

Autentikasi Ganda pada Sistem *Smart Security Home* Menggunakan Sidik Jari dan *Near Field Communication*

Maya Rahayu¹, Arif Indra Irawan²

¹Jurusan Teknik Elektro, Politeknik Negeri Bandung

Jl. Gegerkalong Hilir, Ciwaruga, Kec. Parongpong, Kabupaten Bandung Barat, Indonesia

²Program Studi Teknik Telekomunikasi, Universitas Telkom

Jl. Telekomunikasi No. 1, Terusan Buahbatu - Kec. Dayeuhkolot, Bandung, Indonesia

mayarahayu@polban.ac.id

Abstrak

Dengan berkembangnya teknologi internet, banyak hal yang bisa dikontrol dari jauh, salah satunya sistem keamanan rumah. Proses autentikasi manual menggunakan kunci ataupun kartu pada pintu rumah memiliki resiko untuk hilang. Pada penelitian ini, dirancang dan diimplementasikan suatu sistem pengamanan rumah yang terdiri dari *Near Field Communication* (NFC) dan sensor sidik jari yang diintegrasikan dengan Arduino. NFC reader membaca tag NFC yang kemudian diharuskan memasukan *password* atau *user ID* yang kemudian hak aksesnya diautentikasi NFC reader, lalu pengguna menyentuh sensor sidik jari untuk autentikasi kedua. Lalu hasil autentikasi tersebut memicu engsel pintu otomatis untuk membuka kunci pintu rumah. Fungsi *buzzer* sebagai peringatan jika ada orang yang tidak memiliki akses dan mencoba untuk masuk ke dalam ruangan. Data tersebut kemudian dikirimkan ke kontroler Node MCU kemudian dikirimkan ke *platform* IoT yang digunakan sebagai *cloud database*. Data tersebut juga akan muncul pada *smart phone* pengguna. Berdasarkan hasil pengujian sistem dapat berfungsi dengan baik. Rata-rata *delay* pada sistem di bawah 20 ms dan rata-rata *throughput* yang didapatkan di atas 1500 bit/s.

Kata kunci: *Near Field Communication*, *Internet of Things* (IoT), pintu pintar

Abstract

With the development of internet of things technology, many things can be controlled and automated remotely, one of which is the home security system. It's just that the manual authentication process using a key or card on the door of the house has a risk of being lost. In this study, designed and implemented a home security system consisting of NFC on a smartphone and a fingerprint sensor integrated with Arduino. NFC reader reads the NFC tag from a smartphone that is required to enter a password or user ID, which then has the access right to be authenticated by the NFC reader, then the user touches the fingerprint sensor for second authentication. Then the authentication results trigger the automatic door hinge to unlock the house door. The buzzer functions as a warning if someone does not have access and tries to enter the room. The data is then sent to Node Mcu and then sent to the IoT platform which is used as a cloud database. The data will also appear on the user's smart phone. Based on the test results the system can function properly. The average delay on the system is below 20 ms and the average throughput obtained is above 1500 bit / s.

Keywords: *Near Field Communication*, *Internet of Things* (IoT), smart door

I. PENDAHULUAN

Secara umum, rumah kos atau bahkan sistem keamanan rumah masih menggunakan banyak kunci pintu konvensional di mana masih rentan terhadap pencurian [1] dan rentan untuk hilang bagi pengguna rumah yang pelupa. Berdasarkan laporan Statistik Kriminal 2017 di DKI Jakarta, pada 2016

ada 43.842 kasus kejahatan [2]. Berdasarkan data dari Badan Pusat Statistik, terlihat bahwa kasus pencurian telah terjadi di 229 desa di DKI Jakarta, dari semua kasus kejahatan, ini adalah salah satu kasus kriminal terbesar [2]. Oleh karena itu, diperlukan suatu sistem terintegrasi yang dapat mengatasi masalah ini. Salah satu cara untuk mengatasi masalah ini adalah dengan mengganti

kunci pintu sebelumnya. Sepanjang 2018, Canals mencatat bahwa pertumbuhan *smartphone* di Indonesia mencapai 17,1% dibandingkan dengan 2017, di mana pengiriman *smartphone* ke Indonesia mencapai 38 juta unit [3]. Tidak sedikit orang menggunakan *smartphone* sebagai media komunikasi paling efektif dan murah. Dengan ponsel pintar seseorang dapat mengirim pesan dalam bentuk suara, video dan gambar dengan waktu yang sangat cepat dan langsung [4]. Penggunaan ini membuat *smartphone* saat ini digunakan oleh semua umur dan kelompok sosial [5], di mana salah satu fitur pada *smartphone* adalah *Near Field Communication* (NFC), yang salah satu fungsinya adalah media pembayaran untuk e-toll. Digunakannya NFC pada e-toll karena dibandingkan *Radio Frequency Identification* (RFID), NFC lebih akurat. NFC memiliki jarak penginderaan yang kecil bila dibandingkan dengan RFID.

Berbagai penelitian telah dilakukan mengenai pemanfaatan NFC. Peneliti [6] telah memanfaatkan NFC untuk profiling pada sistem pencahayaan rumah pintar, sedangkan pada [7] telah membuat sistem *wearable* menggunakan gelang NFC yang dapat digunakan untuk sistem otomasi rumah jarak jauh. Penelitian [8] telah membuat integrasi pada *smart home project* menggunakan banyak sensor dan NFC. Pada [9] telah membuat sistem keamanan *smart home* dengan teknologi NFC dan HCE mode. Sistem untuk modularisasi sistem bantu belanja *online* juga telah dirancang menggunakan NFC [10]. Di sisi lain, penelitian [11] membuat penjadwalan peralatan menggunakan skema hibrid algoritma genetika dan optimasi *elephant herd* untuk respon permintaan perumahan. Selain itu, berbagai penelitian juga telah dilakukan memanfaatkan *fingerprint* untuk *smart home*. Seperti pada [12] yang telah menggunakan *fingerprint* untuk sistem kontrol *smart home* berdasarkan lokasi dalam ruangan dan estimasi. Penelitian [13] juga telah membuat prototipe rumah cerdas humanoid yang bisa dikendalikan menggunakan *natural language processing* dan *machine learning*. Pada penelitian [14] telah melakukan peningkatan keamanan otomasi rumah dimana mengintegrasikan sidik jari perangkat ke rumah pintar. Terakhir, [15] telah melakukan penelitian tentang peningkatan keamanan dalam manajemen rumah pintar melalui *multimodal biometric* dan *passcode*.

Pada penelitian ini, dirancang dan diimplementasikan suatu sistem pengamanan rumah yang terdiri dari NFC pada *smartphone* dan sensor sidik jari yang diintegrasikan dengan Arduino. NFC *reader* membaca *tag* NFC dari *smartphone* yang

diharuskan memasukan *password* atau *user ID* yang kemudian hak aksesnya diautentikasi NFC *reader*. Kemudian *user* menyentuh sensor sidik jari untuk autentikasi kedua. Lalu hasil autentikasi tersebut memicu engsel pintu otomatis untuk membuka kunci pintu rumah. Fungsi *buzzer* sebagai peringatan jika ada orang yang tidak memiliki akses dan mencoba untuk masuk ke dalam ruangan. Data tersebut kemudian dikirimkan ke Node MCU kemudian dikirimkan ke *platform IoT* yang digunakan sebagai *cloud database*. Data tersebut juga akan muncul pada *smart phone* pengguna.

II. METODE PENELITIAN

A. Perancangan Sistem

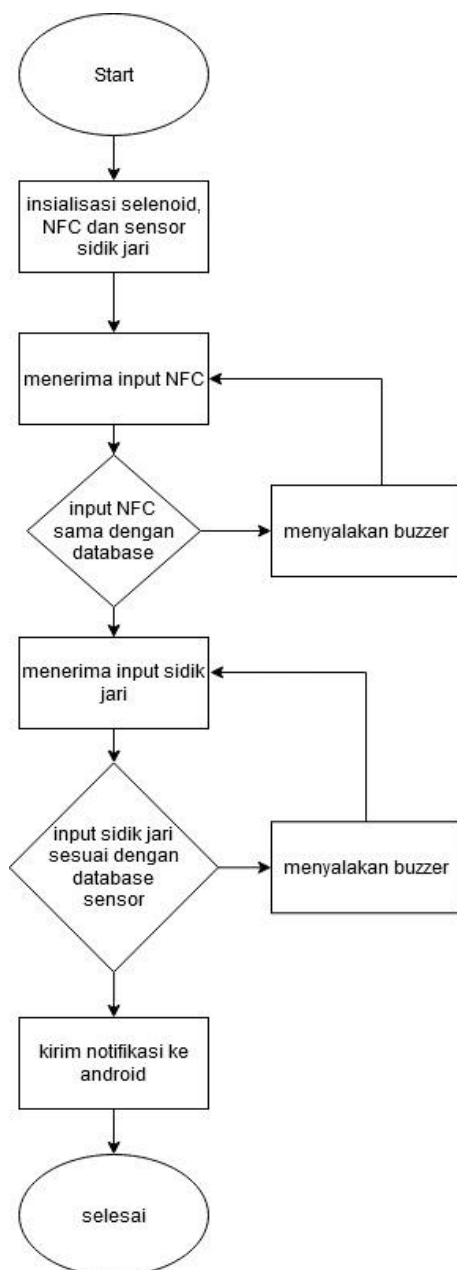
Pada dasarnya, sistem ini dirancang untuk melakukan autentikasi terhadap siapa saja yang akan masuk ke dalam *smart home*. Pada penelitian ini, dilakukan *two way authentication* menggunakan NFC pada *smartphone* dan menggunakan sidik jari. *Two way authentication* dilakukan agar keamanan lebih terjamin. Dengan sistem ini, pengguna dapat memasuki *smart home* hanya dengan *smartphone* pribadi milik pengguna dan dengan sidik jarinya. Dua autentikasi ini adalah barang pribadi milik pengguna yang hampir selalu dibawa kemana-mana oleh pengguna. Selain untuk autentikasi, sistem juga mencatat jam keluar masuk dari pemilik *smart home*, sehingga pemantauan dapat dilakukan dari pemilik rumah pertama ke pemilik rumah lainnya. Sistem ini dikontrol oleh NFC yang diaktifkan dari *smart home* dan sidik jari pengguna, yang akan menghasilkan sinyal input untuk menggerakkan *solenoid door lock* agar bisa membuka pintu rumah. Selain itu, perangkat lunak di *smartphone* juga menampilkan waktu masuk rumah dari tiap pengguna agar tiap pengguna *smart home* bisa saling memantau keberadaan satu sama lain.

Komponen yang di perlukan pada penelitian ini yaitu *smartphone* yang dilengkapi dengan fitur NFC dan NFC *shield* yang ditempatkan pada bagian *input*. Selain itu ada *fingerprint* juga diletakkan di bagian *input*. Arduino digunakan sebagai mini komputer pengolahan data, setelah itu data yang diproses Arduino akan dikirimkan ke server melalui Node MCU yang terhubung secara serial *Inter-Integrated Circuit* (I2C). Setelah itu data akan disimpan di *cloud database* yaitu Cloud, kemudian data tersebut dikirimkan ke *mobile application* yang dimiliki oleh admin ruangan.

Sistem yang dirancang prosesnya dimulai dari validasi *User Identification* (UID) yang dimasukkan pada NFC *smartphone* yang kemudian dibaca oleh NFC *shield* dan diperiksa apakah UID yang

diterima terdaftar dalam user yang memiliki hak akses atau tidak. Kemudian data tersebut diproses secara lokal melalui serial I2C. Validasi yang sama juga dilakukan pada saat penginputan *finger print*. Untuk kelengkapan, cara kerja dari sistem yang dirancang dapat dilihat pada Gambar 1. Dalam penelitian ini, sistem memiliki beberapa spesifikasi yang diharapkan sebagai berikut:

1. Dapat membuka pintu *smart home* yang diaktifkan menggunakan *solenoid door lock* dengan *two way verification*, yaitu dengan sidik jari dan NFC yang ada pada *smartphone* pengguna.
2. Sistem tidak dapat membuka *solenoid door lock* apabila salah satu dari perangkat masukan, yaitu NFC atau sidik jari tidak dapat diidentifikasi.



Gambar 1. Flowchart sistem

3. Apabila ada pengguna yang gagal terautentikasi, sistem segera memberi alarm kepada *smartphone* milik user dan membunyikan *buzzer* yang disimpan di dalam rumah.
4. Sistem dapat merekam dan menampilkan data waktu masuk dari tiap pengguna rumah pada *smartphone* tiap pengguna.

B. Perangkat Keras

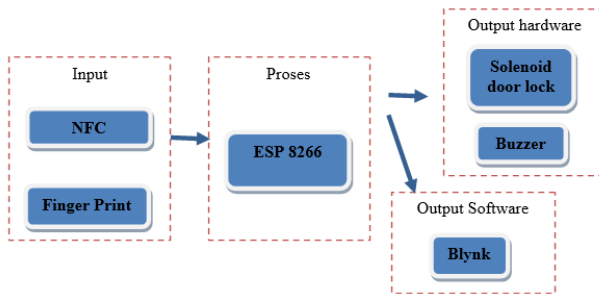
Perangkat keras yang dirancang pada penelitian ini dibuat untuk meningkatkan keamanan pada *smart home*. Perangkat keras yang digunakan terdiri dari *input*, *proses*, dan *output*. Pada bagian *input*, ada sensor sidik jari yang berfungsi sebagai salah satu identifikator dari pengguna *smart home*. Selain itu ada NFC sebagai *input* lainnya pada sistem untuk mengautentikasi pengguna. Kedua *input* tersebut harus diatur untuk memiliki logika AND, agar *solenoid door lock* baru akan terbuka bila kedua *input* mengautentikasi user *smart home* tersebut. Pada bagian perangkat pengontrol, terdapat Arduino yang berfungsi menerima sinyal dari NFC dan sensor sidik jari, memproses sinyal, serta mengirimkan sinyal ke perangkat *output*. Adapun perangkat *output* disini terdiri dari perangkat lunak dan perangkat keras. *Output* perangkat keras dari sistem ini diantara lain adalah *solenoid door lock* dan *buzzer*. *Solenoid door lock* berfungsi untuk membuka pintu *smart home* ketika sistem berhasil mengautentikasi pengguna. *Buzzer* berfungsi untuk memberikan peringatan pada orang-orang di dalam rumah apabila ada user yang gagal terautentikasi oleh sistem. Adapun *output* perangkat lunak pada sistem ini adalah menggunakan platform Blynk. Pada sistem ini, Blynk dirancang menggunakan beberapa *widget* untuk menampilkan waktu masuk rumah dari user yang telah berhasil terautentikasi, serta memberikan peringatan apabila ada user yang gagal terautentikasi. Hal ini dimaksudkan supaya pemilik rumah bisa waspada apabila ada orang tidak dikenal yang mencoba masuk rumah, walaupun pemilik rumah tidak sedang ada di rumah. Desain perangkat keras dalam penelitian ini dapat dilihat pada Gambar 2. Spesifikasi perangkat keras secara keseluruhan dapat dilihat pada Tabel 1. Dalam melakukan perancangan prototipe diperlukan berbagai komponen yang digunakan yang meliputi *hardware* sebagai berikut:

1. Arduino Uno

Pada sistem ini, Arduino Uno berfungsi untuk mengolah data validasi dari NFC dan *finger print*.

2. NFC Shield

NFC Shield berfungsi guna membaca *input* dari NFC *smartphone*.



Gambar 2. Diagram blok sistem

Tabel 1. Spesifikasi perangkat keras

Perangkat Keras	Spesifikasi	Keterangan
ESP 8266	Microcontroller	Tensilica 32 bit RISC CPU
	Operating Voltage	3.3 V
	Input Voltage	7-12 V DC
	Digital I/O Pin	16
	Analog Input Pin (ADC)	1
Android smart phone	Operating system	Android 10
	CPU	Octa-core (2x2.0 GHz Cortex-A75)
	RAM	6 Gb
	Internal Memory	128 Gb
Finger print sensor	Supply voltage	3,8-7,0 V DC
	Operating Current	< 65 mA
Solenoid Door Lock	Input voltage	12 V DC
	Input Current	2 A
Buzzer	Operating voltage	4-8 V DC
	Rated Current	< 30 mA
	Resonant Frequency	~2300 Hz
NFC Reader PN592	Voltage	3.3 ~ 5 V
	SPI	3.3 V TTL with 100 Ω in series
	Communication Distance	5 cm ~ 7 cm

3. Node MCU

Node MCU berfungsi untuk berkomunikasi secara I2C dan menerima data yang dikirimkan Arduino Uno dan meneruskan data yang sudah dikumpulkan ke *cloud*.

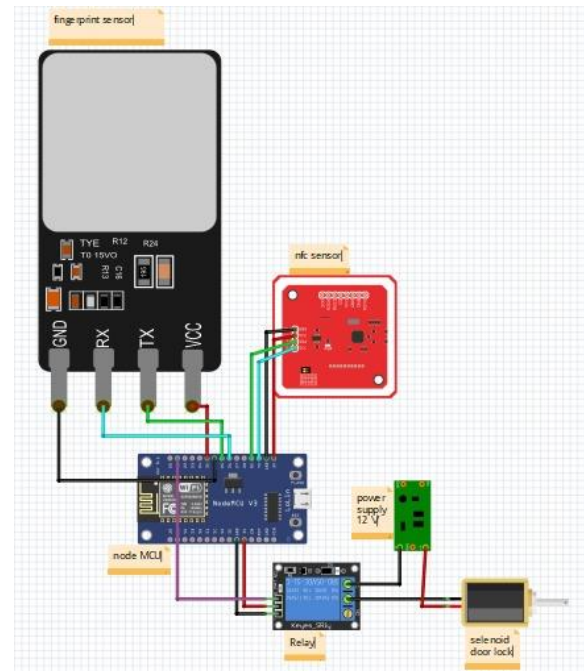
4. Solenoid Door Lock

Solenoid Door Lock berfungsi keluaran dari proses validasi keamanan menggunakan NFC dan *fingerprint*.

5. Buzzer

Buzzer berfungsi sebagai keluaran dari proses validasi sistem keamanan *smart home* menggunakan NFC dan *fingerprint*.

Adapun skematik rangkaian perangkat keras disajikan pada Gambar 3.



Gambar 3. Skematik rangkaian

C. Perangkat Lunak

Di bagian perangkat lunak, digunakan aplikasi android blynk sebagai antarmuka pengguna. Aplikasi ini dirancang untuk antarmuka *input* NFC pada *NFC reader*. Selain itu perangkat lunak digunakan untuk menampilkan data waktu pemilik *smart home* masuk rumah, serta menampilkan peringatan apabila ada orang yang gagal terautentikasi pada sistem.

Adapun perangkat lunak yang digunakan dalam sistem ini diantara lain adalah :

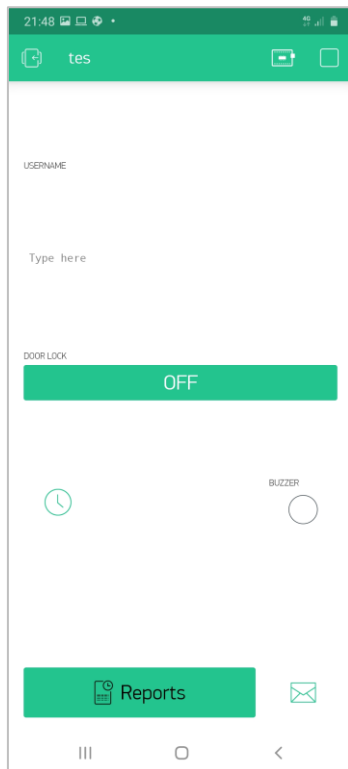
1. Arduino IDE

Arduino IDE digunakan pada computer untuk menuliskan program Arduino untuk memproses data masukan dari NFC dan fingerprint dan menjadi output untuk *buzzer*, *solenoid*, dan Blynk.

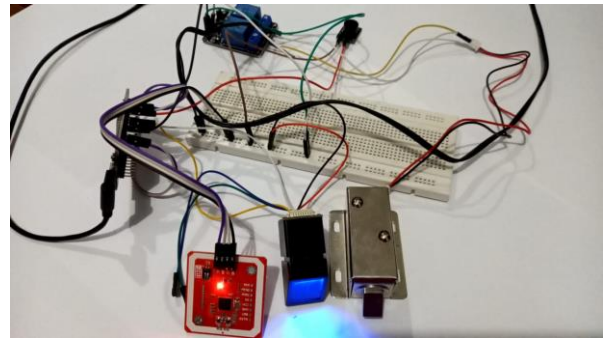
2. Blynk

Blynk adalah perangkat lunak untuk user agar dapat teridentifikasi NFC dan memantau dan melihat jam masuk dan keluar dari pemilik rumah yang telah terotentifikasi pada *smart home*.

Rancangan aplikasi yang dibuat dapat dilihat pada Gambar 4. Setelah dilakukan implementasi sistem, maka akan dilakukan pengujian. Adapun pengujian sistem dilakukan dengan fungsionalitas dan pengujian *Quality of Service* (QoS). QoS adalah kualitas layanan yang terdiri dari seperangkat parameter yang berkaitan dengan kinerja lalu lintas pada jaringan telekomunikasi. Adapun QoS yang diukur pada penelitian ini diantara lain adalah *delay*, *throughput*, dan *packet loss*.



Gambar 4. Perancangan aplikasi



Gambar 5. Implementasi sistem

Tabel 2. Hasil pengujian fungsionalitas sistem

Uji ke-	Conf.	User ID NFC	Two way authentication
1	238	04 17 D5 27 96 62 19	berhasil
2	231	04 17 D5 27 96 62 19	berhasil
3	228	04 17 D5 27 96 62 19	berhasil
4	195	04 17 D5 27 96 62 19	berhasil
5	202	04 17 D5 27 96 62 19	berhasil
6	196	04 17 D5 27 96 62 19	berhasil
7	221	04 17 D5 27 96 62 19	berhasil
8	235	04 17 D5 27 96 62 19	berhasil
9	183	04 17 D5 27 96 62 19	berhasil
10	226	04 17 D5 27 96 62 19	berhasil

Tabel 3. Pengujian QoS

Uji ke-	Delay (ms)	Packet Loss (%)	Throughput (bit/s)
1	6,045	0	6432,121
2	13,277	0	1364,374
3	20,981	0	732,945
4	18,398	0	868,976
5	15,044	0	1051,124
6	12,023	0	3258,098
7	19,732	0	799,923
8	12,543	0	2457,865
9	11,032	0	1112,928
10	16,554	0	1012,065

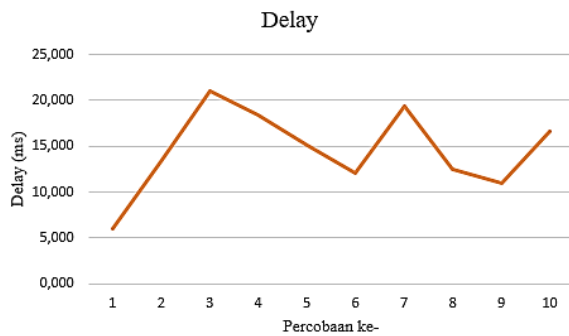
III. HASIL DAN PEMBAHASAN

Pada tahap ini, perangkat keras dan perangkat lunak diimplementasikan sesuai dengan desain yang telah dipaparkan sebelumnya. Hasil implementasi perangkat keras dan perangkat lunak aplikasi Android dapat dilihat pada Gambar 6. Setelah proses implementasi, lalu dilakukan pengujian sistem untuk melihat kinerja keseluruhan. Adapun pengujian yang dilakukan pada sistem ini meliputi pengujian fungsionalitas sistem serta pengujian QoS dengan parameter *delay*, *throughput*, dan *packet loss*.

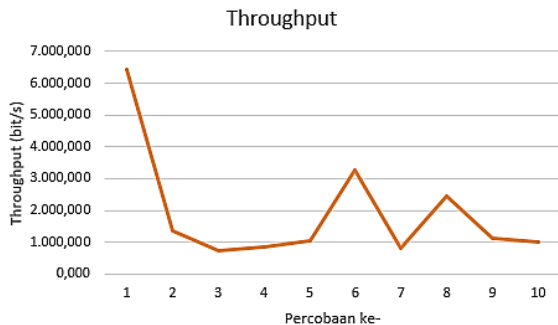
A. Pengujian Fungsionalitas

Pengujian fungsionalitas dilakukan sebanyak 10 kali dimana percobaan 1 sampai 10 dilakukan dengan waktu yang berbeda dengan jeda waktu 10 menit antar percobaan. Prosedur melakukan autentikasi adalah mendaftarkan sidik jari pengguna secara *offline* ke *FLASH memory* yang terdapat pada sensor sidik jari yang digunakan dengan total pengguna yang dapat disimpan mencapai 254 sidik jari, sedangkan proses pendaftaran dilakukan dengan menggunakan virtual pin yang ada pada Blynk dengan total maksimal 120 data NFC yang dapat disimpan. Percobaan pembacaan sensor sidik jari dilakukan secara *offline* tanpa terhubung ke internet, sedangkan pembacaan NFC dan *two way authentication* dilakukan secara daring ke server Blynk.

Adapun parameter yang dapat terlihat adalah *confidence level* dari sensor sidik jari. *Confidence level* adalah tingkat akurasi dari sensor sidik jari. Hasil pengujian ditampilkan pada Tabel 2. Dari 10 percobaan terhadap pengguna yang teregistrasi sistem mampu mendeteksi *two way authentication* dengan baik karena semua percobaan berhasil, dengan rata-rata *confidence level* pada sensor sidik jari 215,5.



Gambar 6. Grafik hasil pengujian delay



Gambar 7. Grafik hasil pengujian throughput

B. Pengujian Quality of Service (QoS)

Pengujian QoS terdiri dari beberapa parameter di dalamnya, diantara lain yaitu *delay*, *packet loss*, serta *throughput*. Hasil pengujian QoS dapat dilihat pada Tabel 3. Percobaan dilakukan dalam hari yang sama dengan interval 60 menit dari pukul 08.00-17.00 WIB untuk memantau kinerja pada tiap jam untuk mengetahui rata-rata kinerja walau di jam sibuk. Grafik pengujian *delay* dapat dilihat pada Gambar 6 dan grafik hasil pengujian throughput dapat dilihat pada Gambar 7.

Dari grafik hasil pengujian tersebut, terlihat *delay* paling tinggi ada pada percobaan ke-3 dan ke-7. Hal itu dikarenakan percobaan ke-3 dilakukan pada pukul 10.00 WIB dan percobaan ke-7 dilakukan pada pukul 13.00 WIB. Jam tersebut dianggap sebagai jam tersibuk dari jaringan yang digunakan, yaitu menggunakan Wi-Fi terhubung pada *Fiber To The Home* (FTTH) salah satu *provider* yang digunakan bersama.

Pada grafik hasil pengujian *throughput*, terlihat pada hasilnya yang berkebalikan dengan grafik *delay*. Semakin kecil *delay*, maka semakin besar *throughput* yang didapatkan. Hal ini selaras dengan rumus *throughput* di bawah ini [16]:

$$\text{Throughput} = \frac{\text{Jumlah data yang dikirim (bit)}}{\text{waktu pengiriman (s)}} \quad (1)$$

Semakin kecil *delay*, maka semakin besar *throughput* yang didapatkan. *Throughput* paling

besar didapatkan pada percobaan pertama di jam yang tidak sibuk, yaitu pukul 08.00, sedangkan *throughput* paling kecil ada pada jam paling sibuk yaitu pukul 10.00 di percobaan ke-3.

Untuk *packet loss*, tidak terdapat paket yang hilang karena protokol komunikasi yang digunakan adalah *Transmission Control Protocol* (TCP), sehingga dilakukan *error control* dan *flow control* dengan baik pada protokol tersebut.

IV. KESIMPULAN

Sistem autentikasi ganda pada sistem keamanan *smart security home* menggunakan sidik jari dan NFC telah berhasil dirancang dan diuji. Perangkat keras sistem ini dapat dibangun menggunakan node MCU, sensor sidik jari, NFC reader, *solenoid door lock* serta *buzzer*. Sistem ini mampu mengontrol *solenoid door lock* dengan autentikasi ganda menggunakan NFC dari *smartphone* pengguna dan sidik jari. Sistem akan mengirimkan notifikasi dan menyalakan *buzzer* apabila ada penyusup yang tidak dikenal. Berdasarkan hasil pengujian fungsionalitas sistem, sistem dapat mendeteksi NFC dan sidik jari dengan baik serta dapat terhubung dengan perangkat lunak dengan baik. Rata-rata *delay* pada sistem adalah 14,554 ms dan rata-rata *throughput* yang didapatkan adalah 1.909,042 bit/s. Penelitian selanjutnya diperlukan untuk pengembangan sistem ini seperti sistem dengan *delay* yang lebih pendek ataupun sistem dengan sensor yang lebih efisien dibandingkan NFC dan sidik jari.

UCAPAN TERIMA KASIH

Ucapan terima kasih diberikan kepada Politeknik Negeri Bandung yang telah berkontribusi dalam pendanaan bagi penelitian ini dengan skema penelitian mandiri dan nomor kontrak penelitian B/249/PL1.R7/PG.00.03/2020.

REFERENSI

- [1] KM. P. Peeters, "Assessing the vulnerability of targets for burglary. Creating a multi-level observational instrument,," 2013.
- [2] B. S. A, "Ada Celah, Rumah Dibobol," Kompas, 22 April 2018. [Online]. Available: <https://www.pressreader.com/indonesia/kompas/20180422/282321090605037>. [Accessed 20 September 2018].
- [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] N. Chandrakar, S. Kaul, M. Mohan, C. Sai Vamsi, and K. R. Prabhu, "NFC based profiling of smart home lighting system," *2015 Int. Conf. Ind. Instrum. Control. ICIC 2015*, pp. 338–341, 2015.
 - [7] O. Bindroo, K. Saxena, and S. K. Khatri, "A wearable NFC wristband for remote home automation system," *2nd Int. Conf. Telecommun. Networks, TEL-NET 2017*, vol. 2018-January, pp. 1–6, 2018.
 - [8] M. Darianian and M. P. Michael, "Smart home mobile RFID-based internet-of-things systems and services," *Proc. - 2008 Int. Conf. Adv. Comput. Theory Eng. ICACTE 2008*, pp. 116–120, 2008.
 - [9] N. Saparkhojayev, A. Dauitbayeva, A. Nurtayev, and G. Baimenshina, "NFC-enabled access control and management system," *2014 Int. Conf. Web Open Access to Learn. ICWOAL 2014*, pp. 2–5, 2015.
 - [10] D. Paradowski and A. Krüger, "Modularization of mobile shopping assistance systems," *2013 5th Int. Work. Near F. Commun. NFC 2013*, 2013.
 - [11] R. Bukhsh, N. Javaid, Z. Iqbal, U. Ahmed, Z. Ahmad, and M. N. Iqbal, "Appliances scheduling using hybrid scheme of genetic algorithm and elephant herd optimization for residential demand response," *Proc. - 32nd IEEE Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2018*, vol. 2018-January, pp. 210–217, 2018.
 - [12] M. Xiong, Y. Wu, Y. Ding, X. Mao, Z. Fang, and H. Huang, "A smart home control system based on indoor location and attitude estimation," *IEEE CITS 2016 - 2016 Int. Conf. Comput. Inf. Telecommun. Syst.*, pp. 0–4, 2016.
 - [13] K. M. Mithil, K. B. Mukesh Kumar, L. Sharma, M. Z. Sayeed Pasha, and H. D. Kallinath, "An interactive voice controlled humanoid smart home prototype using concepts of natural language processing and machine learning," *2018 3rd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2018 - Proc., no. i*, pp. 1537–1546, 2018.
 - [14] A. C. Jose, R. Malekian, and N. Ye, "Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home," *IEEE Access*, vol. 4, pp. 5776–5787, 2016.
 - [15] S. Ibrahim, V. K. Shukla, and R. Bathla, "Security Enhancement in Smart Home Management through Multimodal Biometric and Passcode," *Proc. Int. Conf. Intell. Eng. Manag. ICIEM 2020*, pp. 420–424, 2020.
 - [16] S. Haryadi, *Telecommunication Service and Experience*, no. January 2013. 2013.

