Implementasi Skema Lamport Pada RFID Berbasis Arduino Mega 2560 Pada Sistem Kendali Akses Personel
(Studi Kasus Perguruan Tinggi XYZ)

Therania Dina Puspitasari [1)], Yose Supriadi [2)]

[1)]Badan Siber dan Sandi Negara Jakarta, Indonesia
[2)]Sekolah Tinggi Sandi Negara Bogor, Jawa Barat
Email : theraniadinapuspitasari@gmail.com

Abstrak. *Perkembangan teknologi informasi pada suatu kendali akses (Access Control) membutuhkan suatu pengamanan yang dalam mekanisme sistemnya. Hal tersebut dapat diantisipasi dengan menggunakan teknologi RFID yang dikombinasikan dengan password, namun kombinasi tersebut memiliki kerawanan yaitu kartu RFID yang dapat diduplikasi. Oleh karena itu untuk mengatasi hal tersebut, digunakan Skema Lamport untuk menghasilkan password yang dinamik sehingga sulit mendapatkan password yang sesungguhnya karena menyimpan password dari hasil fungsi hash yang berbeda, selain itu dapat digunakan untuk mengidentifikasi apabila terjadi duplikasi pada kartu RFID. Penelitian ini dilakukan pada salah satu Perguruan Tinggi yang mempunyai fasilitas asrama dan sistem kendali akses ini digunakan untuk proses autentikasi keluar masuk kampus. Penelitian ini menghasilkan prototipe sistem kendali akses yang menggunakan RFID berbasis Arduino, Skema Lamport sebagai fungsi hash password dan database server berbasis web untuk menyimpan hasil hash serta proses autentikasinya. Hasil prototipe tersebut setelah dilakukan beberapa pengujian dapat dijadikan sebagai salah satu altenatif solusi untuk mengantisipasi kerawanan pada pengamanan personel pada kampus tersebut.*

Kata kunci*: RFID, Skema Lamport, Arduino Mega 2560, Access Control.*

1. Pendahuluan
1.1 Latar Belakang

Teknologi informasi didefinisikan sebagai perpaduan antara teknologi komputer dan telekomunikasi dengan teknologi lainnya seperti perangkat keras (*hardware*), perangkat lunak (*software*), *database*, *teknologi* jaringan, dan peralatan telekomunikasi lainnya [1]. Pemanfaatan *hardware*, *database*, dan jaringan dalam suatu organisasi dapat digunakan sebagai kendali akses dalam rangka pengamanan personel dan kepatuhan, sebagai contoh pada akses ruang *server* [2] dan kendali akses absensi pegawai [3]. Dalam rangka untuk memenuhi aspek kepatuhan sistem kendali akses juga dapat digunakan pada berbagai institusi, diantaranya institusi pendidikan.

Kendali akses sebagian besar digunakan pada aspek *Physical Security*, hal ini dilakukan untuk membatasi akses dari personel yang tidak memiliki kewenangan atau menjaga kepatuhan terhadap kebijakan yang telah diterapkan pada suatu organisasi. Salah satu teknologi untuk menerapkan kendali akses adalah dengan menggunakan s*martcard* yang berbasis *Radio Frequency Identification* (RFID) [6]. RFID mempunyai kemampuan untuk identifikasi, *alerting*, *monitoring* (pemantauan) dan autentikasi [7]. Selain itu RFID dapat menyimpan kunci privat (*private key*) [8, 9]. Pada penerapannya penggunaan RFID pada umumnya dikombinasikan dengan *password* [10, 11]. *Password* adalah salah satu mekanisme autentikasi yang paling sederhana dan mudah [12]. Namun, penggunaan *password* mempunyai kerawanan antara lain *guessing attack* (menebak *password* yang digunakan) dan *shoulder surfing attack* (mengamati secara langsung pengguna ketika memasukkan *password*) [13]. Kerawanan tersebut dapat diatasi menggunakan strong *password* yaitu dengan membangkitkan *password* menggunakan fungsi *hash*. Kombinasi menggunakan password yang sudah di *hash* masih memiliki kerawanan berupa duplikasi (*cloning*) kartu RFID sehingga jaminan autentikasi menurun karena ancaman tersebut. Untuk mengantisipasinya maka digunakan skema Lamport yang diimplementasikan pada Arduino Mega 2560 [9].

Skema Lamport *merupakan* skema untuk autentikasi menggunakan rangkaian *password* yang sudah dienkripsi dengan sistem *hash* pada saat proses inisiasi awal. *Password* yang digunakan selalu berubah dengan menggunakan fungsi *hash* dengan metode *One Way Function* (OWF) setiap kali digunakan sehingga sulit memperkirakan *password* yang sebenarnya. Hasil dari enkripsi *password*

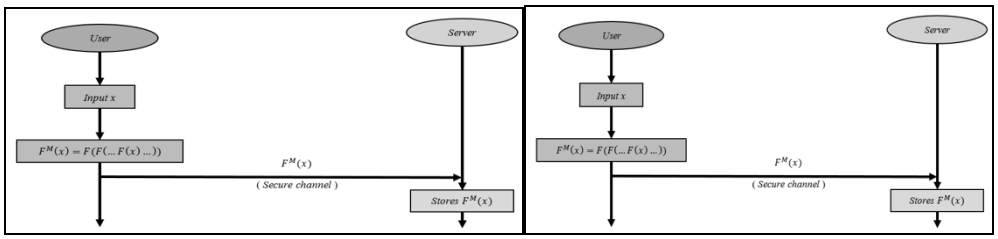
digunakan sebagai *strong password*, sehingga penggunaan Skema Lamport dapat mengatasi kerentanan penggunaan *password*. Selain itu, dengan diterapkannya Skema Lamport, dapat mengidentifikasi terjadinya duplikasi terhadap kartu dengan menggunakan algoritma SHA-256 karena algoritma ini mempunyai ketahanan terhadap serangan dan panjang bit terpendek [9] [14]. Hasil penelitian tersebut berupa prototipe dengan menggunakan Arduino Mega 2560. Pada penelitian ini protipe tersebut akan dihubungan dengan sistem informasi berbasis web untuk mengatur autentikasi pengguna dan waktu masuk akses serta masa kadaluarsa dari kartu kendali akses tersebut.

Studi kasus penerapan teknologi tersebut dilakukan pada sebuah perguruan tinggi yang berasrama dan mempunyai peraturan kehidupan berasrama diantaranya keluar masuk kampus dengan melakukan perizinan. Sebelumnya masih menggunakan mekanisme *paper and pencil* untuk proses perizinannya.. Pada mekanisme tersebut, terdapat permasalahan berupa kesalahan penulisan, modifikasi dan terjadinya antrian mahasiswa saat menuliskan identitas pada buku laporan. Dengan penerapan sistem kendali akses dengan menggunakan RFID berbasis Arduino Mega 2560 sebagai kartu kendali akses sekaligus tanda pengenal yang dilengkapi dengan skema Lamport serta sistem informasi perizinan sebagai aplikasi pengendali dan pengawasan proses keluar masuk mahasiswa diharapkan dapat menjadi salah satu solusi kerangka *physical security* pada kampus dimaksud,. Untuk membuat protipe sistem kendali akses ini digunakan metode pengembangan *software* yaitu SDLC dengan model *prototyping* agar prototipe yang dihasilkan dapat diperbaiki dan sesuai dengan kebutuhan.

1.2 Landasan teori

a. Skema Lamport

Skema *Lamport* adalah skema autentikasi yang digunakan untuk mengatasi kelemahan pada *password* [17]. Terdapat dua proses pada skema lamport yaitu tahap registrasi dan tahap autentikasi [18] yang dapat dilihat pada Gambar 1.



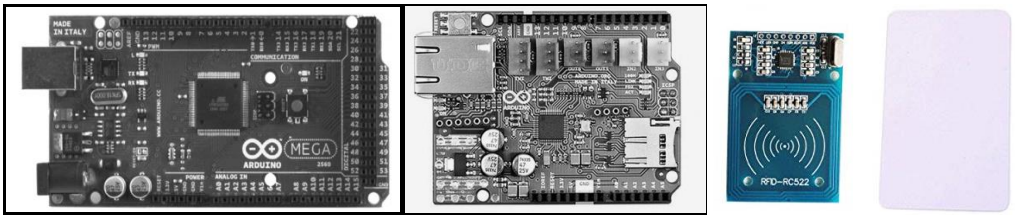
Gambar 6. Skema Lamport tahapan registrasi dan autentikasi [19]

b. Algoritma SHA-26

Algoritma SHA-256 merupakan algortima hash yang memiliki sifat *preimage resistance, 2nd-preimage resistance* [14]. Sifat tersebut merupakan ciri-ciri dari OWHF [15]. SHA-256 dapat digunakan dalam mendukung Skema Lamport, selain itu SHA-256 baik digunakan pada perangkat keras karena efisien dalam implementasi yang mengurangi kekuatan dalam pemakaian pada perangkat [17].

c. RFID, Arduino Mega 2560 dan PHP MySql

Penggunaan kartu RFID sebagai kartu kendali akses, Arduino Mega 2560 sebagai *reader, writer* dan membangkitkan *password* yang di *hash* dengan menggunakan skema Lamport serta menyimpan hasilnya di *database server* menggunakan *Ethernet Shield* . Selain itu digunakan PHP MySQL sebagai *database server* untuk menyimpan penyimpanan nilai *hash* setelah dilakukan registrasi atau inisialisasi nilai *hash* terakhir serta autentikasi waktu keluar masuk kampus.

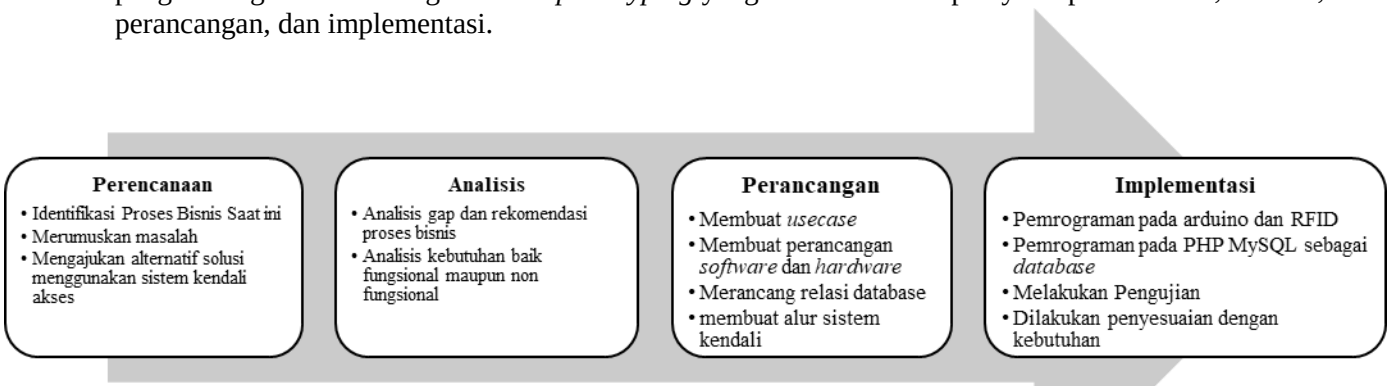


Gambar 2. Arduino Mega 2560, Ethernet Shield dan Kartu RFID

2. Pembahasan

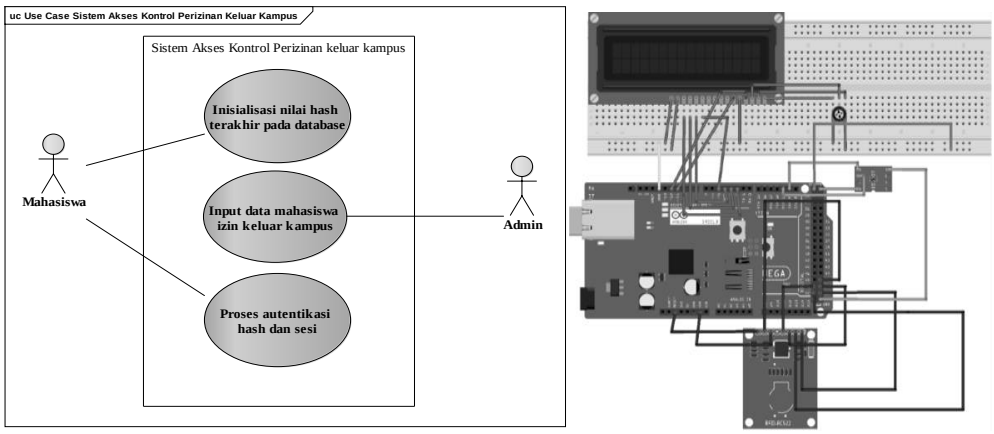
2.1. Metodologi Penelitian

Pada Gambar 3 merupakan kerangka pemikiran dalam implementasi Skema Lamport pada RFID sebagai kendali akses keluar masuk kampus. Kerangka penelitian ini berdasarkan metodologi pengembangan SDLC dengan model *prototyping* yang memiliki 4 tahapan yaitu perencanaan, analisis, perancangan, dan implementasi.



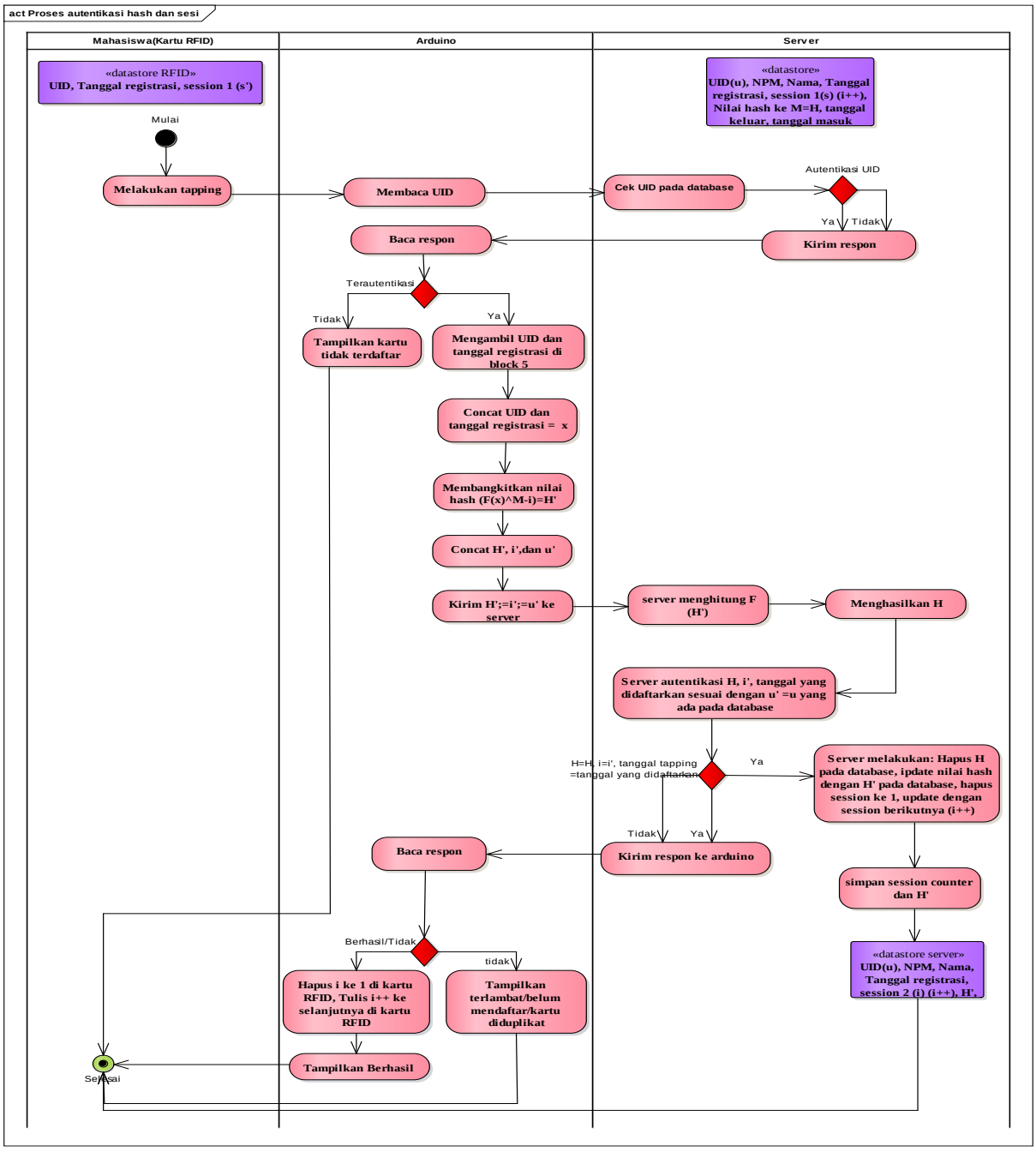
Gambar 3 Metodologi Penelitian SDLC *Prototyping*

Pada proses perencanaan dan analisis dihasilkan suatu rekomendasi proses bisnis ketika mahasiswa keluar masuk kampus yaitu dengan menggunakan kartu kendali akses sebagai autentikasinya dan sebagaimana telah dijelaskan sebelumnya, digunakan skema Lamport untuk mengantisipasi potensi kerawanan yang ada. Sistem kendali akses ini dirancang menggunakan UML (*Unified Model Language)* untuk perancangan perangkat lunak dan aplikasi *fritzing* untuk perancangan pada perangkat keras. Proses *prototyping* dilakukan setelah tahap pengujian dan selanjutnya dilakukan perbaikan agar sesuai dengan kebutuhan.



Gambar 4 Perancangan perangkat lunak dan perangkat keras

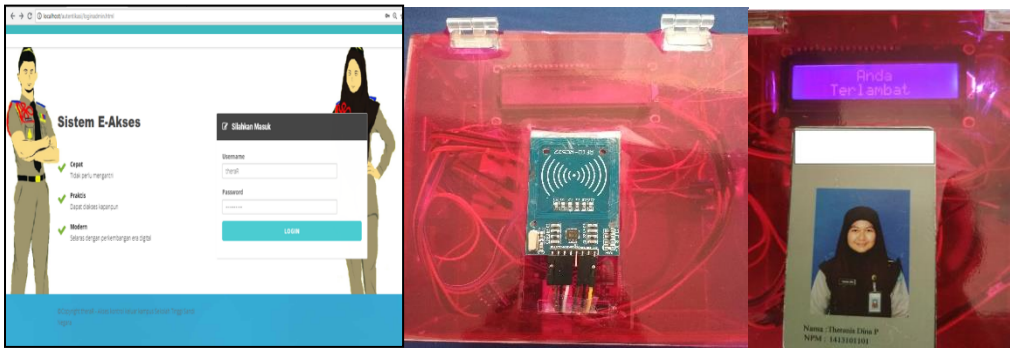
Secara umum salah satu mekanisme proses sistem kendali akses yaitu pada saat mahasiswa keluar kampus seperti ditunjukan *activity diagram* pada Gambar 5. Mahasiswa yang ingin keluar kampus melakukan *tapping* dengan menggunakan kartu kendali akses di Pos Pengamanan Dalam setelah mendapatkan izin dari Admin.



Gambar 5 *Activity Diagram* sistem *e*-akses

2.2. Implementasi dan Pengujiannya

Dengan menggunakan metode *prototyping* dalam proses pemrogramannya ditemukan beberapa kendala baik pada saat melakukan pemrograman pada Arduino maupun pada aplikasi web diperlukan 3 kali tahapan untuk menghasilkan prototipe yang sesuai dengan kebutuhan. Adapun tampilan awal pada aplikasi sistem e-akses dan *output* perangkat keras tersebut seperti yang ditunjukan pada Gambar 6.



Gambar 6 Halaman *login* admin dan produk sistem kendali akses

Secara garis besar terdapat 2 proses pemrograman yang dilakukan yaitu pada Arduino Mega 2560 dsan PHP MySQL sebagai aplikasi antarmuka sekaligus database untuk menyimpan hasil UID RFID dan sesi iterasi proses hash yang dilakukan. Pada Arduino Mega 2560 pemrograman yang dilakukan adalah fungsi baca dan tulis pada kartu RFID serta pembangkitan nilai hash dengan Skema Lamport sesuai iterasinya. Gambar 7 merupakan *sourcecode* dan hasil pada pemrograman di Arduino Mega 2560. Sedangkan pada permrograman PHP My SQL fitur untuk mendukung proses sistem kendali akses ini dibuat fitur-fitur sesuai dengan fungsi CRUD sebagaimana ditampilkan pada Tabel 1.

Gambar 7 Hasil iterasi nilai *hash*, *sourcecode* pembangkit fungsi *hash* dan hasil tulis baca pada Arduino

Tabel 1 Fungsi CRUD Pada Pemrogramanan PHP MySQL

Create	Read	Update	Delete
1. Membuat akun admin 2. Perizinan keluar masuk kampus 3. Registrasi mahasiswa 4. Pendaftaran Mahasiswa 5. Log penggunaan *hash*	1. Membaca UID pada kartu RFID 2. Membaca hasil pembangkitan dari fungsi *hash* Skema Lamport di Arduino 3. Membandingkan nilai *hash*	1. Melakukan perubahan data mahasiswa 2. Melakukan penyimpanan nilai *hash* terakhir dan sesinya 3. Melakukan perubahan data mahasiswa melakukan keluar masuk kampus	1. Menghapus data mahasiswa 2. Menghapus data perizinan 3. Menghapus akun admin

Untuk pengujian sistem kendali akses ini dilakukan berdasarkan tahapan metode *prototyping*, diantaranya pengujian test vektor hasil dari pembangkitan nilai hash yang dilakukan pada Arduino, dibandingkan dengan fungsi pada PHP dan aplikasi *HASHCALC* dengan input yang sama sebagaimana tertera pada Tabel 2. Hal ini dilakukan untuk memverifikasi hasil pembangkitan nilai hash agar sesuai dengan Skema Lamport.

Tabel 2 Tes Vektor Pembangkitan Nilai Hash

Input	Iterasi	Hasil pembangkitan nilai hash di Arduino dengan *input*-an sebagi *string* setiap proses pembangkitan	Hasil pembangkitan nilai *hash* di PHP	Hasil pembangkitan nilai *hash* dengan aplikasi *HASHCALC* dengan *input*-an *text string*.	Hasil akhir
"AKSES KONTROLSTSN"	1	6d5c5f835aea965ac6ceeea7318ea3432066443e99638fbad03b1f9b66eda21b	6d5c5f835aea965ac6ceeea7318ea3432066443e99638fbad03b1f9b66eda21b	6d5c5f835aea965ac6ceeea7318ea3432066443e99638fbad03b1f9b66eda21b	Sesuai
	2	f5e74c5347011d72b28deb089fde6f6dae3d9e3ce7fc48af1fea8f1955b07979	f5e74c5347011d72b28deb089fde6f6dae3d9e3ce7fc48af1fea8f1955b07979	f5e74c5347011d72b28deb089fde6f6dae3d9e3ce7fc48af1fea8f1955b07979	Sesuai
	3	488aecdae8000114d6c62a587ff7434b36730e44e1a838f09ca58430e58a3be7	488aecdae8000114d6c62a587ff7434b36730e44e1a838f09ca58430e58a3be7	488aecdae8000114d6c62a587ff7434b36730e44e1a838f09ca58430e58a3be7	Sesuai
	4	bcc359dfc6f1c99808407e5f834affcf31167e91918bce28b3e5a06f57b24f21	bcc359dfc6f1c99808407e5f834affcf31167e91918bce28b3e5a06f57b24f21	bcc359dfc6f1c99808407e5f834affcf31167e91918bce28b3e5a06f57b24f21	Sesuai
	5	bb526dc79e18383b9a509884f92f87526835adb2bab7d0ef0350f0a7810fa857	bb526dc79e18383b9a509884f92f87526835adb2bab7d0ef0350f0a7810fa857	bb526dc79e18383b9a509884f92f87526835adb2bab7d0ef0350f0a7810fa857	Sesuai

Metode pengujian lainnya dilakukan pengujian *unit testing*, yaitu dengan cara menguji masing-masing modul *sourcecode* berjalan dengan baik dan *integration testing* menguji keseluruhan fungsi dan hubungan antara proses pada Arduino, RFID, *Ethernetshield* dan aplikasi webnya berjalan dengan baik. Gambar 8 adalah contoh tampilan pada proses pengajuan perizinan dan status mahasiswa yang sedang diluar kampus.

Gambar 8 Tampilan Formulir Pengajuan Perizinan dan Status Perizinan Mahasiswa

Selanjutnya dilakukan pengujian performa (*performance test)* dari sistem tersebut, diantara dengan menghitung waktu yang dibutuhkan oleh masing-masing prosesnya, hasilnya seperti pada Tabel 3.

Tabel 3. Waktu Proses Sistem Kendali Akses

No.	**Fungsi-fungsi pada sistem *e*-akses**	**Rata-rata waktu yang dibutuhkan setiap proses (*microsecond*)**
1.	Koneksi pertama	2606995.6 μs
2.	Koneksi kedua	435168.8 μs
3.	Membaca dan mengambil UID	175760.0 μs
4.	Baca sesi pada blok 4 kartu	352218.8 μs
5.	*Concate* UID dan tanggal	216319.6 μs
6.	Kirim UID untuk autentikasi	4294817948.0 μs
7.	Kirim data hasil pembangkitan x	198078.0 μs
8.	Pembangkitan nilai *hash* 100-i	62.4 μs
9.	Baca *string*==berhasil	8.0 μs
10.	Menulis pada kartu	4294936104.0 μs

Selain itu pengujian performa juga dilakukan dengan cara membuat simulasi perizinan dari beberapa mahasiswa yang dilengkapi dengan tanda pengenal serta diisi datanya, lalu melakukan *tapping* pada sistem tersebut hasil perhitungan waktunya dibandingkan dengan proses yang dilakukan secara manual yaitu menulis pada buku laporan, sehingga didapatkan hasil seperti ditunjukan pada Tabel 4. Dari hasil tersebut menunjukan bahwa secara performa lebih cepat, sekaligus tercatat dalam database dan dapat langsung dimonitor perizinan mahasiswa yang keluar masuk kampus.

Tabel 4. Perbandingan Waktu Proses Manual dan Proses Menggunakan Sistem Kendali Akses

Nomor	Mahasiswa	Pos Pengamanan		Proses Autentikasi dengan Sistem Kendali Akses
		Keluar	Masuk	
1	Mahasiswa 1	62s	105s	2,78 s
2	Mahasiswa 2	40s	90s	2,60 s
3	Mahasiswa 3	40s	60s	2,82 s
4	Mahasiswa 4	67s	8s	2,74 s
5	Mahasiswa 5	60s	120s	2,90 s
6	Mahasiswa 6	60s	120s	2,88 s
7	Mahasiswa 7	15s	60s	2,71 s
8	Mahasiswa 8	10s	150s	3,23 s
9	Mahasiswa 9	20s	20s	2,97 s
Rata -rata		**41.55s**	**81.44s**	**2,84**

3.Kesimpulan

a. Hasil prototipe implementasi Skema Lamport pada RFID menggunakan Arduino, *Ethernet shield*, dan didukung PHP MySQL sebagai database dapat digunakan sebagai sistem kendali akses untuk perizinan keluar masuk kampus.
b. Sistem Kendali Akses ini dapat dapat berfungsi untuk memonitor mahasiswa yang melakukan perizinan keluar kampus.
c. *Strong password* yang dihasilkan dari Skema Lamport berupa *password* dinamik yang sudah di *hash* berdasarkan sesi dan dapat menjadi alternatif solusi kerentanan pada password.

d. Sistem Kendali Akses ini dapat menggantikan prosedur keluar masuk kampus mahasiswa dari proses manual (*paper and pencil*) menjadi elektronik.

Ucapan Terima Kasih
Disampaikan terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah membantu dalam pembuatan Sistem Kendali Akses ini sehingga dapat menjadi suatu prototipe dan besar harapan kami dapat dikembangkan dan diimplementasikan pada proses bisnis perizinan di kampus tersebut.

Daftar Pustaka

[1]. S. Maharsi, "Pengaruh Perkembangan Teknologi Inormasi Terhadap Bidang Akuntansi Terhadap Bidang Akuntansi Manajemen," *Ekonomi Akuntansi, Fakultas Ekonomi,* vol. II, pp. 127-137, 2000.

[2]. B. Sumantri, Herman dan S. Husein, "Sistem Keamanan Ruang Server Terkoneksi Database Berbasis RFID," 2013.

[3]. W. Adam dan L. Sagala, "Sistem Absensi Pegawai Menggunakan Teknologi RFID," 2014.

[4]. A. H. Subarjo, "Pemanfaatan Teknologi Informasi untuk Pendidikan Kajian pada Mata Kuliah Kewarganegaraan," *Jurnal Angkasa,* 2013.

[5]. R. Alief, Darjat dan Sudjadi, "Pemanfaatan Teknologi RFID Melalui Kartu Identitas Dosesn pada Prototipe Sistem Ruang Kelas Cerdas," *Transmisi,* 2014.

[6]. U. Farooq, M. ul Hasan, M. Amar, A. Hanif dan U. M. Asad, "RFID Based Security and Access Control System," *IACSIT Internasional Journal of Engineering and Technology,* vol. 6, Agust 2014.

[7]. R. Marti dan M. Langheinrich, "Practical Minimalist Cryptography for RFID Privacy," *IEEE System Journal,* vol. 1, 2007.

[8]. Microsoft, "Security with Smart Card," 2018. [Online]. Available: https://technet.microsoft.com/en-us/library/cc962052.aspx. [Diakses 18 Februari 2018].

[9]. A. Pratama, T. Hidayatullah dan D. S. C. Putranto, "Efficient Implementation of Hash Sequence Authentication Based on RFID," 2017.

[10]. J. Rerungan, D. W. Nugraha dan Y. Anshori, "Sistem Pengaman Pintu Otomatis Menggunakan Radio Frequency Identification (RFID) Tag Card dan Personal identification Number (PIN) Berbasis Mikrokontroler AVR ATMEGA 128," *METRIK,* September 2014.

[11]. S. Hendra, H. R. Ngemba dan B. Mulyono , "Perancangan Prototype Teknologi RFID dan Keypad 4x4 untuk Keamanan Ganda pada Pintu Rumah," *Konferensi Nasional Sistem & Informatika,* 10 Agustus 2017.

[12]. G. R. Li, Y. Wang, C. R. Wang dan J. S. He, "EMAP: An Efficient Mutual Authentication Protocol for Passive RFID Tags," *Automation and Computing,* pp. 108-112, 2013.

[13]. M. Shashi, M. Anirudh, S. M. Ahamer , V. M. Kumar dan M. Sreelatha, "Authentication Schemes for Session Password using COlor and Images," *Journal of Network Security & Its Applictions (IJNSA),* vol. 3, 2011.

[14]. NIST, "Recommendation for Application Using Approved Hash Algorithm," *NIST sPECIAL pUBLICATION 800-107,* 2012.

[15]. A. J. Menezes, P. C. Van Oorschot dan S. A. Vanstone, Handbook Applied Cryptography, New York: CRC Press, 1996.

[16]. A. Dennis, B. H. Wixom dan R. M. Roth, System Analysis & Design, 5th penyunt., Don Fowley, 2015.

[17]. L. Lamport, "Password Authentication with Insecure Communication," *Communication ,* 1981.

[18]. T. Tsuji dan A. Shimizu, Master's Thesis A One Time Password Authentication Method, Kochi University, 2003.