Simulasi Pembayaran Menggunakan RFID (Radio Frequency Identification) Pada Studi Kasus Layanan Mahasiswa

Alvin Santoso, Henry Novianus Palit, Alexander Setiawan
Program Studi Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131 Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
alvinsss05@gmail.com, hnpalit@petra.ac.id, alexander@petra.ac.id

ABSTRAK

Uang merupakan alat untuk melakukan transaksi. Semakin berkembangnya teknologi metode pembayaran juga semakin bervariasi, salah satu caranya bisa dengan *e-money*. Tetapi, meskipun ada metode seperti ini, kegiatan administratif Universitas Kristen Petra masih menggunakan sistem manual sehingga dirasa kurang praktis. Kemudian ketika akan menerapkan metode e-money ada aspek keamanan yang harus dipertimbangkan. Salah satunya adalah cara pengamanan saldo yang berada didalam kartu sehingga saldo tidak dapat diduplikasi.

Untuk mewujudkan pembayaran dengan *e-money* pada kegiatan administratif Universitas Kristen Petra, maka akan dibuat sistem pembayaran dengan menggunakan RFID (*Radio Frequency Identification*) dengan penyimpanan saldo didalam kartu. Ada 3 metode yang akan diujicobakan pada penelitian ini yaitu AES, DES, 3DES dengan mode CBC dan CFB dalam hal perbandingan kecepatan enkripsi dekripsi, penggunaan memori, dan anti duplikasi pada kartu. Selain itu juga akan dilakukan perbandingan kecepatan ketika melakukan top up/pencairan saldo/transaksi layanan antara saldo yang disimpan didalam kartu dan saldo yang disimpan didalam *database*.

Hasil pengujian didapati bahwa anti duplikasi berhasil diterapkan, kecepatan enkripsi dekripsi metode AES, DES, 3DES mode CBC lebih cepat dibandingkan dengan CFB dan jumlah penggunaan memori yang sama pada penggunaan tiap metodenya. Proses penyimpanan data didalam *database* memiliki waktu lebih cepat pada proses top up/pencairan saldo sedangkan metode DES dengan mode CBC lebih cepat saat transaksi layanan.

Kata Kunci: RFID, e-money, AES, DES, 3DES

ABSTRACT

Money is a tool for transactions. The growing of technology make payment methods is also more varied, for example with e-money. However, even there are methods like this, administrative Petra Christian University activities still use manual system so that make less practical. When e-money going to applied, there is a security aspect that must be considered. One of them is how to secure the balance that is on the card so that the balance cannot be duplicated.

To make e-money payment on administrative Petra Christian University there will be make payment system with RFID (Radio Frequency Identification) with money in the card. There are 3 methods, AES, DES, 3DES with CBC and CFB mode in comparison of the speed encryption decryption, memory usage, and anti-duplication on the card. Besides there will be comparison of speed when doing top up/withdrawl balance/transaction when money stored in card and money stored in database.

The test results found that there anti-duplication method successfully applied, encryption decrytion speed AES, DES, 3DES mode CBC more faster than CFB and memory usage same with all of method. Money in database have a faster process in top up/withdrawl balance while DES with CBC mode more faster in transaction.

Keywords: *RFID, e-money, AES, DES, 3DES.*

1. PENDAHULUAN

Uang merupakan alat untuk melakukan transaksi salah satu contoh transaksi adalah kegiatan administratif Universitas Kristen Petra. Biasanya ketika mahasiswa berangkat ke kampus, mahasiswa pasti membawa uang agar bisa melakukan transaksi, tetapi semakin berkembangnya teknologi metode pembayaran juga semakin bervariasi, salah satu caranya bisa dengan *electronic money* atau yang biasa dikenal dengan sebutan e-money. E-money adalah alat pembayaran yang nilai uangnya disimpan dalam suatu media elektronik. Untuk penggunaannya pemilik kartu harus ke tempat yang menyediakan transaksi dengan media tersebut [2]. Kemudian dari segi bentuk e-money memiliki banyak bentuk karena bisa disimpan di bermacam-macam tempat, salah satu\nya dibuat dalam bentuk kartu. Untuk cara kerja e-money bisa ditunjang dengan teknologi RFID. RFID merupakan alat komunikasi dengan elektromagnetik [14]. Contoh nyata penerapan sistem e-money dengan RFID terdapat pada kartu BRIZZI. Kartu BRIZZI merupakan e-money yang diterbitkan oleh BRI dan salah satu fungsinya bisa digunakan untuk pembayaran di jalan tol. Cara pemakaiannya cukup mudah, dengan menempelkan kartu ke mesin pembaca transaksi bisa langsung diproses [3]. Tetapi, meskipun ada metode seperti ini, kegiatan administratif Universitas Kristen Petra masih menggunakan sistem manual sehingga dirasa kurang praktis.

Keuntungan menggunakan e-money salah satunya mengurangi penipuan, karena sifatnya digital dan sulit dipalsukan [13]. Melihat salah satu keuntungan e-money, dapat disimpulkan jika sebenarnya e-money lebih aman dari sistem manual. Walau bisa dibilang aman, tetapi penerapan teknologi e-money ini tidak benar-benar aman. Misalnya kasus pemalsuan kartu dan masih banyak kasus lainnya. Dari total kasus yang ada, total kehilangan

terkait masalah seperti ini sudah mencapai angka 21,84 miliar dolar pada tahun 2015 [8]. Melihat kasus seperti ini membuat e-money memerlukan sebuah sistem keamanan sehingga jumlah kasus yang terjadi bisa berkurang.

Dari penelitian sebelumnya, metode keamanan yang diterapkan pada penggunaan kartu yaitu kartu ditempelkan pada reader, dan kemudian UID akan dicocokan terhadap UID yang ada pada database [5]. Dari penelitian lainnya, metode keamanan yang diterapkan yaitu berupa pencocokan sidik jari pemilik kartu pada database [7]. Keamanan yang diterapkan pada penelitian sebelum sebelumnya memiliki kelebihan aman terhadap duplikasi kartu, tetapi memiliki kelemahan yaitu harus melakukan koneksi terhadap database sehingga tanpa database keamanan sistem ini tidak dapat berjalan, selain itu jika koneksi database memerlukan internet maka memerlukan koneksi internet yang lancar, kemudian jika database memiliki banyak data, maka proses pengecekannya akan semakin lama. Untuk menangami kelemahan sistem penelitian sebelumnya, pada penelitian sekarang dicari metode agar data sulit dibaca oleh orang yang tidak berhak dan anti duplikasi sebagai cara mencegah penipuan.

2. LANDASAN TEORI

2.1 Arduino Uno

Perangkat ini merupakan alat yang paling banyak digunakan dan merupakan papan mikrokontroler ATMega328P. Kata UNO pada perangkat ini merupakan bahasa Italia yang berarti angka 1. Digunakan sebagai penanda perilisan software Arduino IDE. Arduino versi ini juga sekaligus produk pertama yang dilengkapi colokan USB [1].

2.2 RC522

Merupakan perangkat yang melakukan proses baca/tulis kedalam kartu. Bersifat *contacless* sehingga tidak perlu bersentuhan langsung, tetapi cukup didekatkan pada kartu yang akan dibaca/tulis dan data dapat diproses. Cara kerja perangkat yaitu pemancar internal mendorong antena untuk melakukan komunikasi dan penerima melakukan demodulasi dan decoding dari kartu [15].

2.3 Mifare S50

Merupakan *smart card* yang dipakai untuk menyimpan data. Mifare jenis ini memiliki kapasitas penyimpanan 1024 x 8 *bit* EEPROM yang dibagi dalam 16 sektor tiap 4 *block*. 1 *block* mengandung 16 *bytes*. Untuk pembacaannya menggunakan ISO 14443 tipe A dan frekuensinya 13.56 MHz [6].

2.4 AES

National Institute of Standards and Technology (NIST) mulai mengembangkannya sejak tahun 1997 saat ketika diumumkan bahwa AES menjadi pengganti algoritma yang sebelumnya sudah diterapkan yaitu DES (*Data Encryption Standart*). AES tergolong algoritma *symmetric* dimana yang berarti *key* untuk melakukan enkripsi dan dekripsi adalah sama. AES memiliki 3 blok *cipher* dan ukuran *key* yang ukurannya terdiri dari 128, 192, 256) [11]

2.5 DES

International Bussiness Machine (IBM) mendesainnya pada awal tahun 1970. Pada tahun 1977, metode ini diadopsi Federal Information Processing Standart (FIPS) untuk menenkripsi data pada komputer. DES merupakan algoritma enkripsi symmetric. DES memiliki 64 bit key, tetapi 8 bit digunakan sebagai pengecekan parity sehingga tinggal 56 bit. Ciphertext yang dihasilkan memiliki panjang 64 bit [9].

2.6 3DES

3DES ditemukan tahun 1999, dimana algoritma ini merupakan pengembangan algoritma DES (*Data Encryption Standart*). Algoritma ini memiliki *key* sepanjang 168 *bit* yang dibagi 3 masing-masing menjadi 56 *bit*. Dasar pengembangan algoritma ini adalah karena algoritma DES yang memiliki *key* sebanyak 56 *bit* rentan terhadap *brute force attack* [4].

2.7 CBC

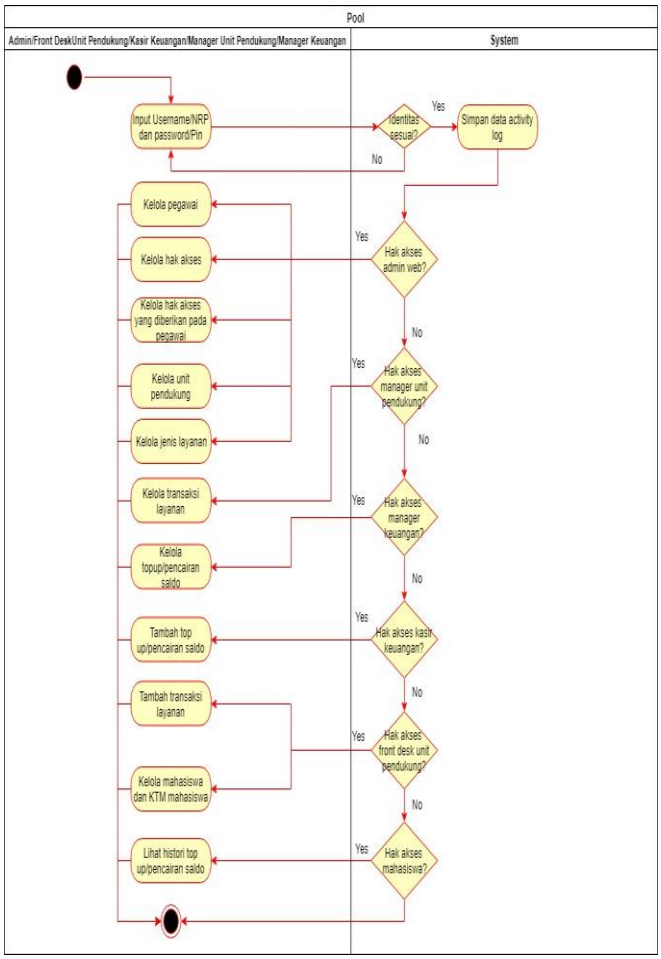
Merupakan mode operasi *block cipher* dengan memakai *initialize vector* dengan panjang tertentu. Mode ini memiliki ciri yaitu ketika melakukan proses dekripsi, maka prosesnya bergantung pada *block* sebelumnya. Jika ada 1 *bit error* bisa mempengaruhi keseluruhan *block* sedangkan untuk proses enkripsi akan menghasilkan *ciphertext* yang sama jika urutan *block* tidak dirubah dan dienkripsi menggunakan *key* dan *initialize vector* yang sama [9].

2.8 CFB

Merupakan mode operasi *block cipher* dengan memakai *initialize vector* dengan panjang tertentu. Berbeda dengan mode CBC (*Cipher Block Chaining*) yang membagi *plaintext* menjadi beberapa bagian *bit*, mode ini langsung melakukan proses enkripsi secara langsung. Pada mode ini *ciphertext block* sebelumnya di enkripsi dan hasilnya dilakukan operasi XOR dengan *plaintext* baru untuk membentuk *ciphertext* baru [12].

3. DESAIN SISTEM

Rancangan hak akses yang akan diimplementasikan pada Biro Administrasi dan Akademik kemahasiswaan (BAAk) dan perpustakaan dapat dilihat pada Gambar 1. Gambar 1 menjelaskan alur pegawai yang memiliki akses dalam melakukan login. Proses login dimulai dengan memasukan NIP pegawai dan password. Kemudian sistem akan melakukan pengecekan dan jika username dan password sesuai maka pegawai akan dapat masuk kedalam sistem. Pegawai yang diijinkan mengakses sistem terdiri dari jabatan admin, *front desk* unit pendukung, kasir keuangan, manager unit pendukung, manager keuangan, dan mahasiswa. Tiap jabatan memiliki akses yang berbeda-beda. Admin dapat melakukan kelola pegawai, hak akses dan akses yang akan diberikan, dan unit pendukung beserta layanan yang disediakan. Manager unit pendukung dapat melakukan kelola transaksi. Manager keuangan dapat melakukan kelola top up/pencairan saldo. Kasir keuangan dapat melakukan tambah top up/pencairan saldo. *Front desk* unit pendukung dapat melakukan kelola mahasiswa beserta KTMnya dan tambah transaksi. Khusus kelola mahasiswa dan KTM hanya dapat dilakukan *front desk* unit pendukung yang berada di BAAk.



Gambar 1 Login sesuai hak akses

4. IMPLEMENTASI SISTEM

4.1 Website Untuk Admin/Mahasiswa

Implementasi website ini dibuat menggunakan HTML yang berfungsi sebagai user interface. Tujuan website bagi mahasiswa sebagai tempat untuk melihat transaksi/top up/pencairan saldo terahir. Pegawai yang memiliki akses sebagai admin dapat melakukan pengelolaan unit pendukung dan layanan yang disediakan, serta hak akses pegawai.

4.2 Aplikasi Untuk Kasir/Manager

Implementasi aplikasi akan digunakan oleh pegawai yang memiliki jabatan kasir/manager. Tujuan utama aplikasi untuk mahasiswa melakukan transaksi layanan/top up/pencairan saldo. Selain itu aplikasi digunakan untuk kasir unit pendukung yang bertempat di Biro Administrasi Akademik Kemahasiswaan untuk memanajemen mahasiswa dan KTM mahasiswa. Dalam aplikasi manager memiliki peran untuk membatalkan top up/pencairan saldo/ transaksi yang sudah dilakukan.

Untuk melakukan implementasi website/aplikasi akan menggunakan *web service* sehingga tidak perlu melakukan proses secara langsung kedalam database. Adapun *web service* yang dibuat mengandung HTTP method: GET (untuk menerima data), POST (untuk proses add), PUT (untuk proses update), DELETE (untuk proses delete).

5. HASIL DAN PEMBAHASAN

Metode DES dengan mode CBC memiliki waktu enkripsi dan dekripsi tercepat yaitu 104,2 detik. Hasil percobaan dapat dilihat pada Tabel 1. Untuk penggunaan memori, tiap metode dan mode tidak memiliki perbedaan yaitu sebesar 0,1%. Untuk anti duplikasi berhasil diterapkan dengan baik. Contoh pengujian anti duplikasi dapat dilihat pada Tabel 3. Percobaan penyimpanan saldo dalam database dengan proses top up memiliki waktu tercepat dengan waktu rata-rata 5,24 detik dan hasilnya dapat dilihat pada Tabel 2.

Tabel 1 Hasil Percobaan DES CBC

Percobaan Ke-	Waktu	Penggunaan Memori
1	00:00:00:097	0,1%
2	00:00:00:107	0,1%
3	00:00:00:103	0,1%
4	00:00:00:106	0,1%
5	00:00:00:108	0,1%
Rata-rata	104,2	0,1%

Tabel 2 Hasil Percobaan Top Up

Percobaan ke -	AES CBC	AES CFB	DES CBC	DES CFB	3DES CBC	3DES CFB	Dengan Pengecekan
1	5,39 detik	5,40 detik	8,50 detik	6,28 detik	5,09 detik	4,56 detik	5,19 detik
2	6,89 detik	7,48 detik	5,26 detik	5,29 detik	6,42 detik	10,04 detik	5,17 detik
3	6,04 detik	5,37 detik	5,12 detik	5,54 detik	5,94 detik	6,09 detik	6,69 detik
4	9,89 detik	5,22 detik	5,81 detik	8,64 detik	6,52 detik	5,01 detik	4,11 detik
5	4,17 detik	5,12 detik	5,08 detik	6,74 detik	5,17 detik	4,69 detik	5,06 detik
rata-rata	6,47 detik	5,71 detik	5,95 detik	6,49 detik	5,82 detik	6,07 detik	5,24 detik
Total rata-rata	5,96 detik						

Tabel 3 Contoh Hasil Percobaan Anti Duplikasi

Percobaan Ke-	UID kartu untuk *key* (Hex)	Hasil Enkripsi (Hex)	UID kartu target duplikasi data (Hex)	Hasil
1	5089EC4B7E08040001A94662C58E611D	86B2A8480AFE56F7	E99EFC0F8408040062636 46566676869	Gagal dibaca
2	5089EC4B7E08040001A94662C58E611D	86B2A8480AFE56F7	8ABA1FBB948804008500B42EF0BB6AA8	Gagal dibaca
3	E99EFC0F84080400626 3646566676869	C63B60B5838A6A5D	5089EC4B7E08040001A94662C58E611D	Gagal dibaca

Tabel 4 Contoh Hasil Percobaan Anti Duplikasi (Lanjutan)

Percobaan Ke-	UID kartu untuk *key* (Hex)	Hasil Enkripsi (Hex)	UID kartu target duplikasi data (Hex)	Hasil
4	E99EFC0F84080400626364656667 6869	C63B60B5838A6A5D	8ABA1FBB948804008500B42EF0BB6AA8	Gagal dibaca
5	8ABA1FBB948804008500B42EF0BB6AA8	D826B12E36A923D0	5089EC4B7E08040001A94662C58E611D	Gagal dibaca
6	8ABA1FBB948804008500B42EF0BB6AA8	D826B12E36A923D0	E99EFC0F8408040062636 46566676869	Gagal dibaca

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasar hasil pengujian, maka dapat disimpulkan beberapa hal sebagai berikut:

1. Mode CFB memiliki waktu rata-rata enkripsi dan dekripsi lebih lambat dibandingkan dengan CBC dengan perbandingan hasil mode CFB tiap metode AES : DES : 3DES = 110,2 : 106,6 : 110,4 *millisecond* sedangkan mode CBC metode AES : DES : 3DES = 108,4 : 104,2 : 109,8 *millisecond*
2. Metode DES dengan mode CBC memiliki waktu rata-rata enkripsi dan dekripsi tercepat yaitu 104,2 *millisecond*
3. Tidak ada perbedaan penggunaan memori antara ketiga metode dan mode yang digunakan yaitu 0,1%
4. Metode enkripsi yang sama dengan mode yang berbeda akan menghasilkan hasil enkripsi yang berbeda.
5. Metode anti duplikasi berupa hasil enkripsi dengan menggunakan UID kartu sebagai key berhasil diterapkan dengan baik
6. Cara penyimpanan saldo didalam database dinilai lebih cepat daripada disimpan didalam kartu. Hasil didapat dari pengujian menunjukan jika pada top up memiliki kecepatan rata-rata 5,24 detik, sedangkan pada pencairan saldo memiliki kecepatan 8,17 detik. Pada transaksi layanan metode DES dengan mode CBC memiliki waktu rata-rata tercepat yaitu 7,41 detik. Adapun faktor yang mempengaruhi kecepatan rata-rata adalah pembacaan data pada kartu yang tidak 100% akurat sehingga membutuhkan waktu dalam membacanya dan jumlah data yang dibaca, karena semakin banyak jumlah data yang dibaca secara otomatis waktu yang dibutuhkan semakin lama.

6.2 Saran

Setelah melakukan evaluasi terhadap sistem keseluruhan, diharapkan skripsi ini dapat dikembangkan dengan saran:

1. Dilakukan uji coba penghubungan metode pembayaran/top up dengan bank sehingga membuat transaksi benar-benar *cashless.*
2. Pembuatan aplikasi mobile apps sehingga memudahkan *customer* (mahasiswa) dalam mengecek histori transaksi.
3. Dilakukan pengujian keamanan terhadap metode enkripsi yang diujicobakan pada penelitian ini.

7. DAFTAR PUSTAKA

[1] Arduino. n.d. .ARDUINO UNO REV3. n.d. . URI= https://store.arduino.cc/usa/arduino-uno-rev3

[2] Bank Indonesia. (n.d.). Edukasi. URI= https://www.bi.go.id/id/edukasi-perlindungan-konsumen/edukasi/produk-dan-jasa-sp/uang-elektronik/Pages/default.aspx

[3] Cermati.com. n.d ..BRIZZI BRI. URI= https://www.cermati.com/e-money/brizzi-bri

[4] Callas, J. 2017 . Triple DES: How strong is the data encryption standard? URI= https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained

[5] Listyani, H. T. 2018 . Simulasi transaksi pembayaran online dengan studi kasus kantin Universitas Kristen Petra. URI= https://dewey.petra.ac.id/catalog/digital/detail?id=42733.

[6] NXP. 2018. MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development. URI= https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf

[7] Prasteyo, A. n.d. . Aplikasi Transaksi Voucher Menggunakan RFID dan Fingerprint. URI= http://www.academia.edu/6619180/APLIKASI_TRANSAKSI_VOUCHER_MENGGUNAKAN_RFID_DAN_FINGERPRINT_Dosen_Jurusan_Teknologi_Informasi_PENS-ITS_2

[8] Report, T. N. 2016 . URI= https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf.

[9] Rouse, M. 2014. Data Encryption Standard (DES). URI= https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard

[10] Rouse, M. 2005 . ciphertext feedback (CFB). URI= https://searchsecurity.techtarget.com/definition/ciphertext-feedback

[11] Rouse, M. 2017. Advanced Encryption Standard (AES). URI=https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[12] Rouse, M. 2019. cipher block chaining (CBC). URI= https://searchsecurity.techtarget.com/definition/cipher-block-chaining

[13] Rosic, A.2016 . 5 Benefits of Cryptocurrency: A New Economy For The Future. URI= https://decentralize.today/5-benefits-of-cryptocurrency-a-new-economy-for-the-future-925747434103

[14] Shea, S. 2017. RFID (Radio Frequency Identification). URI= https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification

[15] NXP. 2016. Standart Performance MIFARE and NTAG Frontend. URI= https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf