transmit data without interaction with humans. The concept of the Internet of Things is often used to control an object through the internet. The application of IoT to this home security system is one of its functions in everyday life. The application of IoT in the system is expected to improve the features of the tools made by researchers.

One of the benefits of IoT is that we can control a device via the internet network, as in the research [2] Neetu Gupta et al where researchers make system architecture designs to unlock doors through Android-based applications. With this design, door security can be guaranteed and has an easy-to-use concept. We can avoid losing keys because the application used is stored on the smartphone we have.

On [3] has designed an automatic locking system using RFID with an Arduino Uno microcontroller. The system provides a numeric keypad to anticipate anomalies or disturbances and enter an emergency password to open the door. To open the door from the inside, the researcher added a push button. in other research [4] has made a Smart Home system whose function is to control the state of the house through an application. The system adopts the concept of the Internet of Things where data from each sensor is sent via the internet and displayed in the application. The results of this study are that the system is running well where data transmission from the sent monitoring system is 100% with an average delay of 9.6 seconds per shipment. Moreover, the control system testing produces an average delay of 2.3 seconds for each controller.

## II. RESEARCH METHOD

In this research there are several methods used by authors to support the research include system design, block diagrams, smart door system logic design, application design, tools and materials used, applications and supporting software.

### *A. System Design*

In this system, the key control is designed to be accessible using two ways with the RFID and IoT systems. With an IoT-controlled presence, the status of the door we can monitor to monitor the safety of the home was successful.

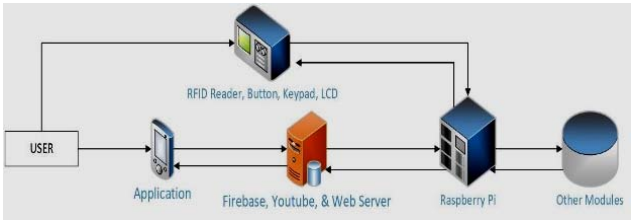


Figure 1. System Design.

Figure 1 shows general view of the system. The system is centered on a microcontroller that determining the system's course when entering the house, the user will be asked to authenticate through the card that he or through the application. When guests arrive, guests simply press the button beside the door so the camera above the door will take pictures from guests break or forcibly opened later the user will get a notification on the application used by the user.

### *B. Block Diagram*

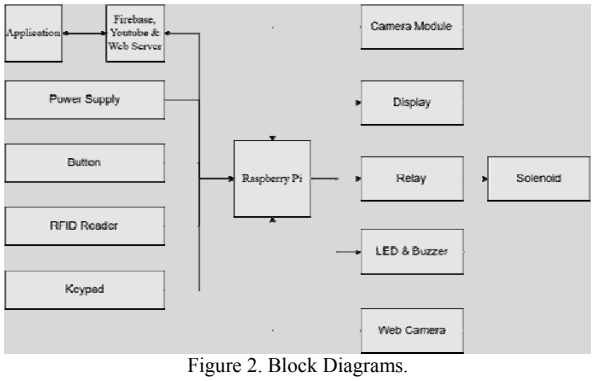


Figure 2. Block Diagrams.

Figure 2 shows block diagrams of designed systems. The system consists of two microprocessors namely the first one is a Raspberry Pi that has an input of 4 pieces originating from the IoT Platform, power supply, Door Bell, RFID Reader, Web Camera, and Camera Module.

### *C. Smart Door System Logic Design*

Programs designed are programs for door access features through RFID or applications, live stream features, doorbell features, alarms, and also notifications. Here is a description of the logic designing program on Raspberry Pi.

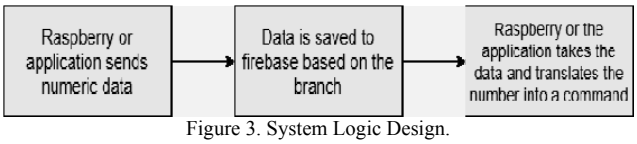


Figure 3. System Logic Design.

Figure 3 shows provide commands between Raspberry Pi and application system using a numeric code, Raspberry Pi or application is going to translate the numbers that exist in the database into a command that has been defined in the program.

### *D. Application Design*

The design of the QRSmartDoor application uses Android Studio, an Android IDE software to create an android application.

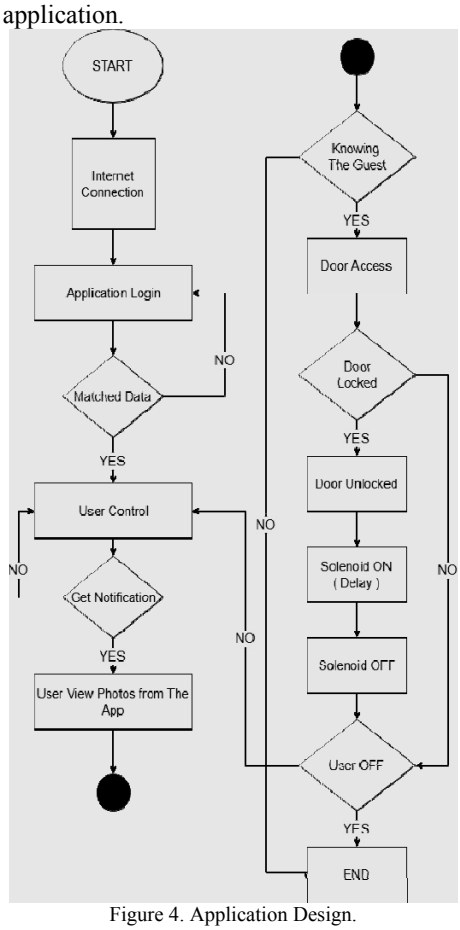


Figure 4. Application Design.

Figure 4 shows about door control using the Internet of Things with the case of a guest coming home.

### *E. Tools and Material Used*

In this research to run the system that have been created, it takes several supporting components that can help run the system to function properly. The following is a table of components that support the whole system.

TABLE I. SYSTEM SUPPORT COMPONENT.

| No | Component | Specifications | Uses |
|---|---|---|---|
| 1 | RFID Reader | MIFARE MFRC522, Frequency 13,56MHz | Read UID from RFID Card |
| 2 | RFID Card | Passive RFID Tag | User authentication for accessing door |
| 3 | Web Camera | Resolution up to 5MP, 1024x768 pixels | QR Code Scanner |
| 4 | Solenoid DC | 12 V | Electric Key Door |
| 5 | Relay | 5 V | As electric switch to open and close the lock |
| 6 | Raspberry Pi 3 | B+ Model, 1GB Ram, 1,2Ghz CPU quad-core | Microcomputer to process the entire system |
| 7 | Camera Module | 1,3MP Resolution | As recorder for live stream feature |
| 8 | Keypad 3x4 | Membrane Matrix 3x4 | For user to input password |
| 9 | LCD | 16x2 | For system process display |
| 10 | Power Supply | 12 V | For the DC solenoid resource |
| 11 | Magnetic Switch | 3 W | For Door alarm Sensors |

Table I shows there are 11 supporting components directly connected to the Raspberry Pi. The 11 components have their own functions as in the table.

### *F. Application and Supporting Software*

In this research needed several applications and supporting software to program the tools and the creation of applications to be used.

TABLE II. APPLICATION AND SUPPORTING SOFTWARE.

| **No** | **Software** | **Uses** |
|---|---|---|
| 1 | Firebase | As system database |
| 2 | Phyton *programming* | Programming language used by Raspberry Pi to program supporting components |
| 3 | Wireshark | As software to record and analyze data communication |
| 4 | Youtube | As streaming server for live stream feature |
| 5 | Docker Container | FFMPEG app Emulator to record video and send it to Youtube |
| 6 | Web Database | To save the photo on the door bell feature |
| 7 | Android Studio | Software for creating Android applications |

Table II shows Firebase as a database on this smart door system can also be called an IoT platform from the system because it works to connect tools with applications through the Internet network. In this research the software is used to retrieve the Quality of Service data from the communication between the tools to the application is Wireshark. The Data then be used as an analysis material to assess how good the system communication is performing. Using Youtube as a streaming server of live streams is because in addition to seeing situations in real time, earlier live stream videos will be saved so that we can see them later.

## III. SIMULATION PARAMETERS

### *A. Performance Test Parameters*

This research using some of test parameter to find out the performance of the network between our prototype, there are:

*A1. Delay:* Delay the time needed for a communication package that the user sends to the device. Delay on a network greatly affects the quality of communication that exists in the network, so delay can also be said as a delay in a communication packet caused by the transmission process from sender to receiver [5], with the following formula:

$$\text{Delay} = tRx - tTx \quad (1)$$

In the equation (1), tRX represents the total time to data arrive in the receiver and time to source send the data.

*A2. Throughput:* Throughput is the number of packages that arrive at the recipient's side within a certain period of time [5]. Throughput can be seen by placing wireshark on the sender or recipient, with the following formula:

$$\text{Throughput} = (rxData) / t \quad (2)$$

In the equation (2), rxData represents the total data that arrive in the receiver, and t is total of time it take to send the data.

*A3. Availability*: Avalability is the possibility of a system or device ready to be used when needed [6].

$$\textit{Availability} = \textit{(uptime/elapsed time)} \times 100\% \quad (3)$$

Availability can be obtained by calculating uptime, and the amount of time earned on each experiment. Uptime is a condition where systems or tools are in a reliable condition [7-9].

*A4. Reliability:* Reliability is the ability of a system or tool can maintain a system in certain conditions and periods of time [6]:

$$\textit{Reliability} = \textit{(uptime – downtime)/uptime)} \times 100\% \quad (4)$$

Reliability can be obtained by calculating the uptime, downtime earned on each experiment. Uptime is a condition where systems or tools are in a reliable condition, and downtime is a condition where the system or tools are in unreliable condition [7].

*B. Method of Testing System*

There are scenarios carried out for testing this system as follows:

-1. Testing Reading Distance RFID Reader: Reading distance testing RFID Reader MFRC522 done to see how far this RFID Reader can read the RFID card that users have been able to later become a guide for users in doing tap RFID card.
-2. Access Rights Testing: This test is done to find out how precise the system is in processing data in the database.
-3. Distance Range of tools to access points Testing: This test is conducted to determine the placement of tools to access the right points in order to function optimally by looking at the delay and throughput of the system. By using 2 test scenarios namely Line of Sight (LOS) and non-Line of Sight (non-LOS) [10].
-3a. LOS Testing: The test is done by placing the tool with access points on open land and testing it by moving the distance between the access points and the tool every 5 meters.
-3b. Non-LOS Testing: This test is done by placing a tool and access points in a different room so that there is a barrier and obstacle between them in the form of a wall. The test is intended to see the system performance when there is an obstacle between the tools with access points [11,12].
-4. Whole system Testing: Overall system testing aims to determine the availability and reliability of the system.

## IV. PERFORMANCE ANALYSIS

*A. RFID Reader Read Distance*

The test is divided into two scenarios, namely without barrier testing between RFID reader and RFID card and using plastic box barrier as thick as 1 mm. The number of RFID cards and RFID tags used are 3 pieces with a composition of 2 RFID cards and 1 RFID tag. Here is the view of the RFID card and the RFID tag used.

*A1. Testing without barrier*

TABLE III. TESTING WITHOUT BARRIER.

| Distance | UID | | |
|---|---|---|---|
| | Card 1 | Card 2 | Tag |
| 0,5 cm | Read | Read | Read |
| 1 cm | Read | Read | Read |
| 1,5 cm | Read | Read | Read |
| 2 cm | Read | Read | Not Read |
| 2,5 cm | Read | Not Read | Not Read |
| 3 cm | Read | Not Read | Not Read |
| 3,5 cm | Not Read | Not Read | Not Read |
| 4 cm | Not Read | Not Read | Not Read |

Table III shows there is a difference in the ability to read RFID reader to third object card and tag. Card 1 has a maximum reading distance is 3.5 cm, card 2 has a maximum readable distance of 2 cm, while for the tag maximum distance is 1.5 cm. The difference is influenced by the ability of the antenna of the chip that is in each card and tag.

*A2. Testing with barrier*

TABLE IV. TESTING WITH BARRIER.

| Distance | UID | | |
|---|---|---|---|
| | Card 1 | Card 2 | Tag |
| 0,5 cm | Read | Read | Read |
| 1 cm | Read | Read | Read |
| 1,5 cm | Read | Read | Not Read |
| 2 cm | Read | Not Read | Not Read |
| 2,5 cm | Read | Not Read | Not Read |
| 3 cm | Not Read | Not Read | Not Read |
| 3,5 cm | Not Read | Not Read | Not Read |
| 4 cm | Not Read | Not Read | Not Read |

There is a difference in the ability to read RFID reader to third object card and tag [13]. Card 1 has a maximum readable distance is 3 cm, card 2 has a maximum readable distance of 1.5 cm, while for the tag maximum distance is 1 cm. The difference is influenced by the ability of the antenna of the chip that is in the Each card and tag [14-15]. From the table can also be concluded that the barrier can affect the reading distance of the RFID reader as far as 0.5 cm.

*B. Access Rights Testing*

At this stage is the test of access rights against the registered card and that is not registered on the database. The test is divided into two scenarios there are testing with registered cards and with cards that are not listed.

*B1. Testing with Registered QR Code*

TABLE V. TESTING REGISTERED QR CODE.

| Test | Registered Card | | |
|---|---|---|---|
| | LCD Information | | |
| | Account 1 | Account 2 | Account 3 |
| 1 | ID Registered | ID Registered | ID Registered |
| 2 | ID Registered | ID Registered | ID Registered |
| 3 | ID Registered | ID Registered | ID Registered |
| 4 | ID Registered | ID Registered | ID Registered |
| 5 | ID Registered | ID Registered | ID Registered |

Table V shows the system successfully identifies the entire card correctly on every test.

*B2. Testing with Not Registered QR Code*

TABLE VI. TESTING NOT REGISTERED QR CODE.

| Not Registered Card | | | |
|---|---|---|---|
| Test | LCD Information | | |
| | Account 1 | Account 2 | Account 3 |
| 1 | ID Not Registered | ID Not Registered | ID Not Registered |
| 2 | ID Not Registered | ID Not Registered | ID Not Registered |
| 3 | ID Not Registered | ID Not Registered | ID Not Registered |
| 4 | ID Not Registered | ID Not Registered | ID Not Registered |
| 5 | ID Not Registered | ID Not Registered | ID Not Registered |

Table VI shows the system successfully identifies the entire card correctly on every test.

*C. LOS Testing*

Testing done by moving the appliance to access points every distance of 5 meters, starting from a distance of 5 meters to a distance of 35 meters. The complainers are meant to be a reference of how far should access points be placed against the appliance in order to function optimally [16,17].

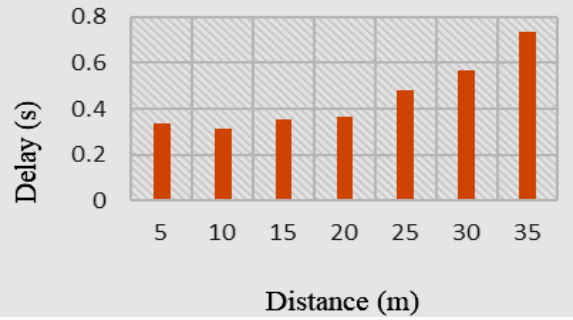


Figure 5. End to end Delay LOS.

Figure 5 shows the biggest end-to-end delay is 0.737 s and the smallest is 0.314 s. The increase in delay in Figure 5 is caused by changing the distance of access points with a device where the further the distance the access points, the signal received by the tool going to be weaker.

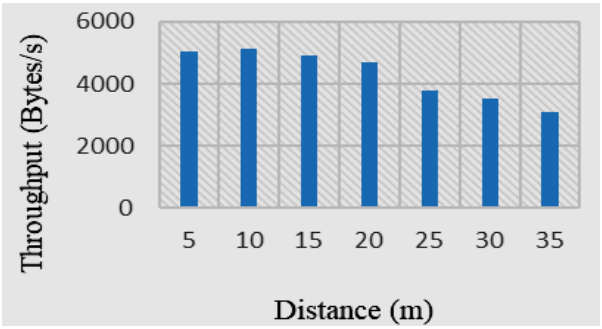


Figure 6. End-to-End Throughput LOS.

Figure 6 shows the largest end-to-end throughput is 5116.35 bytes / s and the smallest is 3080.38 bytes / s. The decrease in throughput in Figure 6 is caused by changing the distance between the access points and the tool which is the further the distance the access points, the signal received by the tool going to weaker.

*D. Non-LOS Testing*

Non-line of sight testing is done by moving the tool to access points to different rooms [18]. The room used amounts to 4 rooms which are rowing together.

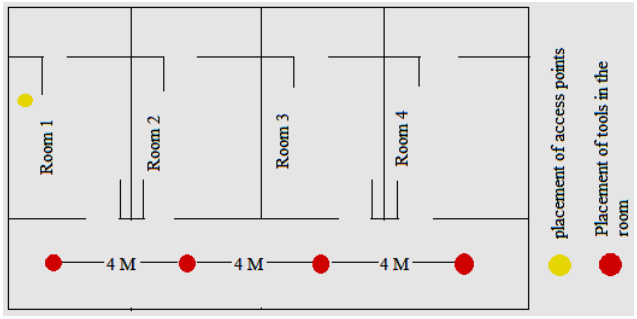


Figure 7. Testing Map.

Figure 7 shows the appliance is moved starting from the room 1 to 4. This test is intended to be a reference when the smart Door tool is implemented in a house that surely has many obstacle in the form of walls or other goods.

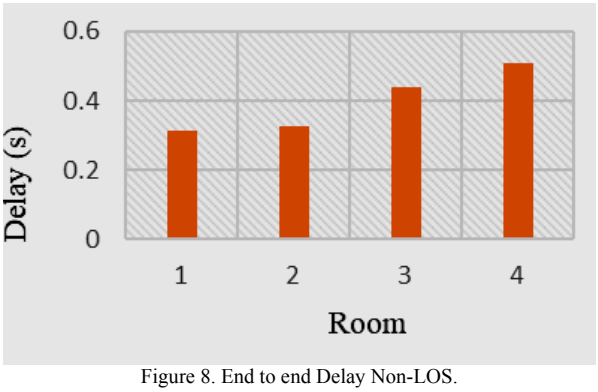


Figure 8. End to end Delay Non-LOS.

Figure 8 shows the biggest end-to-end delay is 0.508 s and the smallest is 0.312 s, The increase in delay due to signal reduction is caused by non-LOS testing which puts the appliance with access points in different rooms so that there is a wall barrier between them. The barrier makes attenuation that weakens the access signal points when received by the appliance [19, 20].

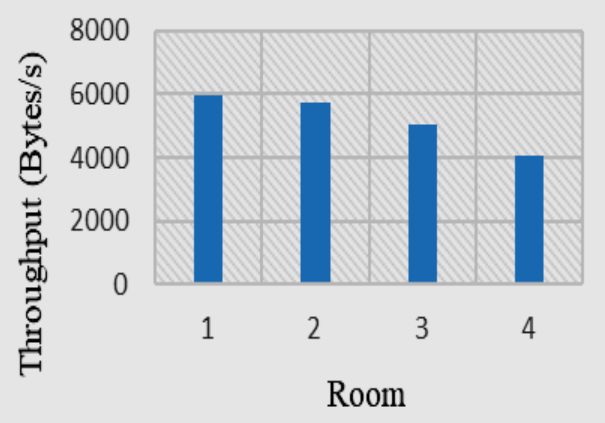


Figure 9. End to end Throughput Non-LOS.

Figure 9 shows the biggest end-to-end throughput is 5984.93 Bytes/sec and the smallest is 4044.76 Bytes/sec, The decrease in throughput due to signal reduction is caused by non-LOS testing which puts the appliance with access points in different rooms so that there is a wall barrier between them. The barrier makes attenuation that weakens the access signal points when received by the appliance.

### *E. Whole System Testing*

Availability and reliability testing of the whole system is done by sending 1000 packets between raspberry pi and the firebase server. After that, the total observation time, uptime, and downtime data from each experiment will be taken.

TABLE VII. WHOLE SYSTEM TESTING.

| Test | Availability | Reliability | Test | Availability | Reliability |
|---|---|---|---|---|---|
| 1 | 97,38 | 97,31 | 16 | 98,06 | 98,02 |
| 2 | 96,88 | 96,78 | 17 | 95,77 | 95,59 |
| 3 | 95,08 | 94,82 | 18 | 95,97 | 95,80 |
| 4 | 97,02 | 96,93 | 19 | 96,31 | 96,17 |
| 5 | 99,19 | 99,18 | 20 | 97,87 | 97,82 |
| 6 | 97,61 | 97,55 | 21 | 96,59 | 96,47 |
| 7 | 95,09 | 94,84 | 22 | 96,14 | 95,98 |
| 8 | 97,78 | 97,73 | 23 | 96,69 | 96,58 |
| 9 | 98,68 | 98,67 | 24 | 98,45 | 98,43 |
| 10 | 96,88 | 96,78 | 25 | 96,54 | 96,42 |
| 11 | 99,34 | 99,33 | 26 | 98,90 | 98,89 |
| 12 | 99,24 | 99,24 | 27 | 97,84 | 97,80 |
| 13 | 95,61 | 95,41 | 28 | 96,08 | 95,92 |
| 14 | 98,77 | 98,75 | 29 | 97,90 | 97,85 |
| 15 | 98,51 | 98,49 | 30 | 99,59 | 99,59 |

Table VII shows the average of availability value obtained from this test is 97.39% while for reliability is 97.30%. Changes in the value of each experiment always change due to the quality of the network which is also always changing.

### *F. Features Testing*

In the Door Bel Feature, when you call the arrival of guests who are in front of the door, guests can notify the user by pressing the provided button next to the keypad. When the button is pressed, the tool will take a picture from the guest and send it to the web server. Images are sent to the web server database instead of Firebase so that users can open images via a link from the image via the application. In addition to images, the system will also send notifications to users whose contents notify the user of the arrival of guests.

While the live stream feature serves as a support for the alarm feature which aims to allow users to see in real time the conditions in which the device is placed when an alarm notification appears in the user's application. There is also a button on the tool so users can turn off and turn on this live stream feature. In addition, users can also view videos from the previous live stream on the "my video" menu on the YouTube web page. The choice of YouTube as a streaming server is because Youtube has a size that is large enough to hold live stream videos.

Feature testing is performed 30 times at an applicable distance of 5 meters. the result of the test is the average throughput for sending images is 130,516 Bytes / seca or 130.51 Kbytes / sec while for the average delay in testing is 0.008 seconds or 8 ms. while for the average delay for the live stream feature is 0.006795497 seconds or 6 ms. While for the average throughput the live stream feature is 457000 Bytes / sec or 457 KBytes / sec.

## V. CONCLUSION

Based on the results of test obtained, it can be concluded that the distance and the presence or absence of barriers between devices with access points can affect the value of delay and throughput, different from testing applications which are not influenced by distance and barrier but based on differences in network quality used, if access points are placed at 10 meters and without a barrier, the value obtained will be more optimal, and for the features testing all features can work so well.

## REFERENCES

[1] M. P. Peeters, "Assessing the vulnerability of targets for burglary. Creating a multi-level observational instrument.," 2013.
[2] N. Gupta, R. Mandal and V. Chadda, "Internet of Things based Door Locking -An Architecture," IJCTA, vol. 9, no. 20, pp. 385-390, 2016.
[3] W. K. Pratiwi, "2018, Pasar Smartphone Indonesia Tumbuh Dua Digit," Tekno Kompas, 2019.
[4] H. H. Wilmer, L. E. Sherman and J. M. Chein, "Smartphones and Cognition: A Review of Research Exploring the Links between Mobile Technology Habits and Cognitive Functioning," Frontiers in Psychology, 2017.
[5] A. I. Nugraha, "FACTORS AFFECTING USE OF SMARTPHONE IN STUDENTS LEARNING ACTIVITIES," Yogyakarta, 2018.
[6] J. H. Chang, "An introduction to using QR codes in scholarly journals," vol. I, 2014.

[7] J. Coleman, "QR Codes: What Are They and Why Should Care?," Kansas State University, Kansas, 2011.
[8] V. P.S, M. W.N, S. V. G and D. N. Harini, "SECURING IoT DEVICES BY GENERATING QR CODES," International Journal of Pure and Applied Mathematics, India, 2018.
[9] G. A. Prakasa, "Prototype Sistem Kunci Pintu Berbasis QR Code dan Arduino," Universitas Muhammadiyah, Surakarta, 2017.
[10] G. Sowmya, G. D. Jyothi, N. Shirisha, K. Navya and B. Padmaja, "Iot Based Smart Door Lock System," pp. 224-225, 2018.
[11] M. Khatu, N. Kaimal, P. Jadhav and S. A. Rizv, "Implementation of Internet of Things for Home Automation," Sryahwa Publication, Maharashtra, 2015.
[12] P. Tambare and P. Venkatachalam, "Internet Of Things Based Intelligent Street Lighting System for Smart City," International Journal of Innovative Research in Science, Engineering and Technology , Kerala, 2016.
[13] S. Winardi, Firmansyah and W. A. Kristiana, "Rancang Bangun Sistem Pengaman Pintu Rumah Menggunakan Android Berbasis Arduino Uno," pp. 98-104, 2016.
[14] J. H. A. I. S. Nazrul Islam, "Quality of Service Analysis of Ethernet Network Based on Packet Size," Bangladesh, 2016.
[15] Fatoni, "Analisis Kualitas Layanan Jaringan Intranet," Universitas Bina Darma, Palembang.
[16] H. Fahmi, "Analisis QOS (Quality Of Service) Pengukuran Delay, Jitter, Packet Lost, dan Throughput Untuk Mendapatkan Kualitas Kerja Radio Streaming Yang Baik," Jurnal Teknologi Informasi dan Komunikasi, Medan, 2018.
[17] R. A. Andam, Sudarno and Suparti, "Kajian Reliabilitas dan Availabilitas," Jurnal Gaussian, pp. 244-252, 2014.
[18] R. Ridho, "Analisis dan Implementasi Smart Home Security System Berbasis IoT," Universitas Telkom, 2017, 2017.
[19] M. S. Akbar, H. Yu and S. Chang, "Delay, Reliability, and Throughput Based QoS Profile: A MAC Layer Performance Optimization Mechanism for Biomedical Applications in Wireless Body Area Sensor Networks," Hindawi Publishing Corporation, Bournemouth, 2016.
[20] S. Saraswat and G. Yadava, "An overview on Reliability, Availability, Maintainability and Supportability (RAMS) Engineering," Indian Institute of Technology, Delhi, 2008.