Security system with RFID control using E-KTP and internet of things

Andi Ainun Najib, Rendy Munadi, Nyoman Bogi Aditya Karna
School of Electrical Engineering, Telkom University, Indonesia

Article Info

Article history:

Received Jan 30, 2021
Revised Mar 30, 2021
Accepted Apr 8, 2021

Keywords:

Android application
E-KTP
Firebase
Internet of things
NodeMCU V3 ESP8266
PIR sensor
Push notification
RFID sensor

ABSTRACT

Crimes against property without using violence, in this case, are theft and burglary is the type of crime that is most common every year. However, home security needs a security system that is more efficient and practical. To overcome this, an internet of things (IoT) is needed. This research evaluated the performance prototype by reading distance from the radio frequency identification (RFID) reader using E-KTP and quality of service performance (i.e throughput and delay) from application android. This research design smart door lock using RFID sensor, passive infrared sensor (PIR), solenoid as door locks, buzzer, led, E-KTP as RFID tags and also android application to controlling and monitoring made with android studio is connected to NodeMCU V3 ESP8266 as storage data and connect with firebase realtime database instead of conventional keys. This research focuses on performance prototype and quality of service from features application is work well. Related to previous works, our evaluation shows that the performance prototype can read identity card (E-KTP) with a maximum distance is 4 cm, and performance quality of service for an application show that throughput and delay with a perfect index according to standardization telecommunications and internet protocol harmonization over network (TIPHON) depending on what features are being evaluated.

Corresponding Author:

Rendy Munadi
School of Electrical Engineering
Telkom University
Jl. Telekomunikasi, Terusan Buah Batu, Bandung 40257, Indonesia
Email: rendymunadi@telkomuniversity.ac.id

1. INTRODUCTION

In this era of technology, the internet of things (IoT) helps a lot in connecting several devices. IoT can be defined as a global infrastructure that enables advanced services by interconnecting [1]. IoT is the interconnection amongst devices via internet, and it enables those devices to send and receive data [2]. IoT become major interest as results of technology development and industry [3]. With the technological development, the demand for smart things is drastically increased in daily-life. The IoT is one of the major components that provide a facility to interact with IoT-enabled devices [4]. The application of IoT has been widely implemented in every sector such as security systems [5], [6], industry [7], [8], agriculture [9]-[11], E-commerce [12], and medicine [13]-[15]. Internet of things can also be used as a controlling, and monitoring home. Home security is a very important feature of home automation and maybe the most crucial one [16], the security level in the home becomes more important and enhanced system always [17], home security system is now paramount because family and home property needs a secure place and safe. Houses and its surroundings must be fully protected from malicious disturbances [18]. However, home security still uses a conventional key, and using a conventional key is not safe from crime. the crime of theft without the use of force like theft and burglary is the type of crime that is the most numerous in terms of number each year [19]. According to the Central Bureau of Statistics, during the period 2011-2018, the type of theft incident was a crime the most common in villages in Indonesia, the number reaching more than 36-45% of all villages. The percentage of villages that experienced thefts in the 2011-2018 period continued to increase. In 2011, 36.78% of villages experienced thefts. In 2014 this figure increased to 41.05% and in 2018 to 45.01% [19].

Based on the research and analysis of home door security system that is being faced by every housing in the capital city, the proposed solution for home security is to design a prototype of home door security system using a radio frequency identification (RFID) system from E-KTP that use a microcontroller as a doormap in a door-based digital home security system [20]. The use of E-KTP as an RFID tag because the function of E-KTP is still minimal and only use for a unique and authentic identity of the population in Indonesia [21]. Identity card (E-KTP) have near field communication (NFC) technology inside it. NFC is a short-range radio technology that allows communication between devices by touching each other or holding adjacent devices [22]. It is a new technology safer than standard RFID [23], E-KTP conforms to ISO 7810 with a format the size of a credit card, namely 53.98 mm x 85.60 mm. Data storage on the chip is in accordance with international standards national institute of standars and technology interagency report (NISTR) 7123 and machine readable travel documents international civil aviation organization (ICAO) 9303 and european union (EU) passport specification 2006. Based on the international standard organization/international electrotechnical commission (ISO/IEC) 7810: 2003 manual, a card with the ISO/ICE 7810 standard is an identification card that belongs to the same smart card class. with a card with ISO/IEC 14443 standard which can be used as an identification card [24]. Various security system for smart door lock has been produced in smart door lock today. Table 1 summarizes the sensing, communication, and support system used by a few IoT-based smart door lock and general systems found in the literature. The purpose of the review was to study the common devices and sensors for the sensing system, options for the communication systems, and the features of the support system.

Table 1. Summary of selected IoT-based smart door lock

Authors	Sensing systems	Communication systems	Software support system
[20]	Arduino Uno, RFID Sensor	Wifi	Web Application
[25]	Arduino Uno, RFID, PIR, Light Sensor	N/A	N/A Only displayed on LCD
[26]	QR scanner, Rasberry pi 3 B+, Camera Pi	Wifi	Web
[27]	STC Single Chip Microcomputer, Module Bluetooth,	Bluetooth	Mobile terminal
[28]	Atmega2560, NFC Module	N/A	NFC Mobile
[29]	Rasberry Pi	Wifi, Bluetooth	Web Application, and Mobile Application

In this paper, the security system with RFID control using E-KTP and IoT using NodeMCU V3 ESP8266 as a microcontroller, RFID sensor, PIR sensor, solenoid, led, buzzer, relay. NodeMCU ESP8266 connects to the internet and uses firebase as a real-time database. Firebase is used to store serial number/unique identification data from E-KTP (UID), data from PIR sensors. Firebase realtime database is a cloud-hosted database. Data is stored as java script object notation (JSON) and synchronized in real-time to every connected client [30]. Communication of RFID is usually performed by a magnetic field, but once electrodes for electric capacitive coupling are used instead of coils for electromagnetic induction by the magnetic field between them, it is possible to read wearable RFID tags [31]. In the android application, it is connected to firebase and in the android application, there is an alert feature, an open feature, and a lock feature. where the open feature and the lock feature for controlling the prototype, and the alert feature to provide a push notification in the form of a warning when the PIR sensor detects movement around the prototype. This paper describes the design and measures performance prototype and an android application that use for system security home using E-KTP and android application.

2. RESEARCH METHOD

The prototype system security utilized a microcontroller base on NodeMCU V3 ESP8266. As depicted in Figure 1, NodeMCU V3 ESP8266 is connected to the internet and firebase real-time database. data on firebase stores serial number/UID data from E-KTP, PIR sensor data, and data for relay controllers. RFID sensor connected to the microcontroller for reading the serial number/UID on E-KTP, PIR sensor for detecting motion, led as a marker that the prototype is connected to wifi, the buzzer is used when the relay is successfully used it will output sound output, and relays for solenoid controllers. Figure 2(a), gives a view of the prototype from the front, and Figure 2(b), gives a view of the prototype from behind.

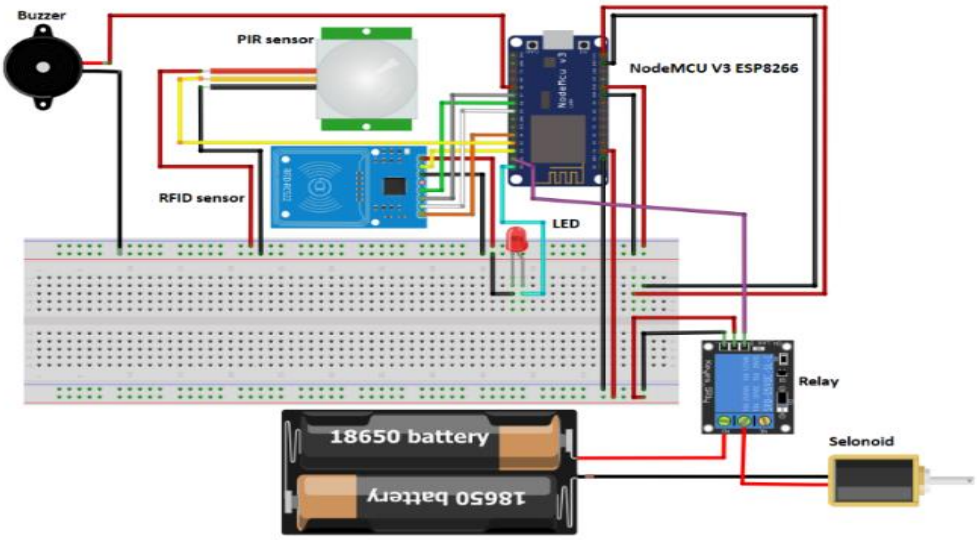
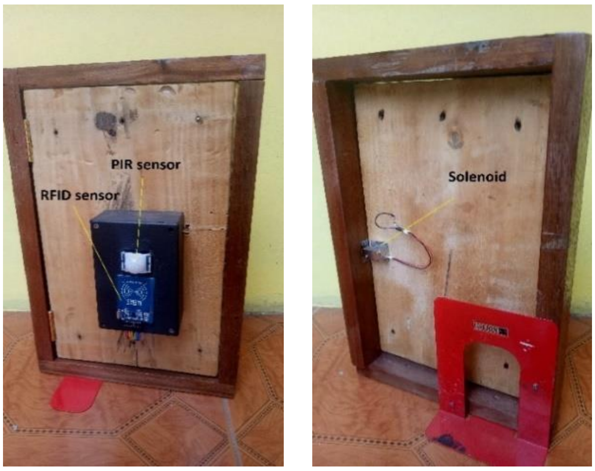


Figure 1. Integration of component prototype system security

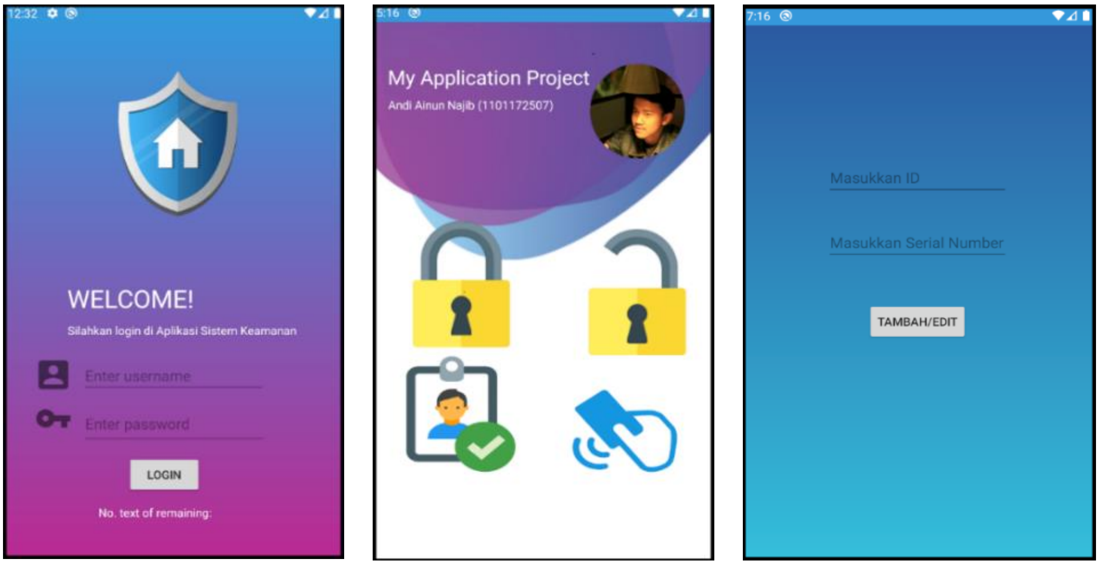


(a) (b)

Figure 2. Design prototype, (a) Prototype design from the front, (b) Prototype design from the behind

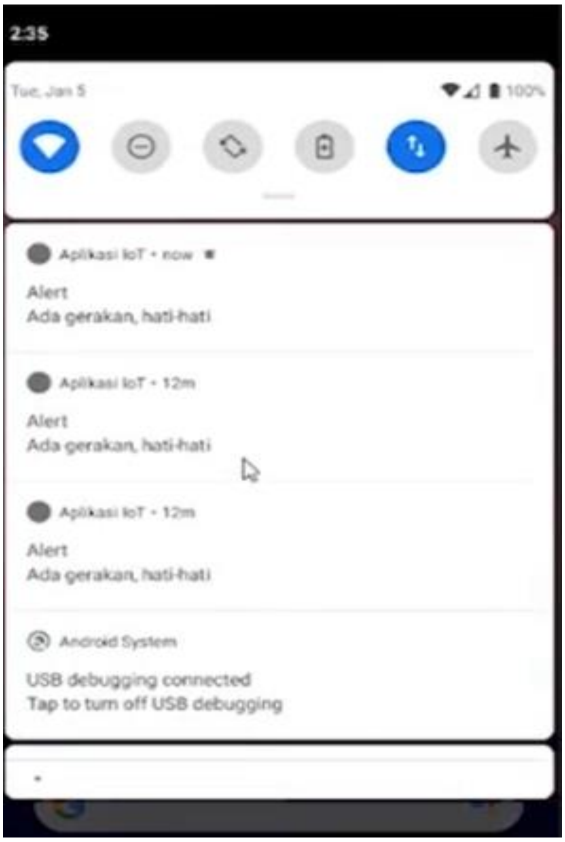
Figure 3(a) and (b) show the user login activity and control activity. In the application there are three features. Lock feature to control the relay and deactivate the solenoid so that the door is closed, an open feature to control the relay and activate the solenoid so that the door opens, and alerts feature to activate the alarm system and provide information if there is movement in the room when the house owner is not around at home. Figure 3(c), in the application user, can add and change the serial number stored on the firebase manually by entering the serial number in the insert and edit activity. As shown in Figure 4, the alert feature sends push notifications based on PIR sensor data via the android application. As shown in Figure 5, firebase provides functionality like, database store data serial number of E-KTP that registered, data from PIR sensor, and data to control relay from android application.

Figure 6(a) illustrates the measurement of the RFID output test for the prototype by collecting data in the form of reading the RFID reader on the E-KTP, when the registered E-KTP card was detected, the solenoid was open. Figure 6(b) in the android application, data collection is carried out in the form of quality of service (QoS) when the open feature is activated, the lock feature is activated, and QoS data collection is in the alert feature of the push notification sender. Tables 2 and 3 shows QoS parameters that uses for testing android application is throughput and delay.



(a) (b) (c)

Figure 3. Android application, (a) Login activity, (b) Control activity, (c) Edit and insert serial number/UID activity


2:35

Tue, Jan 5 100%

Aplikasi IoT • now

Alert
Ada gerakan, hati-hati

Aplikasi IoT • 12m

Alert
Ada gerakan, hati-hati

Aplikasi IoT • 12m

Alert
Ada gerakan, hati-hati

Android System

USB debugging connected
Tap to turn off USB debugging

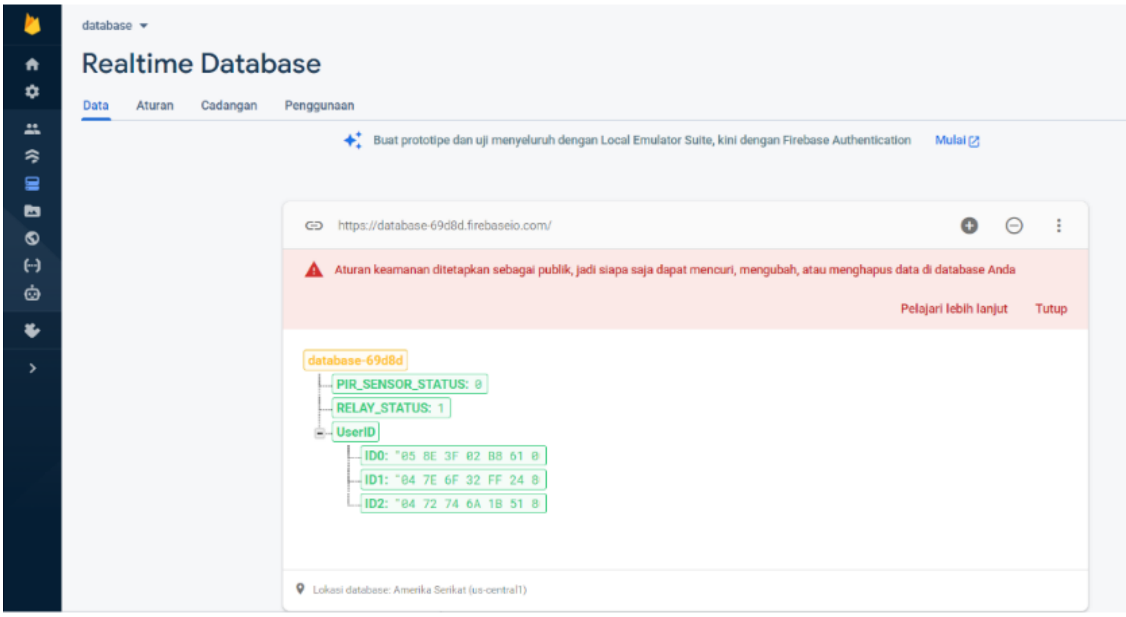
Figure 4. Push notification from android application

Table 2. Throughput categories

Throughput categories	Throughput (bps)	Indeks
Perfect	100	4
Good	75	3
Medium	50	2
Poor	<25	1

Table 3. Delay categories

Throughput categories	Delay (ms)	Indeks
Perfect	<150 ms	4
Good	150 - 300 ms	3
Medium	300 - 450 ms	2
Poor	> 450 ms	1



Buat prototipe dan uji menyeluruh dengan Local Emulator Suite, kini dengan Firebase Authentication

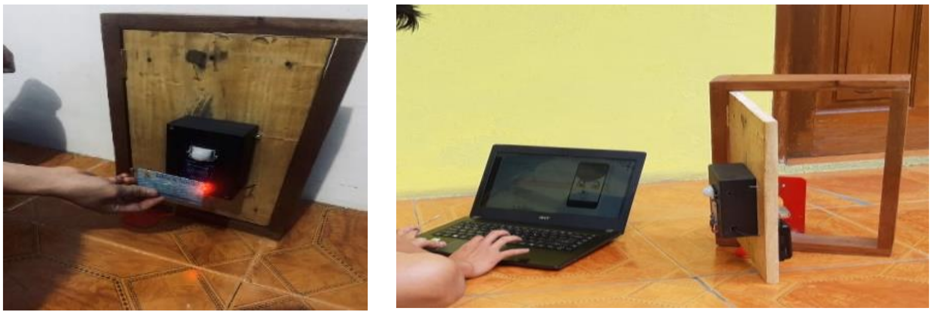
https://database-69d8d.firebaseio.com/

Aturan keamanan ditetapkan sebagai publik, jadi siapa saja dapat mencuri, mengubah, atau menghapus data di database Anda

```
database-69d8d
├─PIR_SENSOR_STATUS: 0
├─RELAY_STATUS: 1
└─UserID
   ├─ID0: "05 8E 3F 02 B8 61 0
   ├─ID1: "04 7E 6F 32 FF 24 8
   └─ID2: "04 72 74 6A 1B 51 8
```

Lokasi database: Amerika Serikat (us-central1)

Figure 5. Firebase platform



(a) (b)

Figure 6. Testing, (a) Measurement of RFID output, (b) QoS performance of android application open feature, lock feature, and alert feature

3. RESULTS AND DISCUSSION

Data were collected by recording the performance of prototype and android applications. Parameters for prototype testing are the reading distance from the RFID reader, and the QoS parameters for testing android applications are throughput and delay.

3.1. Measurement of RFID output

Table 4 measurement of RFID output using 3 E-KTPs from Andi Ainun Najib, Astrid Maydiana, and Khoir Mu'arif were used as registered E-KTPs that serial number of E-KTPs is stored on firebase. the performance of the prototype through reading the E-KTP with an RFID reader using a certain distance without being blocked by any material, and can send E-KTPs data to NodeMCU ESP8266 to what extent can be read by the system. Table 5 present the result of prototype performance for reading E-KTPs registered that RFID reader can reach a maximum distance of 4 cm without being obstructed by any objects, there is no difference in the detection distance of the three E-KTPs used.

Table 4. Serial number of E-KTPs registered

E-KTP	Serial number
Andi Ainun Najib	05 8E 3F 02 B8 61 00
Astrid Maydiana	04 7E 6F 32 FF 24 80
Khoir Mu’arif	04 72 74 6A 1B 51 80

Table 5. Measurement of RFID output

Distance (cm)	E-KTP's Andi	E-KTP's Astrid	E-KTP's Khoir
0	Detected	Detected	Detected
0.5	Detected	Detected	Detected
1	Detected	Detected	Detected
1.5	Detected	Detected	Detected
2	Detected	Detected	Detected
2.5	Detected	Detected	Detected
3	Detected	Detected	Detected
3.5	Detected	Detected	Detected
4	Detected	Detected	Detected
4.5	Not detected	Not detected	Not detected

3.2. QoS performance of android application features open and lock

Table 6 shows QoS performance from the open and lock features activated. Data were collected with 30 experiments to get the average value of QoS for throughput and delay. Figure 7 showing the graph of throughput when open and lock features activated. Throughput more describes the number of successful packet arrivals observed during a certain time interval when the open and lock features activated, the average calculation result of 30 experiments, throughput is 18366.66667 bps with a perfect index based on the standard TIPHON. Figure 8 showing the graph of delay when open and lock features activated. Experiments by taking data as much as 30 times showed the average delay in the lock feature and the open feature was 65.26827336 ms. The delay value is in the range of 49.911 ms to 74.1709 ms so that the delay can be categorized as perfect because it is still vulnerable to <150 ms, based on standardization TIPHON.

Table 6. QoS performance of android application open and lock features

No	Throughput (bps)	Delay (ms)	No.	Throughput (bps)	Delay (ms)
1	27000	60.87786806	16	19000	65.54664388
2	27000	63.91853659	17	15000	67.09237267
3	22000	63.29394318	18	23000	62.59384362
4	13000	67.71182403	19	14000	67.87834391
5	23000	49.91183281	20	20000	62.73843824
6	16000	74.17090445	21	19000	66.89283746
7	11000	66.97773593	22	23000	60.98343621
8	28000	54.87999099	23	13000	68.23434921
9	12000	67.66569118	24	19000	70.23434820
10	15000	66.89841935	25	21000	63.02343222
11	12000	68.93743928	26	13000	66.93424722
12	18000	62.03943048	27	16000	70.20923338
13	13000	69.89218304	28	14000	68.92832276
14	21000	64.45472982	29	18000	67.34368908
15	22000	64.23484378	30	24000	63.54928983
			Average	18366,66667	65,26827336

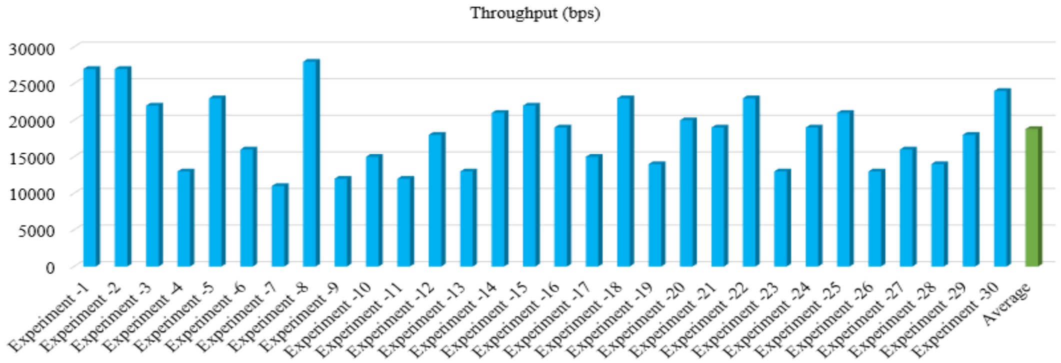


Figure 7. The graph of throughput when open and lock features activated

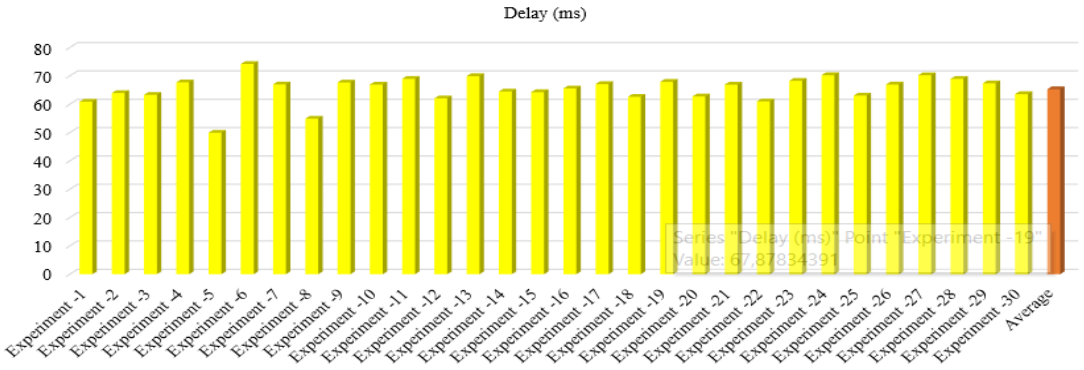


Figure 8. The graph of delay when open and lock features activated

3.3. QoS performance of android application feature alert

QoS performance of android application feature alert in Table 7. Testing is done by providing movement around the device when the PIR sensor detects motion, the android application provides a notification to the android application. Figure 9, describes the number of successful packet arrivals observed when the alert feature is activated during a certain time interval in the alert feature, based on the calculation of the average throughput for the alert feature is 18066.6667 bps, with a perfect index based on standardization TIPHON. Figure 10, experiments by taking data 30 times showed the highest delay was at 75.8353 ms and the lowest was at 49.9182 ms. Based on the calculation results, the average delay is 67.2354995 ms. Delay is categorized as perfect because it is at vulnerable <150 ms, seeing the standardization TIPHON.

Table 7. QoS performance of android application alert feature

No	Throughput (bps)	Delay (ms)	No	Throughput (bps)	Delay (ms)
1	19000	68.71457483	16	26000	61.86453642
2	24000	71.68914741	17	21000	64.63453628
3	11000	72.60040206	18	12000	74.00432483
4	32000	63.04479528	19	18000	66.76422532
5	17000	72.81192657	20	19000	65.92735233
6	14000	67.92497321	21	24000	63.46829375
7	16000	65.69452381	22	13000	66.82363443
8	11000	73.07024252	23	28000	56.73253524
9	12000	74.09588612	24	11000	74.53738464
10	23000	62.03836253	25	27000	60.03937622
11	12000	65.98364623	26	12000	75.83534232
12	19000	69.83645273	27	22000	63.28347663
13	21000	63.64826261	28	23000	49.91823626
14	16000	65.78363529	29	16000	74.17043437
15	12000	71.02374726	30	11000	71.10071761
			Average	18066,66667	67,2354995

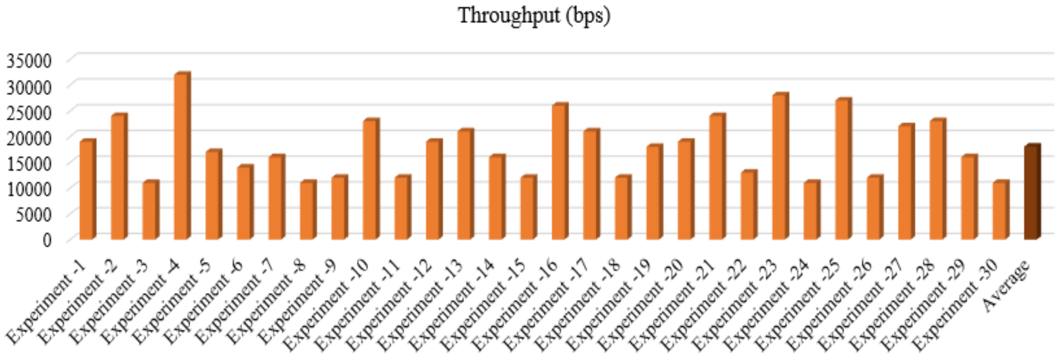


Figure 9. The graph of Throughput when alert feature activated

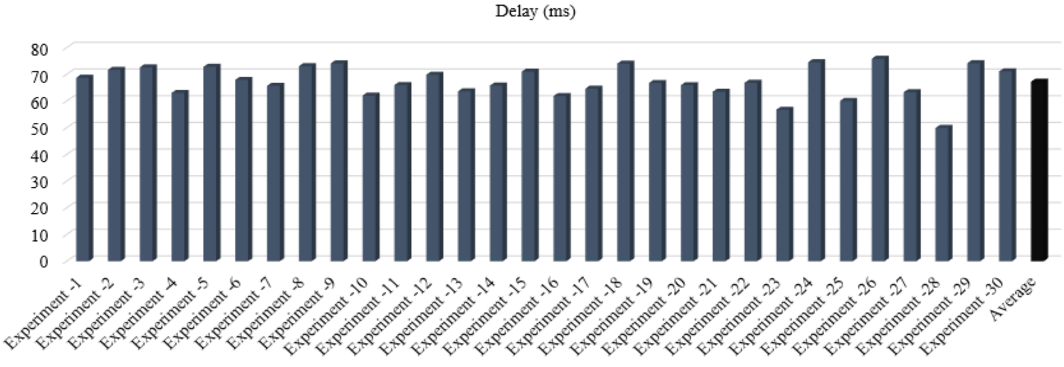


Figure 10. The graph of delay when feature activated

4. CONCLUSION

This paper describes the design and measures performance prototype and an android application that use for system security home using RFID sensor and PIR sensor. The prototype using to detect E-KTP as an RFID tag, and detecting motion, and send motion data to firebase, the application used for monitoring and controlling prototype by android. In this paper, we evaluated the performance prototype by reading distance from the RFID reader and QoS performance (*i.e* throughput and delay). The maximum distance RFID reader can detect E-KTP is 4 cm without being obstructed by any object, the prototype work perfectly detects E-KTP registered in firebase real-time database. The android application had been developed to ease the user in monitoring that is alert feature gives push notification base on PIR sensor and controlling the prototype by lock and open feature that control relay. For the android application, QoS performance for open and lock features, throughput is 18366.66667 bps with a perfect index based on the standard TIPHON, and delay is 65.26827336 ms. The delay value is in the range of 49.911 ms to 74.1709 ms so that the delay can be categorized as perfect because it is still vulnerable to <150 ms, based on standardization TIPHON. QoS performance for alert feature send push notification throughput is 18066.6667 bps, with a perfect index based on standardization TIPHON, and delay is 67.2354995 ms. Delay is categorized as perfect because it is at vulnerable <150 ms, seeing the standardization TIPHON. From the results obtained, the prototype and android application work well as a security system using E-KTP and IoT.

REFERENCES

[1] X. Li and L. Da Xu, "A Review of Internet of Things-Resource Allocation," *IEEE Internet Things Journal*, 2020, doi: 10.1109/jiot.2020.3035542.

[2] M. Husni, H. T. Ciptaningtyas, R. R. Hariadi, I. A. Sabilla, and S. Arifiani, "Integrated smart door system in apartment room based on internet," *TELKOMNIKA Telecommunication Computing Electronics Control*, vol. 17, no. 6, pp. 2747-2754, 2019, doi: 10.12928/TELKOMNIKA.V17I6.12322.

[3] Taryudi, D. B. Adriano, and W. A. Ciptoning Budi, "Iot-based Integrated Home Security and Monitoring System," *Journal of Physics: Conference Series*, vol. 1140, no. 1, pp. 0-7, 2018, doi: 10.1088/1742-6596/1140/1/012006.

[4] R. Sarmah, M. Bhuyan, and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 59-63, doi: 10.1109/WF-IoT.2019.8767229.

[5] Tina, Sonam, Harshit, and M. Singla, "Smart Lightning and Security System," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777632.

[6] K. Agarwal, A. Agarwal, and G. Misra, "Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT," *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 629-633, 2019, doi: 10.1109/I-SMAC47947.2019.9032629.

[7] S. K. Panda, A. Blome, L. Wisniewski, and A. Meyer, "IoT Retrofitting Approach for the Food Industry," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2019, vol. 2019-Septe, pp. 1639-1642, doi: 10.1109/ETFA.2019.8869093.

[8] I. B. Aris, R. K. Z. Sahbusdin and A. F. M. Amin, "Impacts of IoT and big data to automotive industry," *2015 10th Asian Control Conference (ASCC)*, Kota Kinabalu, Malaysia, 2015, pp. 1-5, doi: 10.1109/ASCC.2015.7244878.

[9] R. A. Kjellby, L. R. Cenkeramaddi, A. Frøytlog, and B. B. Lozano, "Kjellby, Rolf A.; Cenkeramaddi, Linga R.; Froytlog, Anders; Loza," 2*019 IEEE 5th World Forum on Internet of Things (WF-IoT'19)*-Limerick, Ireland (2019.4.15.pdf," pp. 545-549, 2019, doi 10.1109_WF-IoT.2019.8767196.

[10] V. Puranik, "Proceedings - 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, IoT-SIU 2019," *Proceedings-2019 4th International Conference Internet Things Smart Innovation Usages, IoT-SIU 2019*, pp. 1-6, 2019.

[11] M. U. H. Al Rasyid, S. Sukaridhoto, M. I. Dzulqornain, and A. Rifa'i, "Integration of IoT and chatbot for aquaculture with natural language processing," *TELKOMNIKA Telecommunication Computing Electronic Control*, vol. 18, no. 2, pp. 640-648, 2020, doi: 10.12928/TELKOMNIKA.V18I2.14788.

[12] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, India, 2015, pp. 1577-1581, doi: 10.1109/ICGCIoT.2015.7380718.

[13] S. S. Chavan, C. Fernandes, P. R. Dumane, and S. L. Varma, "Design and Implementation of Automatic Coin Dispensing Machine," *Lecture Notes in Electrical Engineering*, vol. 570, pp. 379-385, 2020, doi: 10.1007/978-981-13-8715-9_46.

[14] M. Srinivas, P. Durgaprasadarao and V. N. P. Raj, "Intelligent medicine box for medication management using IoT," *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2018, pp. 32-34, doi: 10.1109/ICISC.2018.8399097.

[15] E. I. Agustin, R. T. Yunardi, and A. A. Firdaus, "Voice recognition system for controlling electrical appliances in smart hospital room," *Telkomnika (Telecommunication Computing Electronic Control*, vol. 17, no. 2, pp. 965-972, 2019, doi: 10.12928/TELKOMNIKA.V17I2.11781.

[16] A. Anitha, "Home security system using internet of things," *IOP Conference Series: Materials Science and Engineering*, vol. 263, no. 4, p. 042026, Nov. 2017, doi: 10.1088/1757-899X/263/4/042026.

[17] Z. G. Faisel, M. S. Hussein, and A. M. Abood, "Design and realization of motion detector system for house security," *Telkomnika (Telecommunication Computing Electronic Control*, vol. 17, no. 6, pp. 3211-3217, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13142.

[18] I. V. Paputungan, M. R. Al Fitri and U. Y. Oktiawati, "Motion and Movement Detection for DIY Home Security System," *2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies (CSUDET)*, Penang, Malaysia, 2019, pp. 122-125, doi: 10.1109/CSUDET47057.2019.9214684.

[19] B. P. Statistika, *Statistik Kriminal 2020*, 2020th ed. BPS-Statistics Indonesia, 2020.

[20] M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto, and R. A. Pramono, "e-KTP as the basis of home security system using arduino UNO," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 2017, pp. 1-5, doi: 10.1109/CAIPT.2017.8320693.

[21] Badan Pengkajian dan Penerapan Teknologi, "E-KTP, Unique and Authentic Citizen Identity (in bahasa: E-KTP, Identitas Penduduk Yang Unik Dan Otentik," Badan Pengkajian dan Penerapan Teknologi. [Online]. Available: https://www.bppt.go.id/profil/sejarah/848-e-ktp-identitas-penduduk-yang-unik-dan-otentik. [Accessed: 11-Feb-2020].

[22] R. M. Awangga, N. H. Harani, and M. Y. H. Setyawan, "KAFA: A novel interoperability open framework to utilize Indonesian electronic identity card," *TELKOMNIKA Telecommunication Computing Electronic Control,* vol. 17, no. 2, pp. 712-718, 2019, doi: 10.12928/TELKOMNIKA.V17I2.11755.

[23] R. M. Awangga, N. H. Harani, and M. Y. H. Setyawan, "KANSA: High interoperability e-KTP decentralised database network using distributed hash table," *TELKOMNIKA Telecommunication Computing Electronic Control*, vol. 17, no. 3, pp. 1360-1366, 2019, doi: 10.12928/TELKOMNIKA.V17I3.11758.

[24] E. Saputro, "Design of Automatic Door Security Using E-KTP Based on Microcontroller Atmega328 (in bahasa: Rancang Bangun Pengaman Pintu Otomatis Menggunakan E-KTP Berbasis Mikrokontroler Atmega328)," *Journal Tenik Elektro Unnes*, vol. 8, no. 1, pp. 1-4, 2016, doi: 10.15294/jte.v8i1.8787.

[25] L. Kamelia, M. R. Effendi, and D. F. Pratama, "Integrated Smart House Security System Using Sensors and RFID," in *2018 4th International Conference on Wireless and Telematics (ICWT)*, 2018, pp. 1-5, doi: 10.1109/ICWT.2018.8527803.

[26] A. F. M. Fauzi, N. N. Mohamed, H. Hashim and M. A. Saleh, "Development of Web-Based Smart Security Door Using QR Code System," *2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, Shah Alam, Malaysia, 2020, pp. 13-17, doi: 10.1109/I2CACIS49202.2020.9140200.

[27] Z. Mu, W. Li, C. Lou and M. Liu, "Investigation and Application of Smart Door Locks based on Bluetooth Control Technology," 2*020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, Dalian, China, 2020, pp. 68-72, doi: 10.1109/IPEC49694.2020.9115189.

[28] J. Pacheco and K. Miranda, "Design of a low-cost NFC Door Lock for a Smart Home System," *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Vancouver, BC, Canada, 2020, pp. 1-5, doi: 10.1109/IEMTRONICS51293.2020.9216409.

[29] V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga and S. Bojewar, "Intelligent security lock," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, Tirunelveli, India, 2017, pp. 713-716, doi: 10.1109/ICOEI.2017.8300795.

[30] Y. A. Dharma and R. Tanone, "MSME Recommendation Application using Collaborative Filtering Method and Realtime Database (Case Study: Salatiga City)," *2018 International Conference on Electrical Engineering and Computer Science (ICECOS)*, Pangkal, Indonesia, 2018, pp. 361-366, doi: 10.1109/ICECOS.2018.8605190.

[31] T. Washiro, "HF RFID transponder with capacitive coupling," in *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*, 2017, pp. 12-15, doi: 10.1109/RFID-TA.2017.8098880.

BIOGRAPHIES OF AUTHORS

Andi Ainun Najib obtained B. Eng degrees in Telecommunication Engineering, from the Telkom University, Indonesia in 2021. He is interest in Internet of Things, and programming developer on android.

Rendy Munadi is professor in electrical engineering at Faculty of Electrical Engineering, Telkom University, Indonesia. He received his B. Eng and M. Eng degree in Electrical Engineering from Bandung Institute of Technology, in 1986 and 1997 and he received Doctor degree at Indonesia University, in 2005. Respectively in 2020 he is confirmedi as a professor or professor in the field of electrical engineering, Telkom University, Indonesia. His researcg interest in NwGN, QoS/QoE wireless network, VoIP.

Nyoman Bogi Aditya Karna obtained his B. Eng at STT Telkom, Indonesia, in 1996. He received his M. Eng at Northeastern University, Boston, in 1999. Now he is Senior Lecture on Computer Enggineering and Researcher on Intelligent IoT, Telkom University, Indonesia.