IMPLEMENTASI *NEAR FIELD COMMUNICATION* (NFC) PADA *SMARTPHONE* UNTUK PENGAMANAN RUANGAN SERVER

IMPLEMENTATION NEAR FIELD COMMUNICATION ON SMARTPHONE FOR SECURING SERVER ROOM

Muhamad Hamzah Mushaddiq[1], Rendy Munadi[2], Arif Indra Irawan[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**hamzahmsdq@student.telkomuniversity.ac.id**, [2]**rendymunadi@telkomuniveristy.ac.id**,
[3]**arifirawan@telkomuniversity.ac.id**

Abstrak

Pada saat ini kemajuan teknologi berkembang cukup pesat memberikan banyak kemudahan dan efisiensi dalam kehidupan manusia. *Near Field Communication* (NFC) merupakan salah satu teknologi komunikasi terbaru yang memanfaatkan gelombang radio. Teknologi NFC sampai sekarang semakin berkembang dengan teknoogi yang dimiliki mampu menggantikan beberapa peran sistem yang sudah berjalan. Seperti pada proses pembayaran, *ticketing* dan sistem pengamanan.

Dengan memanfaatkan teknologi NFC yang tertanam pada *smartphone,* maka dirancanglah sistem pengamanan ruangan yang terdiri dari NFC pada *smartphone* dan NFC *reader* yang diintegrasikan dengan Arduino Uno yang terpasang pada pintu ruangan. NFC *reader* yang terpasang di pintu ruangan akan membaca UID yang dikirimkan oleh NFC pada *smartphone,* yang kemudian hak akses nya diautentikasi NFC *reader* yang terintegrasi dengan Arduino Uno, lalu hasil dari autentikasi tersebut akan memicu fungsi *servo* yang berfungsi sebagai tuas untuk membuka dan menutup pintu ruangan, dan hasil autentikasi yang didapat akan dikirimkan ke Node Mcu kemudian dikirimkan ke Antares yang digunakan sebagai *cloud database,* setelah tersimpan di Antares data akan di kirimkan ke *Mobile Application* untuk mengetahui aktifitas *user* yang mengakses ruangan.

Berdasarkan Hasil dari penelitian, sistem pengamanan yang dirancang dapat melakukan proses validasi antara NFC *reader* yang terintegrasi dengan Arduino Uno dengan NFC pada smartphone dengan jarak maksimal 4cm jika tanpa *obstacle*. Sedangkan jika ada *obstacle* proses validasi bisa dilakukan dengan jarak maksimal 3cm. Penggunaan protokol MQTT lebih baik karena nilai delay lebih kecil daripada menggunakan protokol HTTP. Sedangkan nilai throughput HTTP lebih besar daripada protokol MQTT.

Kata Kunci: NFC, *smartphone,* Arduino Uno, Node Mcu, Antares, HTTP, MQTT.

Abstract

At this time the technology advances which evolving rapidly provide a lot of convenience and efficiency in human life. Near Field Communication (NFC) is on ofe the latest communication technologies that utilize radio waaves. NFC technology has been growing until now with the technology that is owned to be able to replace some of the systems that have been running. Like the payment process, ticketing and security systems.

By utilizing NFC technology that is embedded in a smartphone, a room security system consisting of NFC on smartphone and NFC reader is designed that is integrated with Arduino uno which is installed on the door of the room. NFC reader that is installed in the door of the room will read the UID sent by NFC on smartphone, then the access right are authenticated NFC reader integrated wih Arduino uno, then the result of the authentication will triger servo function to open and close the room door, and then the authentication results will be sent to Node Mcu then stored the result in Antares which is used as a cloud database, after being stored in Antares the data will be sent to mobile application for monitoring user who access the room.

Based on the results of the research, the security system design can carry out a validation process between NFC reader integrated with Arduino uno with NFC on smartphone with maximum distance 4cm without obstacle and 3cm with obstacle. MQTT protocol is better than HTTP because the delay value is smaller than HTTP. While the value of HTTP throughput is greater that the MQTT protocol.

Keywords: *NFC, smartphone, Arduino Uno, Node Mcu, Antares, HTTP, MQTT.*

1. Pendahuluan

Pada era globalisasi yang berkembang pesat saat ini *smartphone* menjadi kebutuhan yang tidak bisa dipisahkan. Dalam kehidupan saat ini masyarakat yang memiliki mobilitas tinggi menjadikan *smartphone* sebagai asisten pribadi dalam menjalankan aktifitasnya. Saat ini *smartphone* digunakan sebagai alat bantu *ticketing* dan *payment*. Oleh sebab itu, sangat memungkinkan kedepannya *smartphone* dapat mempermudah

`

manusia dalam mengakses ruangan-ruangan yang membutuhkan pengamanan berlebih. Dengan memanfaatkan NFC fitur yang tersedia di dalam *smartphone* memiliki keunggulan dari sisi praktis dan efisiensi. Praktis karena manusia tidak perlu lagi membawa kunci fisik ataupun kartu akses karena dapat digantikan fungsinya menggunakan *smartphone* yang memiliki fitur NFC didalamnya.

NFC adalah sebuah teknologi nirkabel jarak dekat yang dapat digunakan untuk pertukaran data antar perangkat. Pada *smartphone*, NFC merupakan pengembangan dari *bluetooth* dan *radio frequency identification* (RFID). NFC merupakan spesifikasi standar untuk *smartphone* dan *device* yang serupa untuk membangun transmisi radio antar *device* dengan cara mendekatkan kedua *device* tersebut. Hubungan transmisi radio dapat dibangun diantara dua *device* di dalam waktu yang sangat singkat, berkisar antara 100-150 milisekon kemudian perangkat harus dekat tidak lebih dari 10 sentimeter dan menggunakan 13.56 MHz dari frekuensi band [1].

Dengan banyaknya kantor atau perusahaan yang berkembang dengan pesat pasti mempunyai sebuah ruangan yang tidak bisa di akses oleh semua orang dan hanya bisa di akses oleh orang yang memiliki izin maupun akses untuk memasuki dan menggunakan fasilitas ruangan tersebut, untuk menghindari pembobolan ataupun penyalahgunaan hak akses untuk memasuki ruangan tersebut, maka sangat mungkin dirancang suatu sistem pengamanan pada pintu masuk ruangan yang memanfaatkan teknologi NFC pada smartphone yang digunakan sebagai masukan UID dari user yang memiliki hak akses ruangan, sehingga dapat menjadi kunci virtual yang menggantikan kunci fisik dan kartu akses. Untuk perancangannya, pintu ruangan terpasang NFC *reader* yang terhubung dengan Arduino Uno dan Node Mcu yang dijadikan sebagai penerima data serta informasi yang dikirimkan oleh NFC pada *smartphone* dan terintegrasi dengan beberapa perangkat keras pendukung lainnya. Mekanisme nya yaitu jika NFC pada *smartphone* ditempelkan dengan NFC *reader* yang terpasang di pintu, kemudian jika UID yang dimasukan terdaftar pada sistem maka pintu akan terbuka dan mengirimkan notifikasi kepada *admin* ruangan melalui *mobile app* bahwa *user* tersebut mempunyai akses dan jika tidak terdaftar pada sistem maka pintu tidak akan terbuka dan mengirimkan notifikasi kepada *admin* ruangan melalui *mobile app* bahwa user tersebut tidak mempunyai akses ruangan tersebut

Pada penelitian sebelumnya [2] "Perancangan dan Implementasi sistem akses kontrol pada pintu berbasis teknologi *Near Field Communication* dengan *mikrokontrol*er *Arduino Uno*" mekanisme kerja sistem ini yaitu ketika *user* akan memasuki ruangan menggunakan NFC yang ada di *smartphone* lalu *user* melakukan *tapping* ke NFC *reader* yang terpasang di pintu, kemudian *arduino* berkomunikasi dengan *web server* dan memeriksa apakah *user* tersebut memiliki jika *user* memiliki hak akses maka pintu terbuka. Jika *user* tidak memiliki akses maka pintu tidak akan terbuka, maka sistem akan mengirimkan notifikasi berupa sms kepada *admin* jika ada *user* yang tidak mempunyai hak akses tetapi mencoba untuk masuk kedalam ruangan tersebut.

Penelitian ini mengembangkan sistem yang sudah dibuat pada penelitian sebelumnya yaitu dengan menambahkan beberapa *treatment* jika ada *user* yang tidak memiliki akses namun mencoba untuk mengakses ruangan tersebut yaitu *Buzzer* sebagai alarm, serta mengirimkan notifikasi berupa infomasi yang kepada admin ruangan yang dapat di akes melalui *mobile app* dan melakukan analisa *Hypertex Transfer Protocol* (HTTP) sebagai protokol jalur komunikasi data pada sistem yang dibuat. Sehingga kedepannya sistem pengamanan pada ruangan di perkantoran maupun perusahaan besar semakin aman.

2. Tinjauan Pustaka

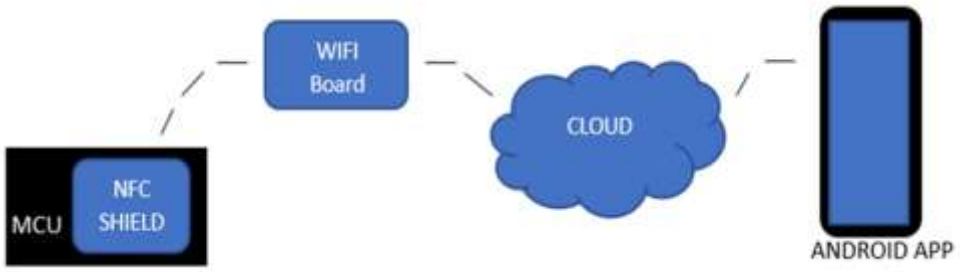
2.1 Pengamanan Ruangan

Keamanan merupakan hal yang sangat mutlak diinginkan oleh setiap orang, dengan adanya rasa aman maka orang tidak akan merasa khawatir. Ruangan *server* termasuk area *data center* yang termasuk aset vital perusahaan dan diperlakukan sesuai dengan persyaratan yang telah ditetapkan dalam sistem manajemen pengamanan perusahaan. Untuk itu perlu adanya sebuah sistem pengamanan untuk ruangan yang memiliki hak akses masuknya terbatas. Sistem keamanan dibuat untuk mengatur serta mengamankan berkas ataupun aset penting yang berada didalam ruangan secara cepat dan efektif dimaksudkan agar segala aktifitas untuk memasuki ruangan tersebut hanya untuk *user* yang memiliki akses. Pada penelitian ini dibahas tentang sistem keamanan ruangan yang dipasang pada pintu masuk ruangan dan kunci ruangannya menggunakan fitur NFC pada *smartphone*. *Admin* mengetahui informasi apabila ada tindakan pencurian pada ruangan yang di amankan melalui notifikasi yang dikirimkan oleh sistem yang dibuat pada penelitian kali ini.

2.2 *Internet of Things*

Internet of Things (IoT) adalah teknologi yang mengoneksikan berbagai benda ke media internet, sehingga manusia bisa mengambil informasi benda-benda tersebut setiap waktunya [3]. Potensi pemanfaatan IoT sangat banyak dan bisa diterapkan di berbagai bidang seperti pertanian, kesehatan, transportasi, dan sebagainya. Tidak mengherankan bila IoT disebut sebagai "the next big thing", telah diperkirakan bahwa banyak benda fisik atau objek dapat dilengkapi dengan berbagai jenis sensor yang terhubung dengan internet melalui suatu jaringan yang memungkinkan melakukan beberapa teknologi seperti penginderaan jarak jauh, *Wireless Sensor Network* (WSN), *Near Field Communication* (NFC).

`



Gambar 1. Desain Prototipe IoT.

2.3 *Near Field Communication*

Near Field Communication (NFC) adalah sebuah konektivitas nirkbel jarak dekat yang memperkenankan pertukaran data antara dua perangkat [4]. NFC pada *Smartphone* merupakan pengembangan dari *Bluetooth* dan RFID, teknologi NFC pada smartphone dapat beroperasi di dalam tiga mode berbeda, yaitu: mode *reader/writer*, *mode peer-to-peer* (P2P), dan mode *Host-based Card Emulation*. Masing- masing mode membutuhkan perangkat NFC menggunakan sebuah format data umum untuk komunikasi [5]. NFC beroperasi pada frekuensi 13,56 MHz dengan kecepatan transmisi pengiriman mencapai 424 kbit/s

Gambar 2. Application Near Field Communication (NFC).[6].

2.4 *Cloud Computing*

Cloud computing merupakan *IT as a Service* (ITaaS) yang menyediakan layanan komputasi, penyimpanan data, dan aplikasi dapat diakses melalui media internet dari pusat data yang tersentralisasi. *Cloud computing* adalah *platform* pengembangan aplikasi berbasis internet yang *scalable* [7]. Secara umum ada tiga jenis tipe layanan pada *cloud computing*, dimana pada ketiga arsitektur tersebut pengguna tidak mengatur secara langsung, ketiga arsitektur tersebut yaitu *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), dan *Software as a Service* (SaaS).

2.5 Antares

Antares sebuah *IoT platform* yang mendukung beberapa protokol seperti HTTP, MQTT, COAP [8]. Penggunaan Antares sebagai *IoT platform* digunakan sebagai media penyimpanan data sementara yang dikirimkan dari mikrokontroller yang kemudian data tersebut dapat dilihat pada *webpage* Antares dan dikirimkan ke *mobile application* berupa notifikasi.

2.6 *Message Queue Telemetry Transport*

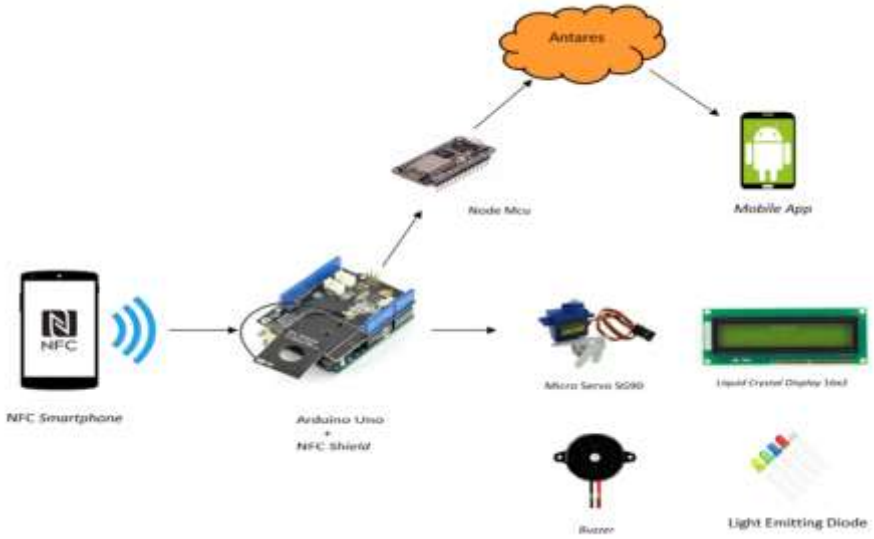
Message Queue Telemetry Transport (MQTT) adalah sebuah protokol komunikasi data *Machine to Machine* (M2M) yang berada pada layer aplikasi [9]. Pada perancangan prototipe penulis menekan sumber daya yang dibutuhkan, dengan melihat kebutuhan yang digunakan protokol ini menjadi pilihan. Melihat dari sifat yang *lightweight message* menjadikan pengiriman data pesan berukuran kecil yaitu hanya sebesar 2 *bytes* untuk setiap jenis data, sehingga memungkinkan untuk bekerja di dalam lingkungan yang terbatas sumber dayanya seperti *bandwidth* yang kecil dan sumber daya listrik yang terbatas. Selain itu protokol ini juga menjamin terkirimnya semua pesan walaupun koneksi terputus sementara, karena protokol *Message Queue Telemetry Transport* (MQTT) menggunakan metode *publish*/*subscribe*.

`

3. Perancangan Sistem

3.1 Desain Perancangan Sistem

Sebelum memulai tahap perancangan perlu melalui beberapa tahapan yaitu membuat desain sistem dan pemilihan komponen. Dalam perancangan sistem pengamanan ruangan ini untuk melakukan komunikasi antara NFC pada *smartphone* dengan NFC *shield* yang diintegasikan dengan Arduino Uno yang terpasang pada pintu masuk ruangan. Sistem yang dirancang prosesnya dimulai dari validasi UID yang dimasukan 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 (*Inter-Integrated Circuit*).



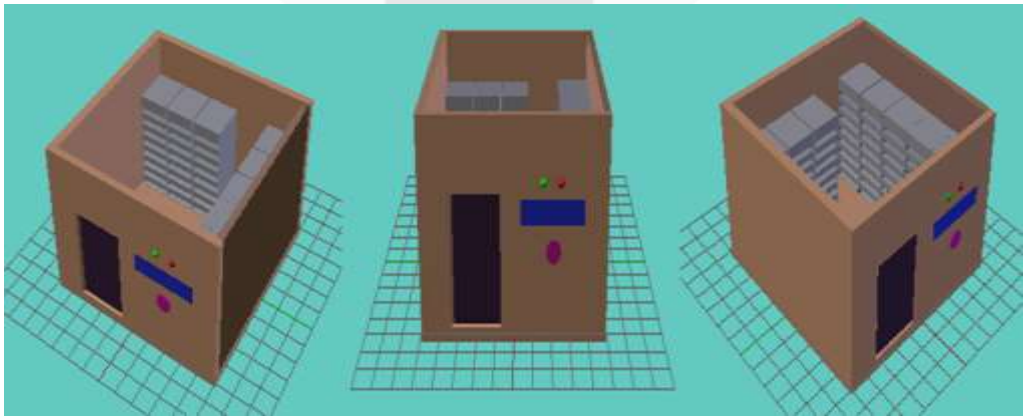
Gambar 3. Arsitektur prototipe sstem keamanan.

3.2 Sistem Komunikasi Antara *Client* dan *Server*

Pada perancangan prototipe ini dilakukan komunikasi antara sistem pengamanan ruangan dan Antares secara *wireless.* Maka dari itu diperlukan Node MCU sebagai *client* dan Antares sebagai *server* yang saling terkoneksi agar dapat melakukan komunikasi. Supaya *client* dapat terhubung dengan *server, client* perlu mengkoneksikan dengan SSID yang terdapat pada *server* untuk konektifitas nya dan menghubungkan *access key* yang terdapat pada *server.* Cara kerja komunikasi nya yaitu *client* mengirim data yang berisi informasi ke *server* menggunakan http atau mqtt protokol.

3.3 Desain Prototipe Ruangan

Berdasarkan desain sistem diatas maka perlu dibuat desain prototipe ruangan yang terbuat dari akrilik, dengan tinggi 20cm, panjang 30cm dan lebar 30cm, tuas pintu menggunakan micro servo yang terpasang di pintu masuk protipe ruangan. LCD 16x2 terpasang di sebelah kanan pintu, LED warna hijau dan merah berada diatas LCD, dan NFC *Shield* terpasang dibawah LCD. Berikut merupakan desain prototipe ruangan seperti pada gambar 4.

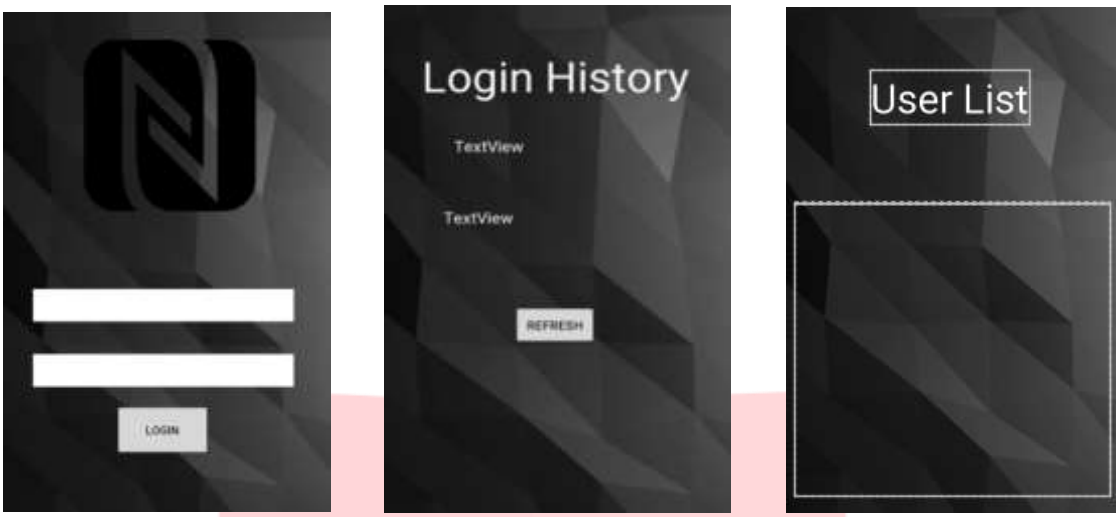


Gambar 4. Desain Prototipe Ruangan.

`

3.4 Desain Prototipe Mobile Application

Berdasarkan desain sistem diatas maka perlu dibuat desain prototipe *mobile application* yang dimiliki *admin* ruangan. Berikut merupakan desain prototipe *mobile application* seperti pada gambar 5.



Gambar 5 Desain Prototipe Ruangan.

Pada gambar 5 merupakan desain menu *login, user list, login history* prototipe *mobile application* yang akan dibuat, pada menu *login* terdapat button username dan password, pada menu *user list* memuat data user yang memiliki akses, dan pada menu *login history* memuat data *user* yang mengakses ruangan. Data yang ditampilkan berupa waktu *login user* secara *real time*, dan data *user* berupa UID dan status *login*. Button *refresh* untuk memuat ulang data *user* yang dipantau akses *login* nya

4. Pengujian

4.1 Pengujian Fungsionalitas Sistem Untuk Hak Akses Benar & Hak Akses Salah

Pengujian ini dilakukan untuk melihat fungsionalitas sistem secara keseluruhan dan mengetahui rasio, ketika proses *tapping* NFC mengirimkan UID 1,2,3 memiliki hak akses dan UID selain 1,2,3 yang tidak memiliki hak akses, Proses pengujian dilakukan masing-masing sebanyak 10 kali. Untuk hasil pengujian dapat dilihat pada tabel 4.1 & tabel 4.2

Tabel 4. 1 Tabel Pengujian Hak Akses Benar

Percobaan Ke -	Servo	Buzzer	Antares	Mobile Application	Status Login
1	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
2	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
3	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
4	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
5	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
6	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
7	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
8	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
9	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil
10	Bergerak	Tidak Aktif	Terhubung	Terhubung	Berhasil

Tabel 4. 2 Tabel Pengujian Hak Akses Salah.

Percobaan Ke -	Servo	Buzzer	Antares	Mobile Application	Status Login
1	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
2	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
3	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
4	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
5	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
6	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
7	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
8	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
9	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal
10	Tidak Bergerak	Aktif	Terhubung	Terhubung	Gagal

`

Pada tabel pengujian diatas dapat dilihat bahwa dari 10 kali masing masing percobaan tidak terdapat kegagalan fungsionalitas pada servo, buzzer, Antares, mobile app berjalan dengan semestinya. Fungsionalitas sistem yang dibuat yaitu 100%.

4.2 Pengujian Validasi Dengan *Obstacle* & Tanpa *Obstacle*

Pada pengujian ini dilakukan dengan cara melakukan *tapping* NFC pada *smartphone* dengan NFC shield, pengujian ini dilakukan berdasarkan jarak antara NFC pada *smartphone* dengan NFC shield dengan *obstacle* & tanpa *obstacle.* pengujian tersebut nantinya akan mendapatkan gambaran seberapa optimal nya jarak *tapping*-nya.

Tabel 4.3 Tabel Pengujian Validasi Tanpa Obstacle.

Percobaan Ke -	Jarak				
	1	2	3	4	5
1	0,2	0,35	1,3	2	0
2	0,28	0,29	1,11	1,79	0
3	0,19	0,32	1,12	1,77	0
4	0,22	0,28	1,18	1,95	0
5	0,25	0,4	1,22	2,4	0
6	0,18	0,39	1,18	2,4	0
7	0,2	0,35	1,58	2	0
8	0,21	0,35	1,31	1,98	0
9	0,22	0,33	1,43	2,4	0
10	0,22	0,39	1,18	1,88	0
Rata-Rata	0,21	0,37	1,24	1,94	0
Keterangan	1	1	1	1	0

Pada tabel pengujian diatas terdapat data berupa jarak dan waktu, jarak yang dimaksud pada tabel pengujian diatas merupakan jarak ketika proses *tapping* NFC *smartphone* dengan NFC shield dilakukan, jarak yang diambil mulai dari 1cm sampai 5cm dari tiap jarak didapat waktu validasi yang berbeda, waktu validasi yaitu waktu respon saat NFC pada *smartphone* dan NFC shield melakukan komunikasi untuk menjalankan perintah yang telah dimasukan dalam Arduino Uno, Pada tiap jarak dilakukan pengujian validasi sebanyak 10 kali, dengan melihat data pada tabel diatas proses validasi antara NFC pada *smartphone* dengan NFC shield bisa dilakukan dengan jarak maksimal 4cm selebihnya proses validasi tidak dapat dilakukan, maksud keterangan diatas yaitu jika 1 berarti proses validasi dapat dilakukan sedangkan jika 0 berarti proses validasi tidak dapat dilakukan.

Tabel 4.4 Tabel Pengujian Validasi Dengan Obstacle.

Percobaan Ke -	Jarak				
	1	2	3	4	5
1	0,3	0,97	2	0	0
2	0,33	1	2,11	0	0
3	0,3	1,3	1,82	0	0
4	0,4	1,22	1,98	0	0
5	0,36	1,17	2	0	0
6	0,3	1,15	2,4	0	0
7	0,3	0,86	1,9	0	0
8	0,38	1,21	2	0	0
9	0,28	1	2	0	0
10	0,24	1	2	0	0
Rata-Rata	0,27	0,985	2	0	0
Keterangan	1	1	1	0	0

Pada tabel pengujian diatas terdapat data berupa jarak dan waktu, jarak yang dimaksud pada tabel pengujian diatas merupakan jarak ketika proses *tapping* NFC *smartphone* dengan NFC shield dengan adanya penghalang berupa akrilik setebal 3mm, jarak yang diambil mulai dari 1cm sampai 5cm dari tiap jarak didapat waktu validasi yaitu waktu respon saat NFC pada *smartphone* dan NFC shield melakukan komunikasi untuk menjalankan perintah yang telah dimasukan dalam Arduino Uno. Pada tiap jarak dilakukan pengujian validasi sebanyak 10 kali, dengan melihat data pada tabel diatas proses validasi antara NFC pada *smartphone* dengan NFC shield bisa dilakukan dengan jarak maksimal 3cm selebihnya proses validasi tidak dapat dilakukan,

`

maksud keterangan diatas yaitu jika 1 berarti proses validasi dapat dilakukan sedangkan jika 0 berarti proses validasi tidak dapat dilakukan.

4.3 Pengujian *Quality of Service* (QoS) Sistem

Pada tahap ini sistem yang dirancang untuk digunakan pada sistem pengamanan ruangan akan dilakukan pengujian dan dilakukan analisa performansinya, akan didapatkan hasil performansi berupa nilai-nilai dari *delay*, *packet loss* dan *throughput* dari penggunaan protokol HTTP dan MQTT. Dengan beberapa parameter yang akan diamati diantaranya yaitu *delay*, *packet loss*, dan *throughput*.

Gambar 6 Grafik Pengujian *Delay, Throughput, Packet Loss* Pada sistem.

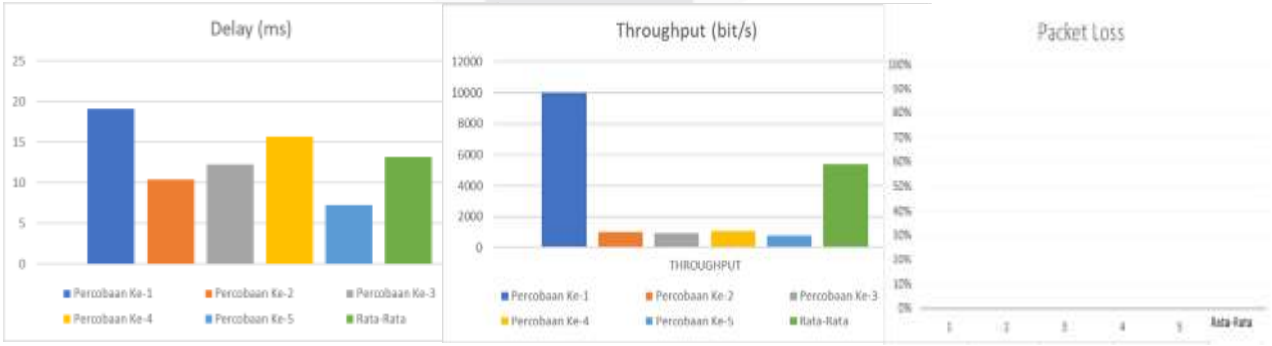
Pada gambar 6 dapat dilihat bahwa penggunaan protokol MQTT lebih baik daripada protokol HTTP dikarenakan protokol HTTP memiliki *delay* yang lebih besar dibandingkan protokol MQTT dan protokol MQTT memiliki nilai *throughtput* yang lebih besar dibandingkan protokol HTTP. Hal ini disebabkan karena, pada protokol HTTP ukuran paket yang dikirim lebih besar dikarenakan menggunakan format ASCII serta pada protokol HTTP memiliki *header size* sebesar 0,1 – 1 KB. Sedangkan, pada protokol MQTT ukuran paket yang digunakan lebih kecil. Protokol MQTT memiliki *header size* sebesar 2 – 4 bytes. Namun penggunaan HTTP dan MQTT sama sama menunjukan hasil yang bagus yaitu dengan melihat *packet loss* sebesar 0%.

4.4 Pengujian *Quality of Service* (QoS) *End User*

Pada Pengujian *Quality of Service* (QoS) pada *end user* dengan perangkat *mobile* diperlukan untuk mengetahui nilai layanan yang akan di berikan. Perangkat *mobile* meminta API Server yang telah dibuat pada Antares. Dengan Data & *Backend Services* menggunakan JSON, *admin* dapat melihat data user yang mengakses ruangan. Pengujian yang dilakukan sebanyak 5 kali.

Tabel 4.4 Pengujian *Quality of Service* (QoS) *End User Mobile Application*

Percobaan Ke -	*PACKET LOSS*	*DELAY*	*THROUGHPUT*
1	0%	19,0608 ms	9991,796 bit/s
2	0%	10,3928 ms	1048,737 bit/s
3	0%	12,2103 ms	921,27 bit/s
4	0%	15,6828 ms	1063,043 bit/s
5	0%	7,2705 ms	810,411 bit/s
Rata-Rata	0%	13,16565 ms	5401,1035 bit/s



Gambar 7 Grafik Pengujian QoS *End User Mobile Application*.

5. Kesimpulan

Berdasarkan hasil dari simulasi, hasil pengujian serta Analisa yang telah dilakukan maka dapat disimpulkan bahwa:

1. Pada penelitian ini telah berhasil mengimplementasikan *Near Field Communication* (NFC) yang terdapat pada *smartphone* dengan NFC shield yang diintegrasikan dengan Arduino Uno yang dijadikan sebagai sistem keamanan ruangan.
2. Rentang jarak proses validasi antara NFC pada *smartphone* dan NFC shield dapat melakukan komunikasi hingga jarak 4 cm tanpa ada penghalang sedangkan jika ada penghalang komunikasi bisa berlangsung hingga jarak 3cm.
3. Data yang didapat dari hasil proses validasi diolah pada Arduino Uno dan kemudian Node Mcu mengirimkan data tersebut menggunakan protokol HTTP dan MQTT dapat berfungsi dengan baik karena mendapatkan nilai *packet loss* sebesar 0% saat pengukuran QoS.
4. Penggunaan protokol MQTT lebih baik daripada protokol HTTP karena nilai delay yang didapat MQTT yaitu 13,5ms dan nilai throughput yang didapat MQTT yaitu 22000 bit/s.
5. Pada penelitian kali ini data yang didapat dari proses validasi bisa diterima serta dilihat pada Antares dan mobile application.

Daftar Pustaka:

[1] G. Gopichand, T. K. Chaitanya and R. R. Kumar, “Near Field Communication and Its Application in Various Field.”, Internation Journal of Engineering Trends and Technology, Vol. 4, no. 4, p. 5, April 2013.

[2] Aisyah, Q, S. Nasution, M, S & Jati, N, A. 2015. “Perancangan dan implementasi sistem akses kontrol pada pintu berbasis teknologi Near Field Communication dengan Mikrokontroler Arduino Uno”, Skripsi. Program Studi S1 Teknik Komputer, Fakultas Teknik Elektro, Universitas Telkom, Bandung.

[3] Dr. Herry Imanta Sitepu, M.T., “IOT (INTERNET OF THINGS): THE NEXT BIG THING”, ITHB 2017. [Online]. Available http://ithb.ac.id/id/iot-internet-of-things-the-next-big-thing/. [diakses 22 september 2018]

[4] S. M. Nasution, E. M. Husni and A. I. Wulandari, "Prototype of Train Ticketing Application Using Near Field Communication (NFC) Technology on Android Device," International Conference on System Engineering and Technology, 11-12 September 2012.

[5] K. Preethi, A. Sinha and N. "Contactless Communication through Near Field Communication," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 4, 2012.

[6] “Sensor – The Lifeblood of the Internet of things” Rajiv, 9 April 2017 . [Online]. Available: https://www.rfpage.com/applications-near-field-communication-future/ [diakses 23 september 2018].

[7] M. R. Effendi, "PENERAPAN TEKNOLOGI CLOUD COMPUTING DI UNIVERSITAS (Studi Kasus: Fakultas Teknologi Informasi Universitas Bayangkara Jakarta)," JURNAL TEKNOLOGI INFORMASI PROGRAM STUDI TEKNIK INFORMATIKA DAN SISTEM INFORMASI, UNIVERSITAS BUNDA MULIA, vol. 12, no. 9, 2016.

[8] “About Antares.” [Online]. Available: https://antares.id/id/index.html# [diakses 15 april 2019].

[9] H. A. Rochman, R. Primananda dan H. Nurwasito, “ Sistem Kendali Berbasis Mikrokontroler Menggunakan Protokol MQTT pada Smarthome,” Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 1, no. 6, p. 448, 2017

`