Sistem Keamanan Informasi pada *Smart Gate* Menggunakan Visual Basic

Khairunnisa Mansur*[1], Zulfajri Basri Hasanuddin[1] , Wardi[1]
[1]Departemen Teknik Elektro, Fakultas Teknik, Universitas Hasanuddin
Jl. Poros Malino Km.6, Bontomarannu, Gowa, Sulawesi Selatan, 92171, Indonesia
*Email: Khairunnisae10@gmail.com

DOI: 10.25042/jpe.052018.07

Abstrak

Kartu identitas atau *identification card* menjadi pendukung utama dalam *gate system*. Penelitian ini bertujuan untuk menerapkan *smart card* pada *smart gate* di kalangan civitas akademika sebagai pengguna. Sistem ini menggunakan *Near Field Communication* (NFC) *smart card* jenis MIFARE sebagai identitas untuk identifikasi dan otentikasi. Proses baca/tulis dikonfigurasi dimana blok data dapat dibaca dengan menggunakan *software* yang telah dirancang dengan menggunakan aplikasi Visual Basic 2010. Proses penulisan data pada NFC tag melalui komunikasi serial dimana data informasi digabungkan menjadi 1 line informasi yang telah melalui tahapan enkripsi kemudian dialokasikan dalam bentuk *array* kedalam blok data yang telah ditentukan dalam penelitian ini yakni blok data 9, 10, 11 dan 13 dengan total data 64 Byte. Keamanan informasi pada NFC tag dilakukan dengan enkripsi metode Caesar Chiper dan rotate letter. Waktu yang dibutuhkan dalam melakukan pembacaan informasi dari database ke NFC tag tanpa adanya penghalang yakni waktu tercepat 1,49 detik dan terlama 2,26 detik dengan rata-rata waktu proses 1,84 detik, sedangkan untuk pengujian dengan menggunakan penghalang diperoleh waktu tercepat 1,53 detik dan waktu terlama 2,21 detik dengan rata-rata waktu proses 1,83 detik. Hal ini menandakan waktu yang digunakan dalam proses penulisan informasi efisien dan tidak terpengaruh oleh adanya penghalang. Hasil penelitian menunjukkan bahwa dengan adanya proses enkripsi informasi pada NFC tag hanya dapat dibaca melalui aplikasi Visual Basic yang telah dirancang dan dilengkapi dengan sistem enkripsi dan dekripsi.

Abstract

Information System Security Identity on Smart Gate using Visual Basic. Card or identification card become the main support in gate system. This research aim to apply smart card at smart gate among academic community as user. This system uses Near Field Communication smart card type MIFARE as identity for identification and authentication. The read/write process is configured where data blocks can be read using software that has been designed using visual basic 2010 applications. The process of writing data on NFC tags through serial communication where data information is combined into 1 line information that has been through the encryption stage will then be allocated in the form Array into data block that has been determined in this research that is data block 9, 10, 11 and 13 with total data 64 Byte. Information security on NFC tags is done by Caesar Chiper method encryption and rotate letter. The time required to read from database to NFC tags without any obstacles is the fastest time of 1.49 seconds and the longest 2.26 seconds with an average processing time of 1.84 seconds, while for testing using a barrier obtained the fastest time 1.53 seconds and the longest time 2.21 seconds with average process time is 1.83 seconds. This indicates the time spent in the process of writing efficient information and not affected by the presence of obstacles. The results showed that the existence of information encryption process on NFC tag can only be read through Visual Basic application that has been designed and equipped with encryption and decryption system.

Kata-kunci: *Enkripsi, smart card, smart gate, Visual Basic*

1. Pendahuluan

Gate system menjadi standar dasar keamanan yang membutuhkan lebih banyak data untuk mengidentifikasi kendaraan atau orang yang masuk dalam suatu lingkungan [1]. Kartu identitas atau *identification card* menjadi pendukung utama dalam *gate system. Gate system* merupakan aplikasi dari akses kontrol yang diproduksi menggunakan teknolgi *magnetic striped cards* dan *proximity cards* untuk proses identifikasi yang lebih cepat dimana sistem akan terbuka otomatis apabila data yang teridentifikasi telah terdaftar.

Smart card memiliki kemampuan untuk menyimpan data identitas serta dapat diprogram pada sisi aplikasinya yang dapat digunakan untuk proses otentifikasi. Sistem *smart card* pada

kampus merupakan bagian pendukung dasar dalam konstruksi informasi. Sistem mengumpulkan banyak data untuk otentikasi yang terintegrasi [2].

Teknologi *Near Field Communication* (NFC) merupakan pengembangan dari teknologi *Radio Frequency Identification* (RFID). NFC *card / tag* dapat diintegrasikan dengan kartu cerdas dan perangkat lainnya. Standar ISO / IEC 14 443 mode pengoperasian *contactless smartcard* dengan kisaran sekitar 10 cm [3]. NFC semakin banyak diterapkan ke berbagai bidang dimana aplikasi terintegrasi ke dalam *mobile* dan perangkat cerdas yang diaplikasikan pada tiket, manajemen akses, dan keamanan [4].

Sistem akses kontrol berdasarkan RFID telah dikembangkan baik menggunakan *smart card* dan *smart phone*. Penelitian Kao & Chung (2008), mengembangkan aplikasi sistem *computer client-end* dengan memanfaatkan kartu IC *contactless* dan *reader* berdasarkan RFID untuk pengendalian gerbang / *gate* kampus dengan proses identifikasi yang dibangun melalui *server-end* database dan Local Area Network (LAN) kampus [5]. Penelitian Woo-Garcia *et al* (2016), kontrol akses dengan sistem RFID untuk menentukan atau memberlakukan kontrol akses dan pembatasan di area utama bangunan universitas yang seharusnya hanya bisa diakses oleh sekelompok kecil staf. Topik penelitian akses kontrol dalam lingungan kampus ini tetap potensial untuk dikembangkan karena masing-masing kampus ingin mengembangkan sistem sendiri, dan juga memiliki inovasi yang berbeda [6].

Bouazzouni *et al* (2016), mengajukan sebuah arsitektur untuk membangun sistem akses kontrol yang aman berbasis Trusted Execution Environtmen (TEE) dan Identity Based Encryption (IBE) [7]. TEE adalah kombinasi dari sebuah perangkat keras dan perangkat lunak dimana eksekusi sistemnya terbagi dalam dua lingkungan. Otentikasi dilakukan berdasarkan IBE dan TEE yang dipresentasikan dalam OP-TEE. Gruntz *et al* (2016), mengembangkan *smart phone* yang berdasarkan sistem akses kontrol secara fisik dimana akses poin tidak secara langsung terhubung ke *server* pusat, tetapi lebih menggunakan konektivitas dari *smart phone* untuk dapat mengakses permintaan akses *online* dari pengguna dengan menggunakan *server* akses pusat [8]. Otentikasi dari *smart phone* berdasar pada kunci kriptografi publik. Kedua penelitian ini memanfaatkan *smart phone* yang dilengkapi NFC untuk melakukan akses, sehingga apabila diterapkan dalam system akses kontrol setiap *user* atau pengguna diwajibkan memiliki *smart phone* yang dilengkapi NFC. Sebagai solusi dalam penelitian yang penulis ajukan dibutuhkan *smart card* NFC sebagai pengganti *smart phone*.

Sebagian besar sistem akses kontrol berbasis RFID rentan pada resiko serangan yang memungkinkan kloning dari *tag* / kartu untuk mendapatkan akses ke fasilitas akses kontrol. Solusi untuk mengatasi resiko tersebut adalah dengan meningkatkan keamanan pada verifikasi dan otentikasi user. Penelitian Jacob *et al* (2015), menerapkan One-Time Password pada system kehadiran menggunakan NFC. One-Time Password dibuat secara otomatis dengan membangkitkan *string* karakter numerik atau alfanumerik pada otentikasi *user* untuk satu kali sesi transaksi menggunkan NFC *card* [9].

Penelitian ini membahas penggunaan NFC card pada prototipe akses kontrol *gate system* dalam lingkungan kampus Fakultas Teknik Universitas Hasanuddin. Akses keluar masuk civitas academika sebagai user dapat dikontrol melalui *gate system*. Kartu identitas berupa NFC card berisi informasi biodata civitas akademika untuk proses identifikasi dan otentikasi. NFC card yang telah teregistrasi akan melakukan proses buka tutup *gate*. Perhatian utama terkait implementasi saat ini yakni mengenai sistem keamanan informasi pada NFC *tag,* beberapa *software* yang beredar tidak dilengkapi dengan sistem keamanan informasi pada proses *write* data ke NFC *tag*. Permasalahan terkait sistem keamanan informasi pada NFC *tag* dapat diatasi dengan melakukan kriptografi enkripsi informasi ketika proses *write* pada nfc *tag*. Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan beritadengan tujuan mendasar aspek keamanan informasi yaitu *autentication,* data *integrity*, *confidentiality* dan *non repudiation* [10]. *Software* yang mampu melakukan proses *read* dan *write* serta enkripsi pada NFC *tag* diharapkan

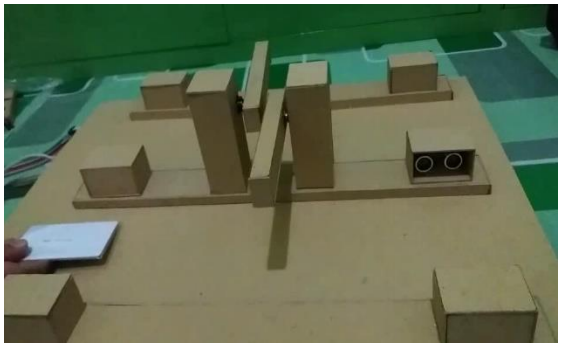
mampu menjadi solusi keamanan sistem informasi.

2. Prototipe *Gate System*

Prototipe *smart gate* terdiri dari PN532 NFC RFID module, mikrokontroller, NFC tag, sensor PING, motor servo, router, dan ethernet shield. Bagian lain pendukung dari *smart gate access control* adalah *server*. *Server* menyimpan semua data user dan riwayat akses masuk dan keluar gate. Pada prototipe yang dirancang server menggunakan *localhost*.

Proses akses masuk atau keluar gate dimulai dengan mendekatkan tag pada *reader* untuk proses *scanning*/pembacaan kartu. NFC tag yang telah terregistrasi akan diidentifikasi sebagai *user* yang berhak untuk untuk mendapatkan akses masuk atau keluar *gate*. Apabila UID terdaftar dan *key* otentikasi telah terverifikasi maka gate akan terbuka dan riwayat *user* akan terupdate pada database server. Gate akan tertutup setelah sensor PING mendeteksi objek yang ada di depannya.

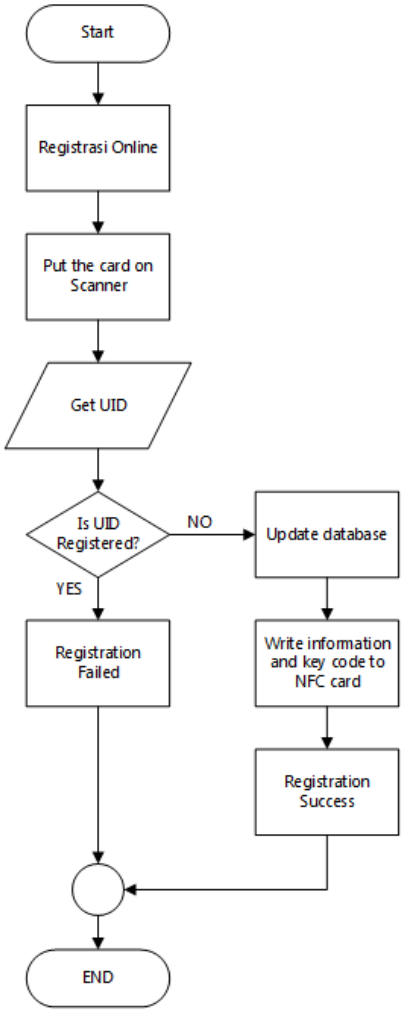
Pada NFC tag akan dituliskan kembali *key* otentikasi untuk digunakan kembali pada saat scanning kartu akses keluar gate. NFC tag hanya dapat digunakan satu kali pemakaian untuk akses masuk dalam waktu bersamaan karena adanya *re-write key* otentikasi pada kartu. Untuk akses keluar dilakukan dengan cara yang sama.



Gambar 1. Prototipe *smart gate access control*

3. Registrasi *Smart Card* pada *Smart Gate System* dengan Proses Enkripsi

Penelitian ini mengarah pada perwujudan *smart campus* sehingga dirancang dalam lingkup civitas akademika. *Smart card* yang dirancang memuat informasi identitas pengguna antara lain nama, NIM, jurusan, status, nomor telepon, dan alamat. Secara khusus, jabatan yang dimaksud adalah mahasiswa, staf, karyawan, dan dosen. Dengan adanya informasi identitas pengguna, maka pihak kampus dapat mengatur siapa yang memiliki hak untuk memanfaatkan suatu sarana dan prasarana yang ada.



Gambar 2. *Flowchart* algoritma registrasi kartu

Smart card yang digunakan adalah jenis Mifare Classic 1K yang terdiri dari 16 Sektor, dimana setiap sektor terdiri dari 4 blok yakni 3 blok data dan satu 1 blok *trailer*, dan masing-masing blok tersebut terdiri atas 16 byte [11]. Dalam penelitian ini, proses baca/tulis akan dikonfigurasi dimana blok data dapat dibaca dengan menggunakan *software* yang telah dirancang dengan menggunakan aplikasi Visual Basic (VB) 2010. Proses penulisan data pada NFC *tag* melalui komunikasi serial dimana data informasi digabungkan menjadi 1 line informasi yang telah melalui tahapan enkripsi kemudian

akan dialokasikan dalam bentuk *array* kedalam blok data yang telah ditentukan dalam penelitian ini yakni blok data 9, 10, 11 dan 13 dengan total data 64 Byte. Pada tahap pengisian informasi pada NFC *tag* dilakukan dua pihak yakni mahasiswa dan pihak administrasi kampus. Proses registrasi dijelaskan melalui *flowchart* algoritma registrasi kartu pada Gambar 2.

Tahap pertama mahasiswa melakukan pengisian biodata secara *online* dan data tersebut akan tersimpan dalam database yang dapat diakses oleh pihak administrasi kampus sebagai pihak yang melakukan verifikasi dan penulisan data pada NFC *tag*. Proses penulisan data pada NFC *tag* melalui beberapa tahap yakni verifikasi data pada database, enkripsi data dan penulisan data ke NFC *tag*. Verifikasi data yakni proses dimana pihak administrasi kampus melakukan pencarian Nomor Induk Mahasiswa (NIM) pada aplikasi VB yang telah dirancang dan dikoneksikan pada *server database* apabila NIM telah terdaftar maka secara otomatis aplikasi VB akan menampilkan informasi yang telah diisi oleh pihak mahasiswa. Informasi yang diperoleh dari database kemudian akan dilakukan proses enkripsi untuk memberikan sistem keamanan informasi pada *tag* sehingga pihak lain tidak dapat melakukan pembacaan blok data tanpa menggunakan apikasi VB dan mengetahui sistem enkripsinya.

4. Hasil dan Pembahasan

Data mahasiswa dilindungi dengan melalui 2 (dua) tahap enkripsi. Enkripsi pertama dilakukan dengan metode Caesar Chiper, metode enkripsi ini berbasis sistem pergerseran dimana huruf/karakter asli akan digantikan dengan karakter lain dan merujuk pada *key* yang telah ditentukan dengan formula enkripsi sebagai $E_n(x) = (x + n)$ dimana, $E_n(x)$ = Hasil enkripsi, X = Karakter asli N = *Key*. Sebagai contoh proses Caesar chipper yakni informasi asli KHAIRUNNISA akan dilakukkan menggunakan Caesar Chiper dengan key 24 maka informasi asli akan melalui proses enkripsi ditunjukkan pada Tabel 1.

Tabel 1. Enkripsi caesar chiper

Informasi	Key	Hasil Enkripsi
K	2	M
H	4	L
A	2	C
I	4	M
R	2	T
U	4	Y
N	2	P
N	4	R
I	2	K
S	4	W
A	2	C

Setelah melalui tahap enkripsi awal Caesar Chiper maka untuk memastikan informasi mahasiswa lebih aman maka dilakukan enkripsi tahap kedua dengan metode *rotate letter* dimana urutan karakter pada informasi dibalik secara utuh. Informasi yang mengalami enkripsi Caesar Chiper yakni MLCMTYPRKWC akan dirotasi menjadi CWKRPYTMCLM dan informasi inilah yang akan diwrite pada NFC *tag* melalui komunikasi serial dari *desktop* ke NFC *reader / write* PN532. Hasil enkripsi menggunakan VB diperlihatkan pada Gambar 3.

Gambar 3. Hasil enkripsi pada visual basic

Smart card yang dirancang berisi informasi identitas pengguna antara lain nama, alamat, nomor identitas, nomor telepon dan jabatan. Jabatan yang dimaksud adalah mahasiswa, staf, karyawan, dan dosen. Dengan adanya informasi identitas pengguna, maka pihak kampus dapat mengatur siapa yang memiliki hak untuk memanfaatkan suatu sarana dan prasarana yang ada dengan menambahkan informasi tertentu pada data blok. Pada pengaplikasiannya untuk proses

read dan *write* informasi pada NFC *tag contactless* diperoleh 2 (dua) data pengujian jarak dan waktu terhadap ada tidaknya penghalang antara *tag* dan *reader*.

Hasil penelitian menunjukkan bahwa dengan adanya proses enkripsi informasi pada NFC tag hanya dapat dibaca melalui aplikasi VB yang telah dirancang dan dilengkapi dengan sistem enkripsi dan dekripsi. Pengujian untuk waktu yang dibutuhkan dalam melakukan pembacaan informasi dari database ke NFC tag tanpa adanya penghalang antara NFC *smart card* dan *reader* yakni waktu tercepat 1.49 detik dan terlama 2.26 detik dengan rata-rata waktu proses 1.84 detik.

Tabel 2. Hasil pengujian respon waktu *smart card* pada *reader* tanpa penghalang

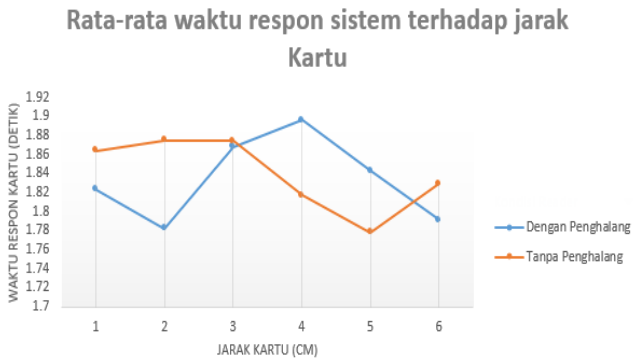
No.	Delay (Detik)					
	1 CM	2 CM	3 CM	4 CM	5 CM	6 CM
1.	1.81	1.64	1.92	2.11	1.6	1.88
2.	1.74	1.96	1.55	1.76	2.11	1.75
3.	1.86	1.91	1.67	1.62	1.84	1.63
4.	2.07	1.64	1.83	1.91	1.73	2.21
5.	1.8	1.59	2.15	2.06	1.67	1.59
6.	1.66	1.53	2.12	1.96	2.19	1.78
7.	1.8	1.93	2.2	1.88	1.75	1.61
8.	1.61	1.84	1.91	2.1	1.66	1.96
9.	1.71	1.97	1.64	1.78	2.18	1.59
10.	2.17	1.81	1.69	1.78	1.7	1.91
Delay rata-rata	1.823	1.782	1.868	1.896	1.843	1.791

Pengujian dengan menggunakan penghalang diperoleh waktu tercepat 1.53 detik dan waktu terlama 2.21 detik dengan rata-rata waktu proses 1.83 detik. Hal ini menandakan waktu yang digunakan dalam proses penulisan informasi efisien dan tidak terpengaruh oleh adanya penghalang.

Tabel 3. Hasil pengujian respon waktu *smart card* pada *reader* dengan penghalang

No.	Delay (Detik)					
	1 CM	2 CM	3 CM	4 CM	5 CM	6 CM
1.	1.69	2.22	1.9	1.42	1.58	1.97
2.	2.11	1.91	1.6	2.23	2.14	2.17
3.	1.67	1.9	1.77	1.56	1.46	1.63
4.	1.76	1.85	2.11	1.93	2.16	1.83
5.	1.95	1.7	1.88	2.2	1.67	1.88
6.	2.18	1.97	1.76	1.66	2.1	1.67
7.	1.88	1.66	2.26	1.49	1.58	1.73
8.	1.58	1.74	1.61	2.12	1.76	1.86
9.	1.75	1.89	1.92	1.88	1.61	1.89
10.	2.07	1.91	1.93	1.68	1.72	1.66
Delay rata-rata	1.864	1.875	1.874	1.817	1.778	1.829

Grafik hasil pengujian respon rata-rata sistem terhadap waktu dapat dilihat pada Gambar 4.



Gambar 4. Respon rata-rata terhadap waktu

5. Kesimpulan

Berdasarkan hasil penelitian dapat disimpulkan bahwa konfigurasi kartu dan reader sangat berpengaruh terhadap kemampuan identifikasi, waktu pemerosesan, ketahanan terhadap penghalang dan keamanan. Penelitian ini dapat dikembangkan dengan mempertimbangkan memori penyimpanan tiap blok sehingga tidak terpaku pada sistem penulisan 16 byte / blok atau 1 Kb / *tag* serta pengembangan kemampuan identifikasi NFC *tag* oleh *reader* terhadap jarak yang membuat sistem ini akan menjadi lebih responsif.

Daftar Pustaka

[1] Gerdeman J. (2015). RFID Changing Gates. IEEE Potentials Magazine. Vol (34) Vol. 40-42.
[2] Zhang T. (2012). Instrumentation, Measurement, Circuits and Systems, AISC 127, pp. 19–26.
[3] Finkenzeller, K. (2010). *RFID Handbook: Fundamentals and applications in contactless smart*

cards, radio frequency identification. 3th edition. Whiley. 2010.

[4] Tu J.F. (2016). A contactless doors lock which controlled by portable devices. International Journal for Computer- Aided Engineering and Software Vol. 33 No. 6, pp. 1631-1641.

[5] Kao L. T. & Chung H.Y. (2008). Design and Implementation of Campus Gate Control System Based on RFID. Proceedings IEEE Asia-Pacific Services Computing Conference, pp 1406 - 1411.

[6] Woo-Garcia. et al. (2016). Design and Implementation of a System Access Control by RFID", International Conference Engineering Summit, II Cumbre Internacional de las Ingenierias (IE-Summit).

[7] Bouazzouni M.A. *et al.* (2016). Trusted Access Kontrol System for Smart Campus. Proceedings International IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, pp 1006-1012.

[8] Gruntz D. *et al.* (2016). MOONACS: a mobile on-/offline NFC-based physical access kontrol system. International Journal of Pervasive Computing and Communications. Vol. 12 No. 1 2016. 2-22.

[9] Jacob J. *et al.* (2015). Mobile Attendance using Near Field Communication. International Conference on Green Computing and Internet of Things (ICGCloT) 2015, pp 1298 - 1303.

[10] Seftyanto, D. dkk. 2012. Peran Algoritma Caesar Chiper dalam Membangun Karakter Akan Kesadaran Informasi. Prosiding Seminar Nasional Matematika dan Pendidikan Matematika dengan tema Kontribusi Pendidikan Matematika dan Matematika dalam Membangun Karakter Guru dan Siswa.

[11] Product data sheet, "MF1S50yyX_V1," ©NXP Semiconductors N.V., 2014.