Optimasi dan Impelementasi Sistem *Contactless Tag-Reader* untuk Akses Kelas dan Laboratorium : Evaluasi Prototipe

Rida Ariyanti Z*[1], Elyas Palantei[1], Intan Sari Areni[1]
[1]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Hasanuddin
Jl. Poros Malino km.6 Bontomarannu, Gowa, Sulawesi Selatan, Indonesia
*Email: [1]ridaariyantizainal@gmail.com

DOI: 10.25042/jpe.052017.09

Abstrak

Smart card contactless yang ada saat ini memiliki jarak jangkau yang terbatas dengan tingkat keamanan yang masih rendah. Oleh karena itu, penelitian ini akan melakukan optimasi pada akses *user* yang lebih jauh dengan jaminan keamanan yang lebih baik. Penelitian ini akan diimplementasikan pada akses *classroom* dan *laboratory*. *Hardware* yang digunakan terdiri atas s*mart card* dan Raspberry Pi yang berfungsi sebagai *server* dan *card reader* yang dapat saling berhubungan dengan mikroprosesor. Pada *smart card* dan Raspberry tersimpan data *user* (nomor induk dan nama) yang bisa mengakses kelas atau laboratorium. Data *User* pada *smart card* tersimpan di chip yang bertindak seperti RAM (*Random Access Memory*). Chip tersebut tertanam pada *Smart card* dengan cara kerja yang sama seperti media penyimpanan. Raspberry yang bertindak sebagai *server* sekaligus sebagai mikroprosesor akan memberikan akses untuk *user* yang telah teregistrasi dengan data *base server*. Penelitian ini menghasilkan sistem akses kelas dengan menggunakan *smart card* dengan jarak >5cm dengan sistem automatis akses untuk *user* yang terdaftar pada sistem. Jika menggunakan teori LOS maka maksimal jarak yang dapat dicapai adalah 12cm. *Historical* tersimpan pada *server* yang mencatat waktu *in* dan *out*, serta durasi waktu selama berada di ruangan. Teknologi tambahan pada sistem akses *classroom* ini dilengkapi dengan sistem *close door* otomatis untuk *double security* pada *classroom*. Kelebihan sistem ini adalah menggunakan *server* sekaligus sebagai mikrokontroller sehingga lebih murah dibandingkan teknologi *smart card* akses yang tersedia saat ini. Sebagai aplikasi tambahan, sistem ini dilengkapi dengan sistem monitoring jarak jauh sehingga tingkat keamanan ruangan dapat dikendalikan dimanapun dan kapan pun.

Abstract

Optimation and Implementation of Contactless Tag-Reader System for Class and Laboratorium Access: Prototype Evaluation. The existing contactless smart cards have limited coverage with low security levels. Therefore, this research perform optimization on user access further with better security assurance. This research implemented in classroom and laboratory access. Hardware that used consists of Smart cards and Raspberry Pi that serves as a server and card reader that could be interconnected with the microprocessor. On the smart card and Raspberry stored user data (registration number and name) that could access the class or laboratory. User's data on smart cards were stored on chips that used RAM (Random Access Memory). The chip was embedded in the Smart card in the same function as storage media. Raspberry that had function as server and microprocessor that provide access to registered users. This study produced classroom access system by using smart card with distance > 5cm with automatic access system for user registered on system. It was according to this research proposed about security and historical data. Historical data stored on the server (Raspberry pi) which records the time in and out, and the duration of time while in the room. Additional technology in the classroom access system is equipped with an automatic door close system for double security in the classroom. The advantages of this system was using server and microcontroller in one package so that it is cheaper than the smart card access technology available today. This sistem has new feature to long distance monitoring for controlling anywhere and everywhere.

Kata kunci: *Contactless, microcontroller, Raspberry Pi, Reader, Smart card*

1. Pendahuluan

Smart card merupakan kartu yang memiliki chip sebagai peyimpanan data yang dapat digunakan untuk sistem akses jaringan, menyimpan nilai dan data lainnya [1]. Teknologi *smart card* didukung oleh kemajuan teknologi komunikasi nirkabel sehingga *smart card* dapat dibuat menjadi *contactless* untuk memudahkan user dalam akses atau pengontrolan. Transmisi data terbuka melalui sistem nirkabel menimbulkan tantangan keamanan, yaitu otentikasi dan privasi *user* [2].

Penelitian sebelumnya tentang *contactless smart card* yang hanya berfokus pada akses file

untuk print data dan evaluasi pada tag [3, 4], yang kemudian dikembangkan akses file pada sistem penyimpanan *cloud* tetapi belum ada jaminan keamanan *user* [5, 6]. Penelitian kemudian berkembang di tahun 2016 yaitu memastikan keamanan data dengan sistem *remote* dan menggunakan ID yang dinamis (berubah-ubah) [7] dan *remote server* memverifikasi legitimasi dari pengguna melalui saluran komunikasi yang terbuka dan tidak aman [8]. Penelitian tersebut sudah terfokus pada otentikasi tetapi belum melakukan sistem akses dengan menggunakan mikrokontroller. Oleh karena itu, penulis melakukan penelitian yang diimplementasikan pada kehidupan sehari-hari dalam bidang akademis, yaitu akses kelas dan laboratorium. Sistem akses kelas dan laboratorium yang menggunakan *smart card* dengan optimasi pada jarak betujuan untuk memudahkan *user* dalam akses serta tambahan algoritma keamanan kelas yang tinggi, yaitu pintu tertutup otomatis. Komputer *host* (dalam penelitian menggunakan Raspberry) dan *card reader* dapat saling berhubungan dengan mikroprosesor [3].

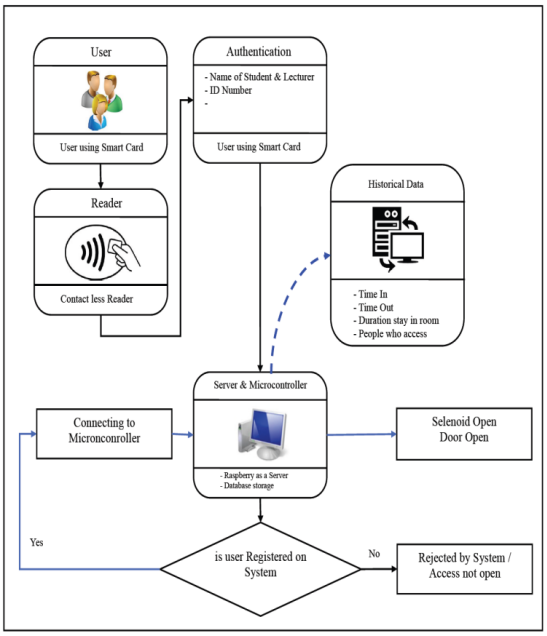
2. Penelitian Terkait

Penelitian dan implementasi *smart card* telah berkembang dari tahun ke tahun. Sebelumnya telah dilakukan penelitianyang menggunakan *contactless* dan IC *smart card* sebagai media untuk otentikasi identitas, menganalisa kondisi dan cara untuk sistem *cloud print*, dan penelitian teknologi *driver key print*, enkripsi data, otentikasi identitas ke pusat print oleh Wu Yun [4]. Penelitian lainnya adalah fokus pada smart card dengan *interface contactless* karena lebih sederhana. Dengan menggunakan Mifare DESFire mampu menemukan beberapa kelemahan dari *smart card* yang dapat menyebabkan kerentanan jika protokol tersebut tidak dilaksanakan dengan baik. Metode ini dapat digunakan oleh peneliti untuk mengevaluasi keamanan pelaksanaan protokol pada beberapa jenis *smart card* [5]. Sedangkan untuk metode *Unified* RB-DAC untuk akses file pada *cloud computing* menggunakan *smart card*. RBDAC ini adalah sistem dimana semua *user* dapat mengakses data yang ditentukan untuk kebutuhan tertentu, tetapi tidak bisa menentukan alokasi data untuk setiap *user*. Dengan demikian untuk mencapai hal tersebut, ditambahkan ACL untuk semua objek (data) dan ACM untuk semua objek dalam sistem [6]. Penelitian terkait *smart car*d tentang otentikasi pengguna jarak jauh dengan mekanisme dimana *server* memverifikasi legitimasi dari pengguna melalui saluran komunikasi yang terbuka dan tidak aman. Otentikasi sandi menggunakan *smart card* telah menjadi salah satu metode yang umum diadopsi untuk melindungi *password* selama proses transmisioleh Zhengxian Gao, dkk. [7].

Berdasarkan penelitian tersebut maka, penelitian ini merupakan optimasi dari penelitian sebelumnya. Penelitian sebelumnya telah mengalami perkembangan menggunakan *smart card* dengan *reader contactless*, namun dengan jarak yang terbatas dan keamanan yang rendah. Pengembangan yang dilakukan adalah menggunakan *server* sekaligus sebagai mikrokontrollernya. Dalam bidang akademisi, keamanan ruangan kelas atau laboratorium merupakan hal yang sangat penting, sehingga dilakukan pengembangan pada sistem dengan menambahkan aplikasi untuk *history user* yang menggunakan ruangan, jam masuk, jam keluar serta durasi *user* berada di dalam ruangan.

3. Desain Sistem

Algoritma yang digunakan pada sistem akses ini adalah sebagai berikut:



Gambar 1. Algoritma akses kelas dan laboratorium

Gambar 1 menunjukkan Algoritma pada sistem akses ruangan kelas dan laboratorium. *User* yang telah terdaftar pada sistem dan tersimpan pada *server* mengakses dengan cara mendekatkan tag pada *reader*. Selanjutnya proses otentikasi apakah *user* tersebut bisa mengakses atau tidak. Sesuai dengan prosedur yang diprogramkan, jika *user* tidak terdaftar, maka pintu tidak akan terbuka. Sedangkan, jika *user* tersebut terdaftar, maka pintu yang menggunakan solenoid dan terhubung pada mikrokontroller akan secara otomatis terbuka.

Secara garis besar, sistem ini terdiri atas dua bagian yaitu perancangan sistem dan pengujian sistem.

3.1. Perancangan Sistem

Raspberry Pi adalah modul mikro komputer yang juga mempunyai input *output* digital port seperti mikrokontroller. Kelebihan Rasberry Pi dibanding mikrokontroller yang lain yaitu mempunyai Port/koneksi untuk *display* berupa TV atau Monitor PC, koneksi USB untuk Keyboard dan Mouse serta memiliki 26 pin I/O digital [8].

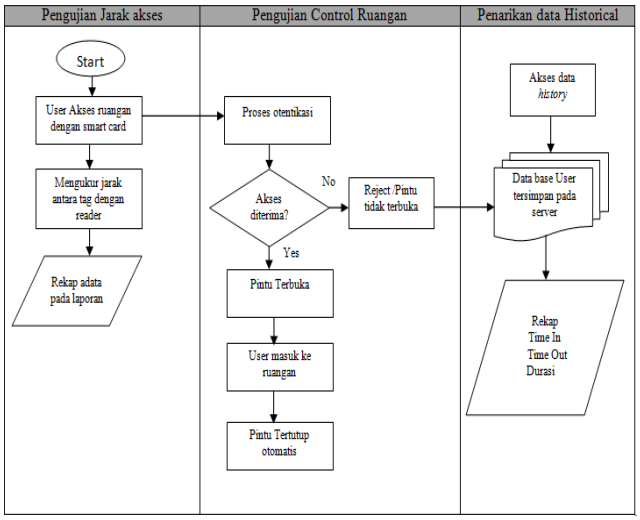
Pembuatan sistem akses ruangan memiliki beberapa tahap, yaitu:

- Memasukkan informasi pada *smart card* (nama, nomor induk mahasiswa / dosen).
- Pemasukan data base pada *server* yaitu *user* yang bisa mengakses yang terdiri atas nama dan nomor induk.
- Pemrograman sistem akses dengan detail *time in , time out, duration.* Sehingga pada saat dilakukan akses data *historical* bisa muncul pada layar.

Sebagai mikrokontroller, Raspberry dikoneksikan dengan solenoid sehingga pintu secara otomatis bisa terbuka saat proses otentikasi selesai.

Pin GPIO dapat dikonfigurasi sebagai input. Koneksi dari GPIO untuk tegangan yang lebih tinggi dari 3.3V kemungkinan akan menghancurkan blok GPIO dalam SoC [9]. Selain sebagai input output pada beberapa pin GPIO juga berfungsi sebagai komunikasi serial diantaranya I2C, SPI dan serial komunikasi UART [10].

3.2. Pengujian Sistem



Gambar 2. Diagram pengujian sistem

Gambar 2 menunjukkan suatu uji sistem yang terdiri dari 3 skenario pengujian yang mengukur jarak tag pada pembaca, sistem akses ruangan dimana saat setelah pengguna mengakses ruangan, pintu akan ditutup secara otomatis. Skenario terakhir adalah mengakses data historis yang tersimpan di *server*. Data berupa waktu, waktu dan durasi pengguna berada di dalam ruangan. Hal ini memungkinkan administrator atau *Person* bertugas mengawasi ruangan. Keamanan ruangan akan dipastikan dengan fitur tambahan yang otomatis menutup pintu saat pengguna memakan waktu terlalu lama untuk memasuki ruangan.

Hasil pengukuran jarak akan dibandingkan dengan perhitungan *Line Of Space* atau *Line Of Straight* (LOS). LOS merupakan garis padang lurus antara 2 titik yang tidak boleh terhalang. Kondisi ini harus dipenuhi untuk memperoleh hasil yang optimal dalam pengiriman sinyal. Pada jarak tertentu tinggi sinyal langsung yang merambat dari pemancar ke penerima dapat dihitung . Selain itu tinggi *obstacle* maksimum yang dapat menghalangi perambatan sinyal pada tempat tersebut dapat dihitung.

LOS dapat diperoleh melalui persamaan berikut :

$$X = \sqrt{h_{Tx}} + \sqrt{h_{Rx}} \qquad (1)$$

Dimana

X : Jarak LOS
h_{Tx} : Tinggi antena pengirim
h_{Rx} : Tinggi antena penerima

Disekitar garis lurus (LOS) antar perangkat wireless yang digunakan sebagai area media rambat frekuensi yang disebut juga dengan zona fresnel [11].

4. Hasil Pengujian Prototipe

Pengujian yang dilakukan adalah pengujian jarak dan pengujian keamanan ruangan.

4.1. Hasil Pengujian Jarak

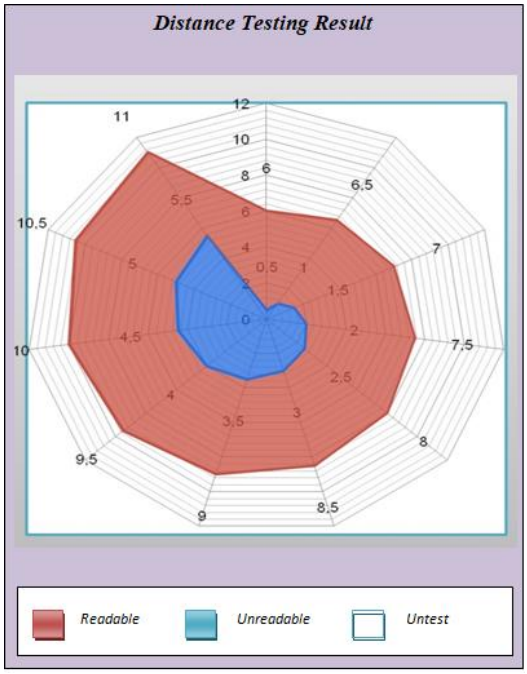
Dari hasil pengujian diperoleh jarak akses sebagai berikut :

Tabel 1. Rincian data yang direkam oleh sistem *smart classroom*

Jarak (cm)	System Testing Results		
	Terbaca	Tidak Terbaca	Pintu Terbuka (Ya / Tidak)
0.5	√	-	Ya
1	√	-	Ya
1.5	√	-	Ya
2	√	-	Ya
2.5	√	-	Ya
3	√	-	Ya
3.5	√	-	Ya
4	√	-	Ya
4.5	√	-	Ya
5	√	-	Ya
5.5	√	-	Ya
6	-	√	Tidak
6.5	-	√	Tidak
7	-	√	Tidak

Pengujian jarak dilakukan dengan cara mendekatkan *tag* ke *reader*. Hasil pengujian dapat dilihat pada Tabel 1 yang menunjukkan bahwa jarak maksimum pembacaan *reader* adalah 5,5 cm. Hal ini menunjukkan sistem yang digunakan telah menggunakan sistem *contactless*karena tidak perlu *tag* ditapkan atau menempel pada *reader*.

Jangkauan dari *tag* yang diukur dari jarak deteksi dengan *reader* diperoleh bahwa maksimal *reader* dapat membaca pada jarak 5cm.



Gambar 3. Jangkauan *tag-reader*

Gambar 3 menunjukkan bahwa semakin jauh jarak maka kemampuan *reader* akan semakin berkurang. Garis berwarna biru menunjukkan paling jauh jarak jangkauan *reader* adalah 5cm, sedangkan garis berwarna menunjukkan *reader* sudah tidak membaca *tag* pada jarak >5,5 cm atau pada grafik area yang diberi warna merah. Pengujian dilakukan dari angka 0,5 cm sampai 7 cm dengan jarak per 0,5 cm, sedangkan pada jarak >7 cm sudah tidak dilakukan pengujian seperti yang ditunjukkan pada gambar area yang berwarna putih.

Pada pengujian *smart classroom* tinggi *reader* dipasang sesuai dengan tinggi ideal yang dapat diakses oleh orang. Sehingga, di pastikan di angka 150cm. Berdasarkan Persamaan 1 dimana X adalah LOS maka, diperoleh :

$$X = \left(\sqrt{h_{Tx}} + \sqrt{h_{Rx}}\right)$$

$$X = \left(\sqrt{150} + \sqrt{150}\right)$$

$$X = (12,24 + 12,24)$$

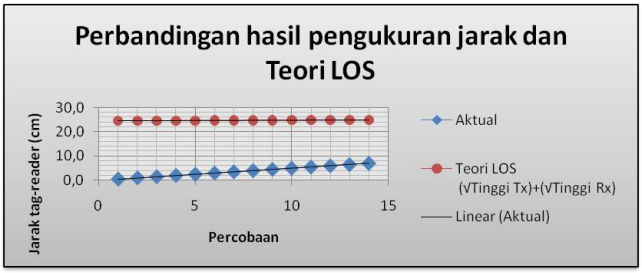
$$X = 24,48$$

Dari perhitungan LOS diperoleh 24,48 cm. Artinya, area coverage *reader* adalah 24,48 cm atau 12,24 cm dari arah depan dan 12,24 dari arah belakang.

Tabel 2. Analisa jarak aktual dan berdasarkan perhitungan LOS

Percobaan	Jarak (cm)	Teori LOS (cm)
1	0,5	24,5153
2	1,0	24,5357
3	1,5	24,5560
4	2,0	24,5763
5	2,5	24,5965
6	3,0	24,6168
7	3,5	24,6370
8	4,0	24,6571
9	4,5	24,6773
10	5,0	24,6973
11	5,5	24,7174
12	6,0	24,7374
13	6,5	24,7574
14	7,0	24,7774

Tabel 2 memperlihatkan bahwa jarak paling dekat antara *tag* dan *reader* adalah 0.5cm sedangkan jarak terjauh adalah 5.5cm. Dari hasil percobaan tersebut dapat dilihat perbandingan jarak aktual dan perhitungan teori LOS pada Gambar berikut :



Gambar 4. Grafik perbandingan hasil pengukuran aktual dan secara teori LOS

Pada Gambar 4 terlihat hasil pengukuran yang diambil sesuai dengan Tabel 3. Pengambilan data dilakukan dengan perbedaan jarak 0,5 cm. Dilakukan sebanyak 14 kali hingga *tag* dan *reader*berada pada jarak 7 cm. Berdasarkan perhitungan secara teori LOS, jarak yang bisa dicapai adalah 12,24 cm namun aktual maksimal yang bisa dideteksi *reader* adalah 5,5cm.

4.2. Pengujian Solenoid

Pengujian pada *solenoid door lock* dilakuan pada *tag* yang telah terdaftar dan belum terdaftar pada *database*.

Solenoid berfungsi dengan baik dengan membuka lock solenoid saat *tag* yang terdaftar didedaktkan pada *reader* baik saat check in maupun *check out* dari kelas. Penujian dilakukan pada *tag* yang tidak terdaftar dan yang terdaftar. Terbukti bahwa *user* yang tidak terdaftar akan tetap terekam pada sistem dengan nama "*unregistered card"*.

Tabel 3. Rincian tampilan user tidak terdaftar

Percobaan	No. Kartu	Tanggal/Waktu
1	115-12-9-1	29-07-2017/08:06:46
2	194-199-245-252	29-07-2017/08:07:25
3	34-45-15-253	29-07-2017/08:08:11

Tabel 3 memperlihatkan sistem akan menunjukkan berapa kartu yang tidak terdaftar yang mengakses ruangan dan frekuensi *user* mencoba mengakses *ruangan*.

4.3. Pengujian Durasi

Hasil pengujian ditampilkan dalam *form*at berupa (jam : menit : detik). Pengukuran durasi dapat dilihat pada persamaan berikut :

Durasi = Waktu keluar - Waktu masuk (2)

Pengujian ini dilakukan pada salah satu kartu atas nama Enal Roffca dimana pada pengujian pertama saat masuk pada pukul 06:16:34 dan keluar pada pukul 06:17:19. Berdasarkan Persamaan 2 selisih waktu pada pengujian adalah 45 detik. Hal ini menunjukkan bahwa rekaman durasi detail sampai pada detik.

Tabel waktu yang tecatat adalah tabel waktu masuk, waktu keluar, dan durasi waktu. Pada pengaturan awal, semua tabel kosong. Dan saat *user* melakukan *scan* untuk masuk maka tabel waktu masuk akan di update dengan waktu pada sistem raspberry saat *user* melakukan scan.

Gambar 5. Tampilan awal absen

Seperti pada Gambar 5, tampilan sistem masih dalam keadaan tidak ada *user* yang mengakses. Saat *user* melakukancheck in, maka

akan muncul rekapan absen seperti pada Gambar 6.

Gambar 6. *User* check in

Pada Gambar 6 *user* melakukan *check in* pada pukul 06:16:34 namun belum melakukan *check out*. Artinya, selama waktu tersebut *user* masih berada di dalam ruangan. Pada tabel durasi waktu masih 0 karena waktu *check out* masih belum terekam dalam sistem. Saat melakukan *check out* sistem akan mendeteksi waktu *check out dan* secara otomatis akan muncul durasi berada di ruangan dan tabel durasi akan di *update* sesuai dengan waktu *check out*. Selisih waktu akan otomatis dihitung ketika waktu masuk dan waktu keluar terisi dan tercatat sebagai durasi.

5. Kesimpulan

Dari hasil penelitian dan analisa yang telah dilakukan, disimpulkan bahwa pembuatan prototipe dan pengujian sistem *smart classroom* maksimal jarak *tag* ke *reader* terdekat 0,5cm dan terjauh 5,5 cm. Jika dibandingkan dengan perhitungan secara teori LOS jarak terdekat 12,2 cm dan jarak terjauh adalah 12,3cm. Percobaan *prototype* dengan menggunakan solenoid menunjukkan bahwa saat *user* yang terdaftar mengakses masuk dan keluar maka solenoid secara otomatis terbuka dan tercatat pada sistem, sedangkan *user* yang tidak terdaftar pada sistem mengakses maka solenoid tidak akan terbuka dan akan tercatat pada sistem. Percobaan sistem keamanan dengan menggunakan 3 kartu yang tidak terdaftar tercatat detail waktu dan nomor kartu nomor yang mencoba mengakses ruangan, tetapi ditolak oleh sistem dan tercatat.

Ucapan Terimakasih

Penelitian ini dibantu oleh anggota Komunitas Cyber Tech Jurusan Elektro Universitas Hasanuddin.

Referensi

[1] M. Wassim Raad, Tarek Sheltami ,M. Sallout, “A Smart card Based Prepaid Electricity System”, IEEE [Pervasive Computing and Applications, 2007. ICPCA 2007. 2nd International Conference].

[2] Alavalapati Goutham Reddy, Eun-Jun Yoon, Ashok Kumar Das, Kee Young Yoo, “Lightweight Authentication With Keyagreement Protocol For Mobile Network Environment Using Smart Cards”, IEEE [The Institution of Engineering and Technology 2016].

[3] Agnes C. Noubissi, Julien Iguchi-Cartigny, Jean-Louis Lanet, “Hot Updates for Java Based Smart cards”,IEEE, 2011 [ICDE Workshops].

[4] Wu Yun, “Research of Cloud Print Key Technology Base on Identity “. IEEE, 2012 [Third World Congress on Software Engineering].

[5] Matej Kacic, Petr Hanacek, Martin Henzl, Ivan Homoliak, “A concept of behavioral reputation system in wireless networks”, IEEE, 2013 47th International Carnahan Conference on Security Technology (ICCST).

[6] B. Linkesh, S.Durga, E. Chowdary, Unified RB-DAC Approach With Secure Authentication Using Smart card Architecture, IEEE [2014 3rd International Conference on Eco-friendly Computing and Communication Systems].

[7] Shanu Gaharana, Darpan Anand, “Dynamic ID Based Remote User Authentication In Multi Server Environment Using Smart cards: A Review”, IEEE, 2015, International Conference on Computational Intelligence and Communication Networks (CICN).

[8] Zhengxian Gao, Shou Hsuan Stephen Huang, Wei Ding, “Cryptanalysis of Three Dynamic ID-Based Remote User Authentication Schemes Using Smart cards”, 2016, IEEE International Conference of Online Analysis and Computing Science (ICOACS).

[9] Qihao He; Bruce Segee; Vincent Weaver, “Raspberry Pi 2 B+ GPU Power, Performance, and Energy Implications”, IEEE, 2016 International Conference on Computational Science and Computational.

[10] Vamsikrishna Patchava, Hari Babu Kandala, P Ravi Babu, “A Smart Home Automation technique with Raspberry Pi using IoT”, IEEE, 2015, International Conference on Smart Sensors and Systems (IC-SSS).

[11] Muhadir. Rancang Bangun Sistem Identifikasi Kendaraan Pada Akses Masuk Menggunakan Teknologi RFID. 2008. Depok: Departemen Teknik Elektro Fakultas Teknik, Universitas Indonesia.