JURNAL INFOTEL
Informatika - Telekomunikasi - Elektronika

Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

Penerapan Kartu Elektronis Berbasis *Near Field Communication (NFC)* Pada Sistem Keamanan Pintu Rumah Cerdas

Danny Kurnianto[1], Eka Setia Nugraha[2], Vencentius Krisma Ekaristi[3]
[1,2,3]STT Telematika Telkom (ST3 Telkom) Purwokerto
[1,2,3]Jl. D.I Panjaitan No.128 Purwokerto, Indonesia
Email korespondensi : dannykurnianto@st3telkom.ac.id

Dikirim 01 Januari 2017, Direvisi 21 Januari 2017, Diterima 25 Februari 2017

Abstrak – Berdasarkan data laporan Badan Pusat Statistik (BPS) tahun 2015 bahwa angka kejadian tindak pencurian di Indonesia sampai tahun 2014 masih tergolong tinggi. Tidak adanya penerapan sistem keamanan pintu di setiap rumah menjadi salah satu sebab terjadinya tindak pencurian. Penggunaan kartu elektronis berbasis *Near Field Communication* (NFC) menjadi pilihan yang tepat untuk sistem keamanan pintu rumah karena teknologi NFC memberikan jaminan keamanan yang lebih baik untuk teknologi yang sejenis dengan konsumsi daya yang rendah. Proses otentifikasi sistem keamanan pintu elektronis dilakukan dengan membaca kode unik dari kartu *NFC Tag* yang akan dicocokkan dengan kode unik kartu NFC di basis data sistem. Jika hasil otentifikasi telah benar, Arduino sebagai pusat pengendali akan mengaktifkan *solenoid lock door* sehingga pintu akan terbuka. Hasil pengujian sistem menunjukkan bahwa jarak pembacaan sesungguhnya dari kartu NFC Tag sebesar 7 cm dengan jangkauan sudut pembacaan antara 0º - 85º. Tingkat keberhasilan sistem dalam melakukan proses otentifikasi sebesar 100%.

Kata kunci – sistem keamanan pintu elektronis, near field communication, NFC Tag.

Abstract - Based on data from the Badan Pusat Statistik (BPS) report in 2015 that the incidence of theft in Indonesia until 2014 was still high**.** One of the factors that led to this case is the lack of implementation of electronic door security systems in people's homes. The use of electronic card-based Near Field Communication (NFC) can be suitable choice because NFC technology provides better security guarantees for similar technology with low power consumption. The authentication process is done by reading the unique code from the card NFC tag that will be matched with the NFC card's unique code in the database system. If the authentication result is correct, Arduino as the central controller activates a solenoid lock door so that the door will be open. The test results showed that the actual reading distance of the card NFC tag by 7 cm with a range of reading angles between 0º - 85º. The success rate of the system in the authentication process of 100%.

Keywords - security systems of electronic door, near field communication, NFC Tag.

I. PENDAHULUAN

Kebutuhan dasar manusia yang harus dipenuhi selain dari sandang, pangan dan papan adalah keamanan. Rasa aman merupakan salah satu hak asasi manusia yang harus diperolah setiap orang. Hal ini seperti yang tertuang dalam UUD 1945 Pasal 28G ayat 1 yang berbunyi "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi" [1]. Terciptanya kesejahteraan sosial di masyarakat salah satunya adalah dengan adanya jaminan keamananan dari pemeritah, dalam hal ini yaitu aparat penegak hukum, sesuai dengan yang diamanatkan dalam Pembukaan UUD 1945.

Berdasarkan data dari Badan Pusat Statistik (BPS) tahun 2015 bahwa jumlah tindak kejahatan pencurian dengan kekerasan pada periode 2010-2014 berfluktuatif. Tahun 2010 terdapat 11.133 kasus dan meningkat menjadi 12.355 kasus pada tahun 2012.

Jumlah ini menurun di tahun 2014 yaitu dengan jumlah 11.758 kasus. Sedangkan untuk jumlah tindak kejahatan pencurian tanpa kekerasan pada periode 2010-2014, cenderung menurun. Pada tahun 2010 terdapat 127.364 kasus dan jumlah ini turun menjadi 117.751 kasus pada tahun 2014 [1]. Data diatas menunjukkan bahwa jumlah kasus tindak kejahatan pencurian masih tergolong berada pada angka yang tinggi setiap tahunnya.

Terjadinya tindak pencurian dapat disebabkan oleh tingkat kewaspadaan masyarakat kurang, sistem keamanan kurang memadai, ataupun jaminan keamanan dari penegak hukum yang kurang mencukupi. Terkait dengan sistem keamanan, sebagian besar masyarakat masih belum menerapkan sistem keamanan elektronis di rumah-rumah mereka. Padahal, dengan diterapkannya sistem keamanan elektronis yang terintegrasi dengan aplikasi rumah cerdas akan memberikan kenyamanan yang lebih baik, keselamatan dan keamanan yang lebih terjamin [2].

Rumah cerdas dapat diartikan sebagai perangkat yang memiliki sistem otomatisasi sangat canggih untuk mengendalikan lampu dan suhu, perangkat multi media untuk memantau dan menghidupkan sistem keamanan yang terhubung dengan pintu atau jendela dan beberapa fungsi yang lainnya [3]. Salah satu bagian dari aplikasi rumah cerdas adalah sistem keamanan elektronis pada pintu rumah. Sistem keamanan pintu elektronis dapat berfungsi untuk membuka dan menutup pintu secara elektronis, alarm otomatis ketika terjadi tindak pembobolan pintu secara paksa, dan memicu aktifnya perangkat lain yang terintegrasi dengan aplikasi rumah cerdas.

Sistem keamanan pintu elektronis dapat difungsikan untuk memberikan peringatan kepada pemilik rumah melalui media sms (*short message service*) saat terjadi pembobolan pintu secara paksa [4]. Fungsi untuk membuka dan menutup pintu secara elektronis dari jarak jauh dapat dilakukan dengan memanfaatkan media *bluetooth* dan *smatphone* android [5][6]. Sistem keamanan pintu yang digunakan sebagai pemicu aktifnya perangkat lain pada sistem rumah cerdas dilakukan dengan memasang sensor maknetik pada daun pintu [7]. Perangkat elektronik lain (seperti lampu, pengatur suhu dan lainnya) akan aktif jika terjadi pergerakan pada daun pintu yang menandakan ada seseorang yang masuk melalui pintu tersebut.

Proses otentifikasi dari pemilik rumah pada sistem keamanan pintu dibutuhkan untuk lebih memberikan jaminan keamanan bagi pemilik rumah. Hal ini dapat dilakukan dengan memasang *keypad* sebagai perangkat yang digunakan untuk memasukkan kata kunci tertentu [8]. Jika kata kuncinya sesuai maka pintu dapat terbuka secara elektronis dan juga sebaliknya. Kelemahan dari penggunaan kata kunci adalah mudah untuk dibobol, mudah untuk dilupakan. Untuk mengatasi kelemahan proses otentifikasi di atas, saat ini berkembang penelitian sebuah kartu pintar yang disebut *Near Field Communication* (NFC). NFC adalah sebuah teknologi baru untuk perangkat-perangkat elektronik yang memungkinkan perangkat-perangkat tersebut saling berkomunikasi satu sama lain dengan hanya menyentuh atau mendekatkannya dalam jarak yang sangat dekat (*contactless*). Meskipun pada penerapannya, NFC dijalankan mirip sebuah *Bluetooth* pada perangkat *mobile*, akan tetapi prinsip kerjanya berdasarkan teknologi *Radio Frequency Identification* (RFID) [9]. Beberapa keunggulan NFC dibandingkan dengan teknologi sejenis seperti tingkat keamanan yang lebih baik, kebutuhan daya kecil, pengaturan koneksi yang sederhana menyebabkan NFC menjadi pilihan utama dalam penerapan sistem keamanan elektronis saat ini [10].

Teknologi NFC telah diterapkan pada beberapa aplikasi seperti aplikasi STNK online [11]. Pada aplikasi STNK online, tag NFC yang berisi data nomor STNK diletakkan pada setiap kendaraan bermotor dan *smartphone* yang tertanam NFC digunakan sebagai reader tag NFC. Pada saat *smartphone* membaca informasi nomor STNK pada tag NFC, maka data tersebut akan disimpan di sebuah server yang terhubung melalui jaringan internet. Data-data STNK pada server tersebut akan ditampilkan di sebuah *interface* berupa website SNTK online.

Selanjutnya aplikasi yang dikembangkan sebagai sistem otentifikasi pada e-voting menggunakan teknologi NFC [12]. Aplikasi ini digunakan sebagai *problem solving* pada kelemahan pemilihan suara secara manual pada pemilihan umum. Sistem pada aplikasi ini terdiri dari 3 bagian utama yaitu perangkat input data, reader dan basis data server. Perangkat input data berupa *smartphone* (*password* atau nomor IMEI) dan e-ktp. Input data akan dibaca oleh reader kemudian data tersebut akan dilakukan proses otentifikasi dengan data pemilih pada basis data server. Jika identitas pemilih sesuai, maka reader akan meminta data-data kandidat yang bisa dipilih oleh pemilih. Jadi reader juga berfungsi sebagai perangkat pemilihan suara menggunakan *touchscreen.*

Teknologi NFC juga diterapkan pada aplikasi *smart room* untuk pengendalian akses ruangan [13]. Pada kasus dengan jumlah ruang banyak, maka data dari tag NFC (berupa ID pengguna) akan dibaca oleh reader dan kemudian dikirimkan ke master menggunakan *Radio Frequency* (RF). Data tersebut akan disimpan di basis data server secara *cloud* , dengan begitu dapat diakses oleh siapa saja yang membutuhkan informasi tersebut. Data pengguna akan ditampilkan pada sebuah website sebagai penampil informasi.

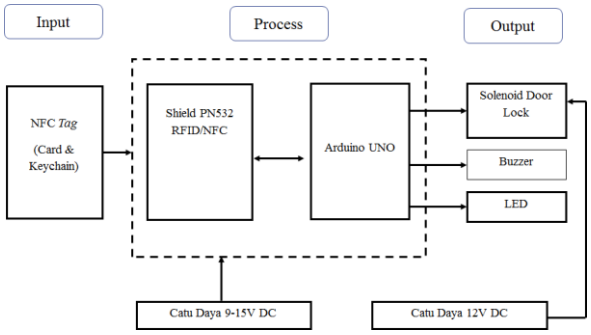
Berdasarkan keunggulan teknologi NFC yang telah digunakan pada beberapa aplikasi, maka pada penelitian ini digunakan NFC sebagai kartu elektronis untuk membuka pintu dengan melalui proses otentifikasi terlebih dahulu. Tujuan penelitian ini adalah untuk mengetahui seberapa tinggi tingkat keberhasilan otentifikasi kartu NFC yang digunakan dalam sistem keamanan pintu rumah.

ISSN : 2085-3688; e-ISSN : 2460-0997

II. METODE PENELITIAN

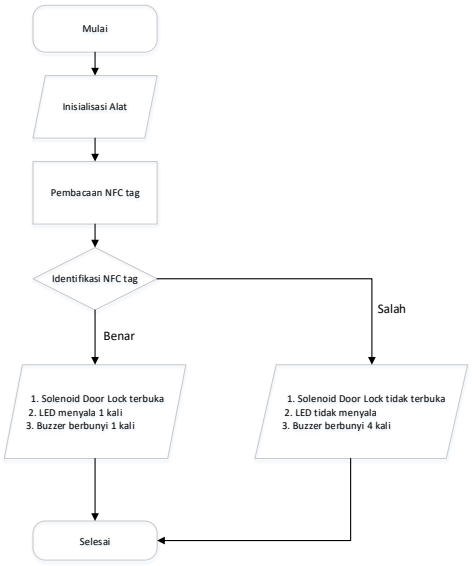
A. *Prinsip Kerja Sistem*

Sistem keamanan pintu elektronis berbasis NFC yang dirancang menggunakan beberapa komponen seperti *NFC tag MIRAFE Classic*, *NFC reader PN532 RFID/NFC*, Modul Arduino Uno, *Solenoid door lock*, buzzer dan LED. Diagram blok sistem keamanan pintu elektronis berbasis NFC ditunjukkan pada Gambar 1.



Gambar 1. Diagram Blok Sstem

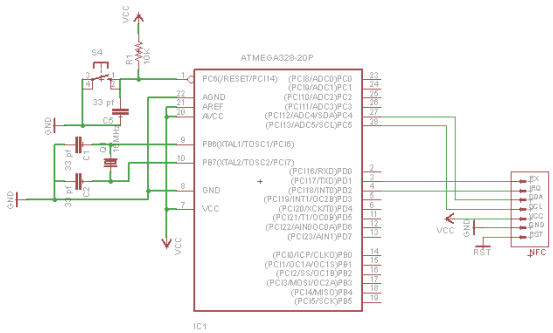
NFC tag yang berfungsi sebagai kunci elektronis menyimpan sebuah *unique identifier* (UID) dalam bentuk bilangan heksadesimal. UID akan dibaca oleh NFC reader saat kartu NFC didekatkan padanya. Proses otentifikasi dilakukan dengan mencocokkan UID kartu *NFC tag* dengan UID yang telah disimpan didalam basis data sistem. Jika UID dari NFC tag sesuai atau sama dengan UID basis data maka Arduino akan mengaktifkan *solenoid door lock* dan mengaktifkan buzzer serta LED sebagai indikator bahwa pintu sudah terbuka. Jika UID dari NFC tag tidak sesuai dengan UID basis data, maka Arduino tidak akan mengaktifkan *solenoid door lock* sehingga pintu tetap terkunci. Pada Gambar 2 ditunjukkan diagram alir sistem keamanan pintu elektronis berbasis NFC.



Gambar 2. Diagram Alir Sistem

B. *Rangkaian Antarmuka NFC Reader (Shield PN532 RFID/NFC)*

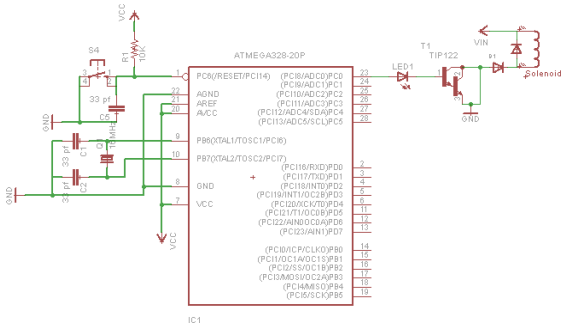
NFC reader pada sistem yang dirancang menggunakan *Shield* PN532 RFID/NFC yang akan dihubungkan dengan Arduino Uno R3. Komunikasi data antara *Shield* PN532 dengan Arduino menggunakan jenis komunikasi serial *Inter-Integrated Circuit* atau yang biasa disebut komunikasi I2C. Untuk dapat berkomunikasi, pada Shield PN532 digunakan pin IRQ dan reset. Pin SEL0 dan SEL1 dibiarkan tetap pada kondisi terbuka (*open circuit*). Pada Gambar 3 ditunjukkan rangkaian antarmuka NFC *reader*.



Gambar 3. Rangkaian antarmuka *NFC Reader* (*Shield PN532*)

C. *Rangkaian Antarmuka Solenoid Door Lock*

Solenoid Door Lock merupakan komponen elektromagnetik yang terdiri dari kumparan tembaga dengan dynamo dipusatnya. Ketika kumparan dialiri tegangan maka slot kunci akan tertarik ke pusat kumparan, begitupun sebaliknya. Tegangan operasional *solenoid door lock* sebesar 12 V dengan arus sebesar 2A. Transistor digunakan sebagai sakelar elekronik dan mendriver tegangan pada solenoid tersebut. Pada Gambar 4 ditunjukkan rangkaian antarmuka *Solenoid Door Lock.*

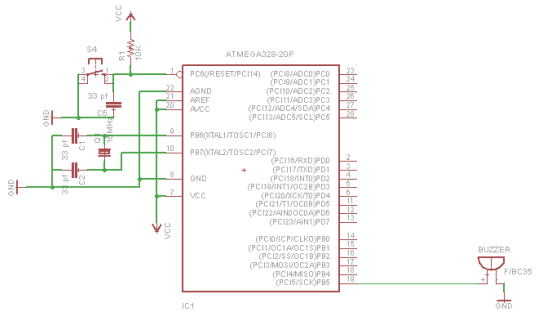


Gambar 4. Rangkaian Antarmuka *Solenoid Door Lock*

D. *Rangkaian Antarmuka Buzzer*

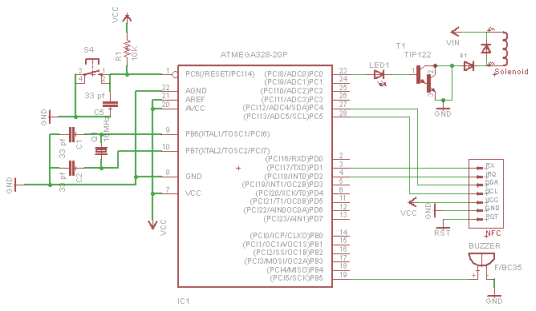
Buzzer digunakan sebagai indikator suara yang menandakan kondisi pembacaan kartu NFC tag yang digunakan sebagai kunci pintu. Untuk pembacaan NFC tag yang benar, buzzer akan mengeluarkan bunyi bip satu kali, sedang untuk pembacaan NFC tag salah maka buzzer akan mengeluarkan bunyi bip sebanyak empat kali. Satu kaki buzzer dihubungkan dengan pin PB5 pada chip ATMega328 sedangkan kaki yang lain dihubungkan dengan *ground*. Untuk

membunyikan buzzer dilakukan dengan memberikan tegangan berlogika *high* ("1") pada pin PB5 dan untuk mematikan bunyi buzzer, pada pin PB5 diberi tegangan berlogika *low* ("0"). Pada Gambar 5 ditunjukkan rangkaian antarmuka buzzer.



Gambar 5. Rangkaian Antarmuka Buzzer

Pada Gambar 6 ditunjukkan rangkaian keseluruhan sistem.



Gambar 6. Rangkaian Keseluruhan Sistem

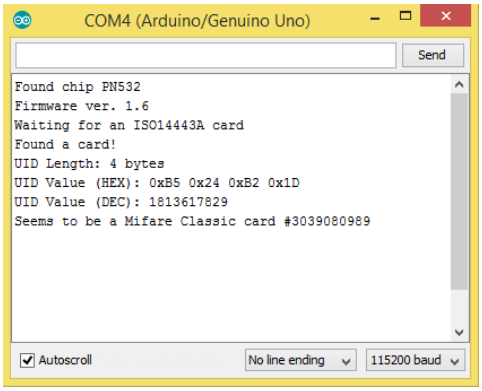
III. HASIL DAN PEMBAHASAN

Hasil penelitian yang akan dibahas adalah hasil pengujian pada bagian pembacaan NFC tag, pengujian jarak pembacaan NFC tag, pengujian sudut pembacaan NFC tag dan pengujian skenario sistem yang terdiri dari 5 skenario.

A. *Pengujian Pembacaan NFC Tag*

Pengujian ini ditujukan untuk mengetahui *unique identifier* (UID) pada kartu NFC tag yang nantinya akan digunakan dalam proses otentifikasi untuk membuka slot kunci. Pengujian ini menggunakan lima buah kartu NFC tag. Pada Gambar 7 ditunjukkan hasil pembacaan UID dari salah satu NFC tag. UID kartu NFC berbentuk bilangan heksadesimal dengan nilai "0xB5 0x24 0xB2 0x1D". Kode heksadesimal ini diubah kedalam bentuk desimal untuk proses otentifikasi. Selain data berupa UID kartu, data lain yang tersimpan dalam kartu adalah jenis kartu Mifare Classic dan serial number kartu.

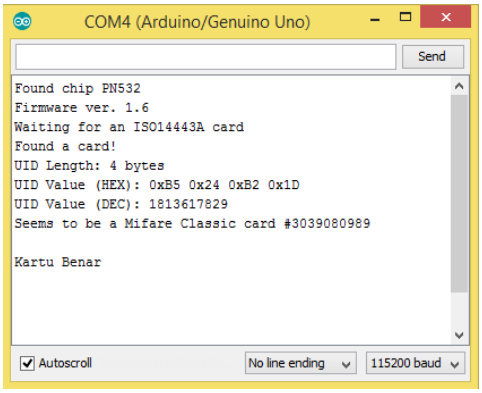
Pada Tabel 1 ditunjukkan hasil pembacaan dari lima buah kartu NFC tag. Berdasarkan pengujian pembacaan kelima kartu NFC tag, masing-masing kartu memiliki *unique identifier* yangberbeda-beda seperti yang ditunjukkan pada Tabel 1.



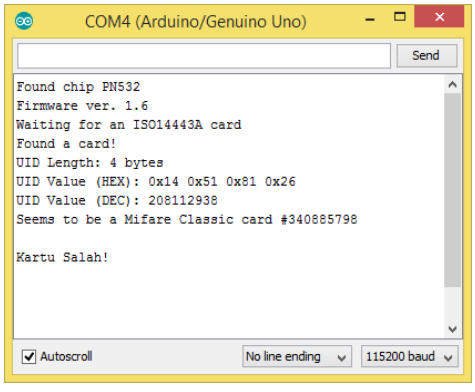
Gambar 7. Hasil Pembacaan UID kartu NFC tag

B. *Pengujian Otentifikasi Kata Kunci*

Pengujian otentifikasi kata kunci dilakukan dengan mencocokkan kata kunci yang berasal dari *unique identifier* NFC tag dengan *unique identifier* basis data. *Unique identifier* yang digunakan berupa bilangan desimal. Berikut ini hasil pengujian kata kunci berupa bilangan desimal "1813617829" yang telah disimpan terlebih dahulu pada basis data. Pengujian pertama menggunakan kartu NFC tag yang benar (memiliki *unique identifier* "1813617829") dan pengujian kedua menggunakan kartu NFC tag yang salah. Pada Gambar 8 ditunjukkan hasil pengujian kartu *NFC tag* yang benar. Sedangkan pada Gambar 9 ditunjukkan hasil pengujian kartu *NFC tag* yang salah.



Gambar 8. Hasil Pengujian Kartu NFC Tag Benar



Gambar 9. Hasil Pengujian Kartu NFC Tag Salah

C. Pengujian Jarak Pembacaan NFC Tag

Pengujian ini bertujuan untuk memastikan jarak pembacaan sebenarnya pada NFC reader terhadap NFC tag. Berdasarkan deskripsi datasheet NFC reader (Shield PN532 RFID/NFC) bahwa pembacaan NFC tag dapat dilakukan sampai jarak maksimal 10 cm. Pada Tabel 2 ditunjukkan hasil pengujian jarak pembacaan NFC Tag. Berdasarkan hasil pengujian jarak pembacaan NFC Tag seperti yang ditunjukkan pada Tabel 2 bahwa jarak pembacaan sesungguhnya dari NFC Tag adalah sampai jarak 7 cm, hal ini berbeda dengan deskripsi jarak pembacaan yang dijelaskan pada datasheet NFC reader.

D. Pengujian Sudut Pembacaan NFC Tag

Pengujian sudut pembacaan NFC Tag ini bertujuan untuk mengetahui seberapa besar sudut pembacaan yang dapat dilakukan oleh NFC reader. Pengujian dilakukan dengan mengatur parameter sudut pembacaan mulai dari sudut 0º sampai 90º. Pada Tabel 3 ditunjukkan hasil pengujian sudut pembacaan NFC Tag.

Berdasarkan hasil pengujian sudut pembacaan NFC Tag pada Tabel 3 bahwa kartu NFC Tag tetap dapat dibaca hingga pada sudut kemiringan 85 derajat. Pada posisi 90 derajat atau posisi tegak lurus NFC tag tidak dapat dibaca lagi.

Tabel 1. Hasil Pembacaan UID Pada Lima NFC Tag

NFC tag		Unique Identifier		
		Hex	Dec	Serial Number
Kartu	A	0xB5 0x24 0xB2 0x1D	1813617829	#3039080989
	B	0xB4 0xB8 0x80 0x26	18018412838	#3031990310
	C	0x14 0x51 0x81 0x26	208112938	#340885798
Gantungan Kunci	D	0x70 0x4A 0x0E 0x1F	112741431	#1883901471
	E	0x70 0x99 0xD1 0x1E	11215320930	#1889128734

Tabel 2. Hasil Pengujian Jarak Pembacaan NFC Tag

NFC tag	Hasil Pembacaan NFC tag														
	Jarak (cm)														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Kartu A	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-
Kartu B	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-
Kartu C	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-
Gantungan Kunci D	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-
Gantungan Kunci E	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-

Tabel 3. Hasil Pengujian Sudut Pembacaan NFC Tag

NFC tag	Sudut (Derajat)																	
	0	5	10	15	20	25	30	35	40	45	50	55	65	70	75	80	85	90
Kartu A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Kartu B	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Kartu C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Gantungan Kunci D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Gantungan Kunci E	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-

E. Pengujian Skenario Pembacaan NFC Tag

Pengujian skenario pembacaan NFC Tag menggunakan lebih dari satu kartu NFC Tag. Pengujian ini bertujuan untuk melihat proses otentikasi kunci pintu elektronik untuk dapat mengenali lebih dari satu NFC tag dan dapat membuka slot kunci pintu elektronik yang sama. Skenario yang digunakan dalam pengujian ini sebanyak lima skenario yaitu dengan menambahkan satu NFC tag baru pada setiap skenarionya dan sisanya dibuat pada kondisi pembacaan NFC tag yang salah.

a) Skenario 1

Pada skenario 1 diatur kondisi bahwa kartu NFC Tag A sebagai kartu yang sah untuk proses otentifikasi dan membuka slot kunci sedangkan

kartu yang lain diatur sebagai kartu tidak sah. Pada Tabel 4 ditunjukkan skenario 1.

Tabel 4. Skenario 1

NFC tag	Hasil Pembacaan			
	Terbaca	Tidak Terbaca	Slot Terbuka	Slot Tidak Terbuka
Kartu A	✓	-	✓	-
Kartu B	-	✓	-	✓
Kartu C	-	✓	-	✓
Gantungan Kunci D	-	✓	-	✓
Gantungan Kunci E	-	✓	-	✓

Pengujian skenario 1 dilakukan sebanyak 5 kali dengan hasil yang ditunjukkan seperti pada Tabel 5.

Tabel 5. Hasil Pengujian Skenario 1

Uji Ke-	Pembacaan Kartu NFC Tag				
	A	B	C	Gantungan Kunci	
				D	E
1	terbaca	tidak	tidak	tidak	tidak
2	terbaca	tidak	tidak	tidak	tidak
3	terbaca	tidak	tidak	tidak	tidak
4	terbaca	tidak	tidak	tidak	tidak
5	terbaca	tidak	tidak	tidak	tidak

Dari hasil pengujian skenario 1 sebanyak 5 kali menunjukkan bahwa sistem dapat membaca kartu NFC Tag A sebagai kartu yang sah dan dapat mengenali empat kartu yang lain sebagai kartu yang tidak sah.

b) Skenario 2

Pada skenario 2 diatur kondisi bahwa kartu NFC Tag A dan B sebagai kartu yang sah untuk otentifikasi dan membuka slot kunci sedangkan kartu yang lain diatur sebagai kartu yang tidak sah. Pada Tabel 6 ditunjukkan skenario 2.

Tabel 6. Skenario 2

NFC tag	Hasil Pembacaan			
	Terbaca	Tidak Terbaca	Slot Terbuka	Slot Tidak Terbuka
Kartu A	✓	-	✓	-
Kartu B	✓	-	✓	-
Kartu C	-	✓	-	✓
Gantungan Kunci D	-	✓	-	✓
Gantungan Kunci E	-	✓	-	✓

Pengujian skenario 2 dilakukan sebanyak 5 kali dengan hasil yang ditunjukkan seperti pada Tabel 7.

Dari hasil pengujian skenario 2 sebanyak 5 kali menunjukkan bahwa sistem dapat membaca kartu NFC Tag A dan B sebagai kartu yang sah dan dapat mengenali tiga kartu yang lain sebagai kartu yang tidak sah.

Tabel 7. Hasil Pengujian Skenario 2

Uji Ke-	Pembacaan Kartu NFC Tag				
	A	B	C	Gantungan Kunci	
				D	E
1	terbaca	terbaca	tidak	tidak	tidak
2	terbaca	terbaca	tidak	tidak	tidak
3	terbaca	terbaca	tidak	tidak	tidak
4	terbaca	terbaca	tidak	tidak	tidak
5	terbaca	terbaca	tidak	tidak	tidak

c) Skenario 3

Pada skenario 3 diatur kondisi bahwa kartu NFC Tag A,B dan C sebagai kartu yang sah untuk proses otentifikasi dan membuka slot kunci sedangkan kartu yang lain diatur sebagai kartu tidak sah. Pada Tabel 8 ditunjukkan skenario 3.

Tabel 8. Skenario 3

NFC tag	Hasil Pembacaan			
	Terbaca	Tidak Terbaca	Slot Terbuka	Slot Tidak Terbuka
Kartu A	✓	-	✓	-
Kartu B	✓	-	✓	-
Kartu C	✓	-	✓	-
Gantungan Kunci D	-	✓	-	✓
Gantungan Kunci E	-	✓	-	✓

Pengujian skenario 3 dilakukan sebanyak 5 kali dengan hasil yang ditunjukkan seperti pada Tabel 9.

Tabel 9. Hasil Pengujian Skenario 3

Uji Ke-	Pembacaan Kartu NFC Tag				
	A	B	C	Gantungan Kunci	
				D	E
1	terbaca	terbaca	terbaca	tidak	tidak
2	terbaca	terbaca	terbaca	tidak	tidak
3	terbaca	terbaca	terbaca	tidak	tidak
4	terbaca	terbaca	terbaca	tidak	tidak
5	terbaca	terbaca	terbaca	tidak	tidak

Dari hasil pengujian skenario 3 sebanyak 5 kali pengujian menunjukkan bahwa sistem dapat membaca kartu NFC Tag A, B dan C sebagai kartu yang sah dan dapat mengenali dua kartu yang lain sebagai kartu tidak sah.

d) Skenario 4

Pada skenario 4 diatur kondisi bahwa kartu NFC Tag A, B, C dan D sebagai kartu yang sah

untuk proses otentifikasi dan membuka slot kunci sedangkan kartu yang lain diatur sebagai kartu tidak sah. Pada Tabel 10 ditunjukkan skenario 4.

Tabel 10. Skenario 4

NFC tag	Hasil Pembacaan			
	Terbaca	Tidak Terbaca	Slot Terbuka	Slot Tidak Terbuka
Kartu A	✓	-	✓	-
Kartu B	✓	-	✓	-
Kartu C	✓	-	✓	-
Gantungan Kunci D	✓	-	✓	-
Gantungan Kunci E	-	✓	-	✓

Pengujian skenario 4 dilakukan sebanyak 5 kali dengan hasil yang ditunjukkan seperti pada Tabel 11.

Tabel 11. Hasil Pengujian Skenario 4

Uji Ke-	Pembacaan Kartu NFC Tag				
	A	B	C	Gantungan Kunci	
				D	E
1	terbaca	terbaca	terbaca	terbaca	tidak
2	terbaca	terbaca	terbaca	terbaca	tidak
3	terbaca	terbaca	terbaca	terbaca	tidak
4	terbaca	terbaca	terbaca	terbaca	tidak
5	terbaca	terbaca	terbaca	terbaca	tidak

Dari hasil pengujian skenario 4 sebanyak 5 kali pengujian menunjukkan bahwa sistem dapat membaca kartu NFC Tag A, B, C dan D sebagai kartu yang sah dan dapat mengenali satu kartu yang lain sebagai kartu tidak sah.

e) Skenario 5

Pada skenario 5 diatur kondisi bahwa kelima kartu NFC Tag sebagai kartu yang sah untuk proses otentifikasi dan membuka slot kunci. Pada Tabel 12 ditunjukkan skenario 5.

Tabel 12. Skenario 5

NFC tag	Hasil Pembacaan			
	Terbaca	Tidak Terbaca	Slot Terbuka	Slot Tidak Terbuka
Kartu A	✓	-	✓	-
Kartu B	✓	-	✓	-
Kartu C	✓	-	✓	-
Gantungan Kunci D	✓	-	✓	-
Gantungan Kunci E	✓	-	✓	-

Pengujian skenario 5 dilakukan sebanyak 5 kali dengan hasil yang ditunjukkan seperti pada Tabel 13.

Tabel 13. Hasil Pengujian Skenario 5

Uji Ke-	Pembacaan Kartu NFC Tag				
	A	B	C	Gantungan Kunci	
				D	E
1	terbaca	terbaca	terbaca	terbaca	terbaca
2	terbaca	terbaca	terbaca	terbaca	terbaca
3	terbaca	terbaca	terbaca	terbaca	terbaca
4	terbaca	terbaca	terbaca	terbaca	terbaca
5	terbaca	terbaca	terbaca	terbaca	terbaca

Dari hasil pengujian skenario 5 sebanyak 5 kali pengujian menunjukkan bahwa sistem dapat membaca semua kartu NFC sebagai kartu yang sah.

Berdasarkan hasil pengujian skenario pembacaan 5 buah NFC Tag dengan pengujian sebanyak 5 kali untuk setiap skenario menunjukkan bahwa tingkat keberhasilan sistem keamanan pintu berbasis NFC mencapai nilai 100%. Ini artinya bahwa sistem dapat melakukan proses otentifikasi kartu NFC Tag dengan benar sesuai dengan rancangan awal sistem tanpa terjadinya kesalahan dalam mengenali kartu *NFC Tag*.

IV. PENUTUP

A. Kesimpulan

Dari hasil pengujian sistem secara keseluruhan dapat disimpulkan bahwa jarak maksimal sesungguhnya untuk pembacaan *NFC Tag Mirafe Classic* menggunakan *NFC reader PN532 RFID/NFC* sebesar 7 cm. Sudut maksimal pembacaan *NFC Tag Mirafe Classic* menggunakan *NFC reader PN532 RFID/NFC* sebesar 85^{o}. Kemudian tingkat keberhasilan sistem dengan menggunakan 5 skenario sebesar 100%.

DAFTAR PUSTAKA

[1] "Statistik Kriminal 2015," Badan Pusat Statistik, Jakarta, 2015.

[2] S. Kumar, "Ubiquitous Smart Home System Using Android Application," *IJCNC*, vol. 6, no. 1, pp. 33–43, 2014.

[3] D. Bregman, R. Blvd, and R. Lezion, "Smart Home Intelligence - The eHome that Learns," *Int. J. Smart Home Smart Vol.4, No.4*, vol. 4, no. 4, pp. 35–46, 2010.

[4] S. Riyadi and B. E. Purnama, "Sistem Pengendalian Keamanan Pintu Rumas Berbasis SMS Menggunakan Mikrokontroler ATMega 8535," *IJNS*, vol. 2, no. 4, pp. 7–11, 2013.

[5] A. F. Silvia, E. Haritman, and Y. Muladi, "Rancang Bangun Akses Kontrol Pintu Gerbang Berbasis Arduino dan Android," *ELECTRANS*, vol. 13, no. 1, pp. 1–10, 2014.

[6] S. Winardi, Firmansyah, and W. A. Kristiana, "Rancang Bangun Sistem Pengaman Pintu Rumah Menggunakan Android Berbasis Arduino Uno," *NARODROID*, vol. 2, no. 1, 2016.

[7] D. Kurnianto, A. M. Hadi, and E. Wahyudi, "Perancangan Sistem Kendali Otomatis Pada Smart Home Menggunakan Modul Arduino Uno," *JNTE*, vol. 5, no. 2, 2016.

[8] H. Guntoro, Y. Somantri, and E. Haritman, "Rancang Bangun Magnetic Door Lock Menggunakan Keypad dan Solenoid Berbasis Mkrokontroler Arduino Uno," *ELECTRANS*, vol. 12, no. 1, pp. 39–48, 2013.

[9] M. U. Yaqub and U. A. Shaikh, "Near Field Communication," 2012.

[10] G. Jain and S. Dahiya, "NFC : Advantages, Limits and Future Scope," vol. 4, no. 4, pp. 1–12, 2015.

[11] R. H. F. Kontu, A. A. E. Sinsuw, S. T. Mt, and J. T. Elektro-ft, "Perancangan Sistem Pembaca Surat Tanda Nomor Kendaraan Dengan Teknologi NFC," *E-journal Tek. Elekro dan Komput.*, pp. 79–85, 2015.

[12] T. Ahmad, R. M. Ijtihadie, and A. Wicaksono, "PENGEMBANGAN SISTEM OTENTIKASI PADA E-VOTING," in *Seminar Nasional Sistem Informasi Indonesia*, 2014, no. September, pp. 461–466.

[13] D. Palma and J. E. Agudo, "An Internet of Things Example: Classrooms Access Control over Near Field Communication," *Sensor*, vol. 14, no. 4, pp. 6998–7012, 2014.