# Sistem *e-money* berbasis *Contactless Smartcard* dengan Teknologi RFID

**Samuel Aditya Utomo[1], Darmawan Utomo[2], Banu Wirawan Yohanes[3]**

[1]Program Studi Teknik Elektro,
Fakultas Teknik Elektronika dan Komputer,
Universitas Kristen Satya Wacana, Salatiga
612005070@student.uksw.edu

[2,3]Program Studi Sistem Komputer,
Fakultas Teknik Elektronika dan Komputer,
Universitas Kristen Satya Wacana, Salatiga
[2]darmawan@staff.uksw.edu, [3]banu.yohanes@staff.uksw.edu

**Ringkasan**

Sistem pembayaran elektronik makin banyak dilakukan baik melalui *phone banking*, *Internet banking*, maupun *smartcard* berbasis RFID. Selain kemudahan dalam bertransaksi, sistem pembayaran elektronik juga menawarkan keringanan biaya transaksi. Namun transaksi elektronik tersebut dapat menyediakan celah keamanan data pengguna, penyedia layanan, dan transaksi. Artikel ini membahas salah satu metode pembayaran elektronik, yaitu sistem *e-money* dan aplikasi prototipe menggunakan *contactless smartcard* dengan teknologi RFID. Data transaksi yang dikirim antar komputer yang berpartisipasi pada transaksi *e-money* perlu diotentikasi untuk menjamin kerahasiaan data (*confidentiality*) dan dienkripsi untuk menjamin privasi bagi para pelaku transaksi. Algoritma enkripsi yang digunakan adalah 3DES karena menawarkan tingkat keamanan data yang lebih baik daripada DES, namun tetap mempertahankan performa implementasi pada perangkat keras yang baik. Hasil pengujian prototipe sistem *e-money* pada sebuah jaringan lokal fakultas menunjukkan potensi yang cukup baik untuk dapat diterapkan di lingkungan kampus.

**Kata kunci:** *e-money*, *contactless smartcard*, RFID

## 1. Pendahuluan

Perkembangan teknologi sistem komputer dan Internet memberi dampak terhadap munculnya inovasi dalam pembayaran elektronik (*electronic payment*). Fasilitas lengkap dengan kemudahan akses via Internet dan tanpa antrian seperti di bank konvensional menjadi alasan makin populernya layanan tersebut. Beberapa contoh pembayaran elektronik antara lain *phone banking*, *Internet banking*, dan pembayaran dengan kartu kredit/debit atau kartu ATM.

Meskipun beragam jenis teknologi yang digunakan, namun semua cara pembayaran elektronik itu masih terkait langsung dengan rekening nasabah pada bank tertentu. Untuk setiap instruksi pembayaran perlu otoritas dari pengguna dan akan dibebankan langsung ke rekening nasabah yang bersangkutan. Selain itu jika menggunakan kartu maka setiap bulannya dikenakan biaya administrasi yang tentu dapat merugikan pengguna kartu.

Kemudian dikembangkan sistem pembayaran elektronik menggunakan *electronic money* (*e-money*) yang memiliki karakteristik berbeda dengan pembayaran elektronik sebelumnya. Dimana pembayaran dengan menggunakan *e-money* tidak memotong saldo rekening nasabah yang menggunakannya. Dengan demikian pada prisipnya seseorang yang memiliki *e-money* sama dengan memiliki uang tunai. Hanya saja nilai uang tersebut telah dikonversi ke dalam bentuk elektronik. Untuk mengamankan transaksi *e-money* perlu digunakan otentikasi pengguna sistem untuk menjamin kerahasiaan data transaksi (*confidentiality*) dan enkripsi data transaksi untuk menjamin privasi pengguna, penyedia layanan, dan transaksi.

Teknologi *radio frequency identification* (RFID) merupakan metode pengumpulan data identitas dan identifikasi secara otomatis menggunakan frekuensi radio [1]. Sistem perangkat keras RFID terdiri dari dua elemen, yaitu *reader*/*interogator* dan *transponder*/*tag*. Contoh sebuah aplikasi RFID telah diterapkan pada tiket busway [2].

Artikel ini membahas pembuatan prototipe sistem *e-money* menggunakan teknologi RFID pada *contactless smartcard* [1] yang diharapkan dapat mempermudah transaksi jual beli di lingkungan kampus UKSW Salatiga. Pendahuluan dituliskan pada bagian 1. Perancangan sistem meliputi arsitektur sistem perangkat keras dan cara kerja sistem perangkat lunak, termasuk sistem keamanan jaringan komputer disajikan pada bagian 2. Bagian 3 berisi pengujian sistem dan analisis hasilnya. Kemudian bagian 4 berisi kesimpulan.

## 2. Perancangan Sistem

Sistem *e-money* dirancang untuk dapat dijalankan pada jaringan komputer lokal (*local area network*, LAN) yang menghubungkan setiap komputer yang dilengkapi RFID *reader*.

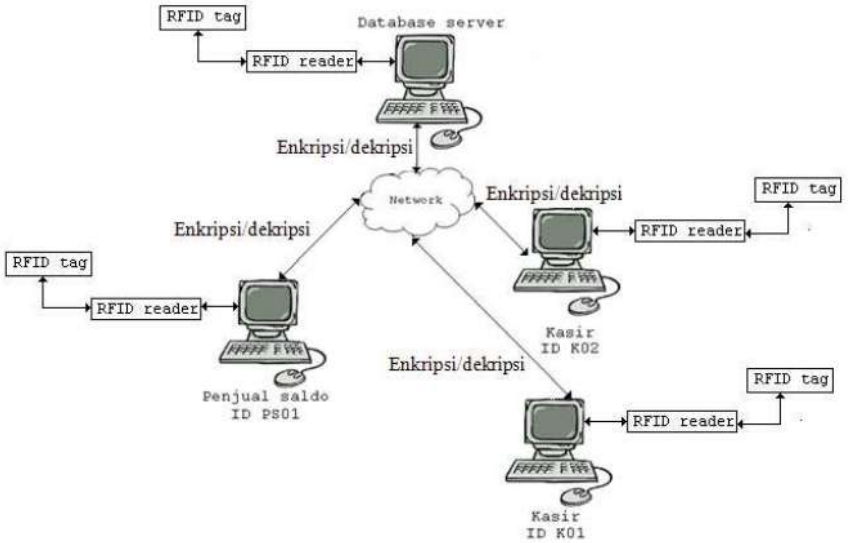
### 2.1. Arsitektur Sistem

Secara garis besar terdapat tiga pihak yang terlibat dalam sistem *e-money* ini, yaitu server penyedia layanan, penjual saldo *e-money*, dan kasir/tempat transaksi jual beli. Ketiga pihak terkait saling terhubung dalam sebuah LAN. Selain itu, ditambahkan fitur keamanan jaringan komputer dengan metode enkripsi/penyandian data menggunakan algoritma *triple data encryption standard* (3DES). Gambar 1 menampilkan diagram blok arsitektur sistem *e-money* yang dibuat.

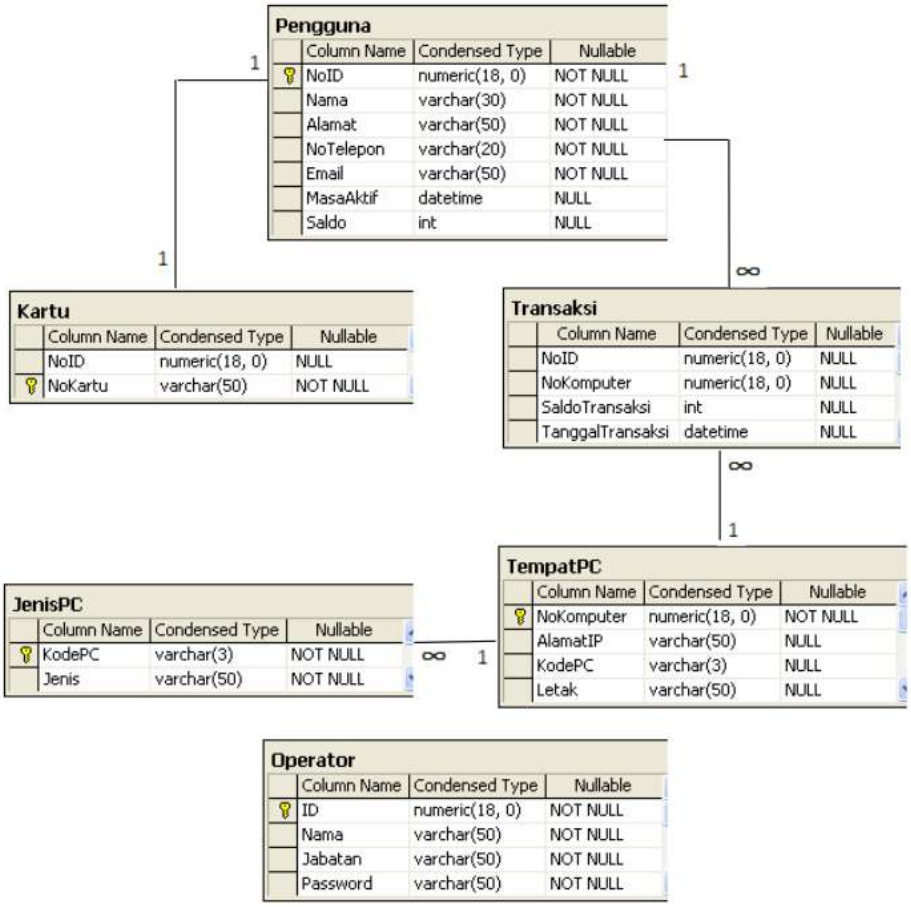
### 2.2. Sistem Perangkat Lunak

Sistem perangkat lunak terdapat pada setiap komputer yang terlibat, dengan sebuah database terpusat untuk menyimpan data registrasi pengguna kartu/pembeli dan penjual, beserta transaksi yang dilakukan setiap pihak. Diagram relasi antar entitas (*entity relationship diagram*, ERD) dari database ditampilkan pada Gambar 2.

Terdapat enam tabel dalam database pusat tersebut, yaitu tabel Pengguna, TempatPC, Transaksi, JenisPC, Kartu, dan Operator. Tabel Pengguna berisi data pengguna kartu. Tabel JenisPC berisi data jenis komputer yang digunakan untuk transaksi, baik komputer kasir atau komputer penjual saldo. Tabel TempatPC berisikan data letak komputer dan alamat IP yang telah ditentukan. Tabel Transaksi berisi data transaksi yang telah dilakukan oleh penggguna kartu. Setiap transaksi yang dilakukan akan dicatat di dalam tabel Transaksi. Tabel Kartu berisi data nomor kartu dan nomor identitas pengguna kartu.




Gambar 1. Diagram blok arsitektur sistem *e-money*




Gambar 2. Diagram relasi antar entitas pada database sistem *e-money*

Server penyedia layanan ditetapkan sebagai tempat pembuatan identitas pengguna baru dan tempat registrasi ulang kartu apabila masa aktif kartu habis. Program untuk pembuatan identitas pengguna baru diawali dengan tampilan form windows tempat pengisian identitas pengguna. Data pengguna yang diisikan pada form tersebut akan disimpan ke dalam database. Kemudian mengecek ada tidaknya tag pada kartu menggunakan RFID *reader*. Jika ada, maka data pengguna akan disimpan ke dalam tag RFID tersebut.

Proses registrasi ulang dimulai dengan inisialisasi sistem dan pengecekan tag RFID menggunakan *reader*. Jika data terbaca dari tag RFID maka akan dicocokkan dengan data dalam database dan ditampilkan. Untuk registrasi ulang atau perpanjangan masa aktif, operator komputer server perlu mengganti data masa aktifnya. Untuk perubahan identitas pengguna, maka operator perlu mengubah identitas sesuai dengan identitas pengguna yang baru. Data berupa nomor ID, saldo, dan masa aktif dikirim ke tag RFID.

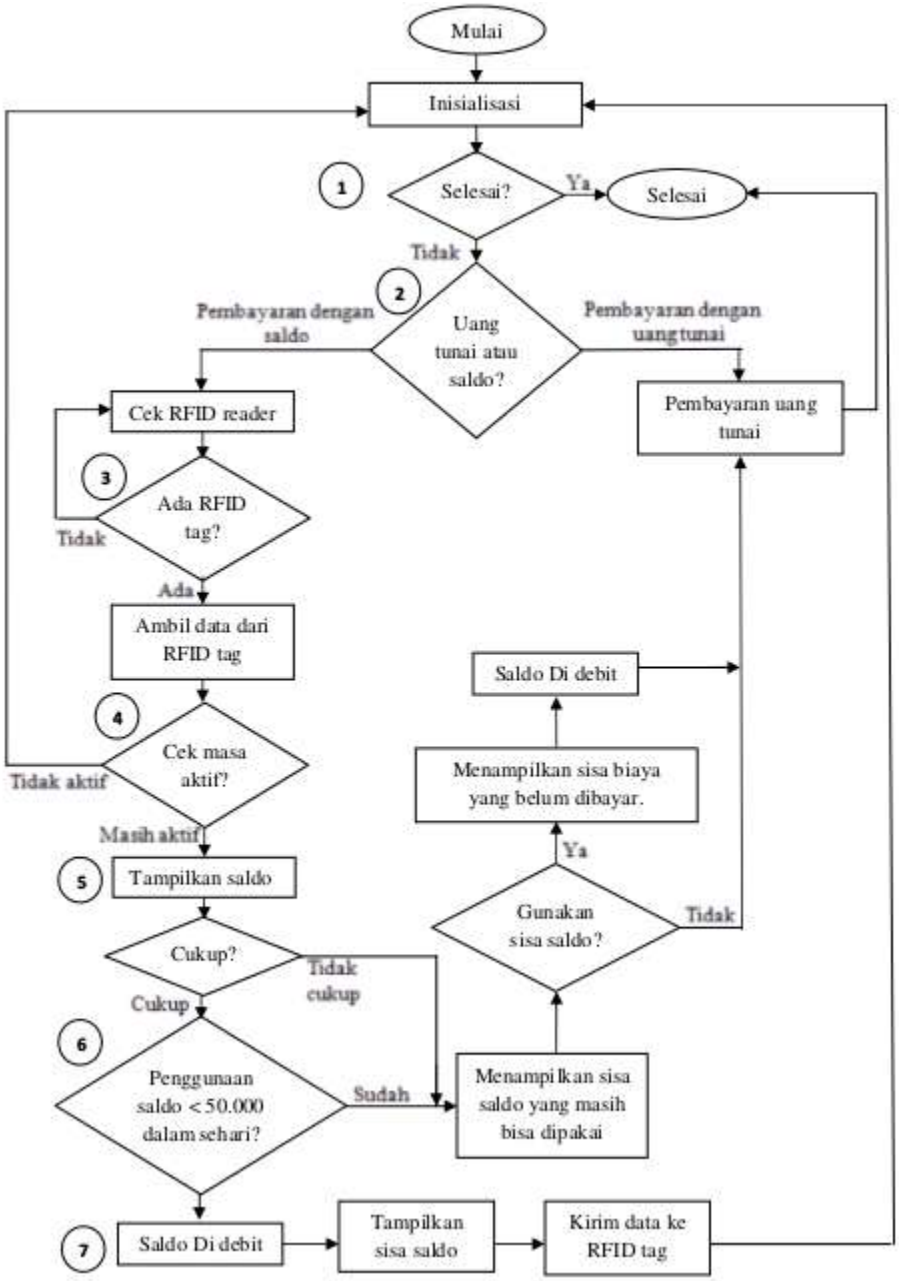
Komputer penjual saldo digunakan untuk menambahkan saldo dan melihat sisa saldo yang dimiliki oleh pengguna, dengan bantuan seorang operator. Setelah inisialisasi, sistem akan mengecek tag RFID menggunakan *reader* untuk mengambil data nomor ID pengguna kartu. Nomor ID ini dicocokkan dengan data pada database untuk mengecek masa aktif kartu. Jika kartu masih berlaku, maka program akan melanjutkan untuk menampilkan saldo yang dimiliki pengguna. Jika kartu sudah tidak berlaku, maka pengguna wajib melakukan registrasi ulang di server. Setelah itu, pemakai akan diminta untuk memilih antara melanjutkan pengisian pulsa dengan membayar sejumlah uang yang sesuai atau melihat jumlah saldo yang dimiliki.

Komputer tempat transaksi/jual-beli item digunakan untuk mengurangi saldo sesuai dengan transaksi yang dilakukan pengguna, dengan bantuan operator. Setelah inisialisasi, masukkan jumlah nominal belanja pengguna dan diberikan pilihan untuk membayar dengan uang tunai atau dengan saldo *e-money* yang dimiliki. Jika pengguna membayar dengan *e-money*, maka kartu RFID nya perlu ditaruh di *reader* untuk diambil data nomor ID dari tag RFID. Nomor ID akan dicocokkan dengan data dalam database. Selain itu program juga mengecek masa aktif dan sisa saldo untuk validasi transaksi. Batas maksimal penggunaan saldo *e-money* dalam transaksi per hari adalah 50.000 rupiah. Diagram alir program transaksi/jual-beli item ditampilkan pada Gambar 3.

### 2.3. Sistem Keamanan Jaringan Komputer

Untuk mengamankan privasi data transaksi *e-money* dan penggunanya digunakan algoritma enkripsi *triple data encryption standard* (3DES). Pada dasarnya 3DES merupakan skema enkripsi blok *cipher* yang simetrik dengan menerapkan algoritma enkripsi DES tiga kali pada setiap blok data [3]. Hal ini diperlukan untuk mengatasi persoalan panjang kunci DES 56 bit yang dinilai terlalu pendek saat ini. Karena perkembangan komputasi yang pesat, serangan *brute-force* menggunakan 1 juta mesin dimana setiap mesin mampu menguji 1 juta kunci per detik memungkinkan untuk mencari satu kunci dalam waktu rata-rata 12 jam saja.

Terdapat tiga tahapan pada 3DES dengan kunci sepanjang 56 bit pada setiap tahapnya yaitu $K_{DES1}$, $K_{DES2}$ dan $K_{DES3}$. Pada tahap pertama *plaintext* dienkripsi menggunakan kunci $K_{DES1}$ untuk menghasilkan *pre-ciphertext* pertama. Kemudian tahap kedua *pre-ciphertext* pertama didekripsi menggunakan kunci $K_{DES2}$ untuk menghasilkan *pre-ciphertext* kedua. Terakhir tahap ketiga *pre-ciphertext* kedua dienkripsi menggunakan kunci $K_{DES3}$ untuk menghasilkan *ciphertext*.




Gambar 3. Diagram alir transaksi menggunakan *e-money*

Seperti halnya skema enkripsi lain, terdapat dua masukan bagi fungsi enkripsi DES: *plaintext* yang akan dienkripsi dan kunci enkripsi, dimana sebuah blok *plaintext* berukuran 64 bit dan kuncinya 56 bit. Meskipun ukuran kunci sebenarnya 64 bit, namun hanya 56 bit yang digunakan sedangkan 8 bit sisanya dapat dipakai sebagai bit *parity* atau bit sembarang. Skema enkripsi DES dapat dilihat pada Gambar 4.

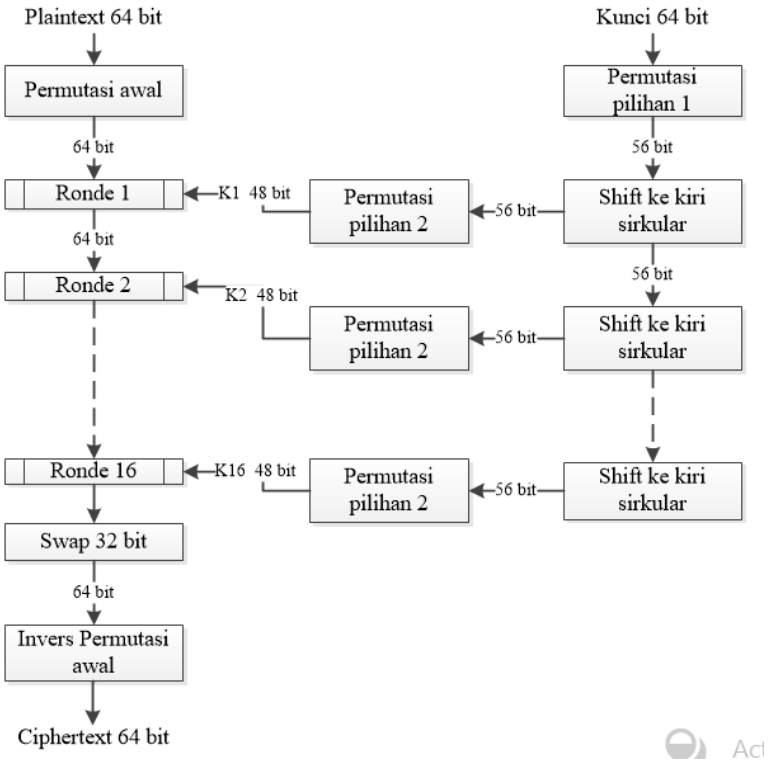
Pertama, blok *plaintext* 64 bit dilewatkan kepada sebuah matriks permutasi awal (*initial permutation*, IP) yang menyusun ulang bitnya untuk menghasilkan masukan yang dipermutasi. Diikuti sebuah fase yang terdiri dari 16 ronde dari fungsi yang sama. Fungsi

tersebut meliputi permutasi dan subtitusi. Keluaran dari ronde terakhir (ronde 16) terdiri dari 64 bit sebagai fungsi dari *plaintext* dan kunci. Bagian kiri dan kanan dari keluaran tersebut dipertukarkan (*swap*) untuk menghasilkan *preoutput*. Akhirnya, *preoutput* dilewatkan pada sebuah permutasi [IP-1] yang merupakan invers dari fungsi IP, untuk menghasilkan *ciphertext* sepanjang 64 bit. DES memiliki struktur yang sama diluar permutasi awal dan akhir, yaitu sebuah *cipher* Feistel.

Dalam satu ronde DES masukan 64 bit dibagi menjadi dua bagian, 32 bit kiri (*left*, L) dan 32 bit kanan (*right*, R). Seperti *cipher* Feistel lainnya, pemrosesan data pada setiap ronde dapat diringkas oleh persamaan berikut:

$$L_i = R_{i-1} \; ; 1 \leq i \leq 16 \tag{1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \tag{2}$$




Gambar 4. Skema enkripsi DES

Kunci ronde $K_i$ sepanjang 48 bit dan masukan $R$ sepanjang 32 bit. Pertama, masukan $R$ diekspansi menjadi 48 bit menggunakan tabel permutasi ditambah dengan ekspansi, termasuk duplikasi dari 16 dari bit $R$. Hasilnya 48 bit di XOR-kan dengan $K_i$. Hasil 48 bit ini yang dilewatkan pada sebuah fungsi subtitusi untuk menghasilkan keluaran 32 bit yang dipermutasikan.

Untuk dekripsi DES, sama seperti *cipher* Feistel lain, algoritma yang digunakan sama dengan enkripsi tetapi urutan penggunaan kunci turunan dibalik. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah $K_1$, $K_2$, $K_3$, ..., $K_{16}$ maka proses dekripsi urutan kunci internal yang digunakan adalah $K_{16}$, $K_{15}$, $K_{14}$, ..., $K_1$.

## 3. Hasil Pengujian dan Analisis

Untuk pengujian sistem secara keseluruhan diberikan contoh 4 kasus. Pertama adalah pengguna kartu baru, kedua adalah pengguna kartu yang batas masa aktif kartunya sudah melebihi batas penggunaan, ketiga adalah pengguna kartu yang saldonya tidak mencukupi untuk membayar daftar belanja, dan keempat dimana pengguna sudah menggunakan lebih dari saldonya 50.000 rupiah dalam sehari.

### 3.1. Pengguna Kartu Baru

Pengguna datang ke komputer server untuk mendaftarkan dirinya ke operator. Setelah data pengguna kartu baru diisi lengkap seperti contoh kasus pada Gambar 5.(a), maka operator komputer menekan tombol *add* dan data pengguna kartu pertama akan tersimpan di database. Pada menu pembuatan kartu operator komputer menuliskan NoID, saldo, dan masa aktif seperti ditampilkan pada Gambar 5.(b), kemudian menekan tombol Simpan Dalam Kartu, maka data akan disimpan di dalam memori kartu. NoID pengguna kartu pertama itu akan disimpan pada Tabel Kartu di database sesuai dengan nomor kartu yang telah digunakan, untuk menghindari penggunaan lebih dari satu kartu bagi seorang pengguna.

Pada pembayaran pembelian barang, operator komputer kasir menjumlahkan harga barang yang akan dibeli, dan selanjutnya pengguna kartu pertama perlu meletakkan kartunya pada RFID *Reader* OMNIKEY 5321 [4]. Data transaksi ini seperti ditunjukkan pada Gambar 5.(c) disimpan pada Tabel Transaksi. Dan sisa saldo pengguna kartu pertama akan di *update* pada Tabel Pengguna.

Untuk pembelian saldo, pengguna kartu datang ke penjual saldo. Setelah saldo yang sudah berhasil ditambahkan setelah proses pengisian data pada Gambar 6.(a), maka data saldo terbaru akan disimpan kembali ke Tabel Pengguna. Selain itu, transaksi pembelian saldo ini juga akan disimpan pada Tabel Transaksi. Laporan transaksi untuk pengguna kartu dapat dilihat pada laporan jumlah transaksi pada sisi server seperti ditampilkan pada Gambar 6.(b).

### 3.2. Pengguna Kartu yang Masa Aktifnya Habis

Apabila pengguna kartu kedua ingin mengisikan saldonya, maka proses transaksi tidak dapat dilakukan karena batas masa aktifnya habis, seperti diunjukkan pada Gambar 7. Pengguna diharuskan melakukan registrasi ulang ke komputer server. Jika pengguna bertransaksi, maka sistem akan membatalkan karena batas masa aktif kartu habis dan akan menampilkan peringatan untuk registrasi ulang terlebih dahulu.

### 3.3. Pengguna Kartu yang Saldonya Tidak Mencukupi

Pengguna kartu yang saldonya tidak mencukupi untuk melakukan pembelian barang, ditunjukkan pada Gambar 8.

### 3.4. Pengguna kartu menggunakan saldo lebih dari 50.000 dalam sehari

Sistem akan menampilkan sisa saldo yang masih bisa dipakai. Pengguna kartu dapat memilih untuk membayar total belanja dengan uang tunai atau menggunakan sisa saldonya dan selajutnya membayar total belanjaannya dengan uang tunai.


(a) (b) (c)

Gambar 5. (a) Contoh kasus pengisian data bagi pengguna kartu baru; (b) Pengisian saldo pada kartu baru; dan (c) Penggunaan saldo untuk membeli barang


(a) (b)

Gambar 6. (a) Contoh kasus pengisian saldo kartu; dan (b) Laporan penggunaan saldo pada kartu


Gambar 7. Contoh kasus penggunaan kartu yang masa aktifnya telah habis


Gambar 8. Contoh kasus penggunaan kartu yang saldonya kurang dari nilai transaksi

### 3.5. Ringkasan

Ringkasan hasil pengujian keseluruhan sistem *e-money* ditampilkan pada Tabel 1. Pengujian pada sisi kasir sempat mengalami beberaoa kegagalan penyimpanan data transaksi yang disebabkan oleh kartu yang digunakan salah dan kesalahan sistem pada RFID *reader*. Sementara kegagalan pada sisi penjual saldo disebabkan karena saldo yang

diisikan melebihi batas yang ditentukan, yaitu 1.000.000 rupiah, namun sistem belum dapat memberi proteksi.

Tabel 1. Ringkasan hasil pengujian sistem *e-money* secara keseluruhan

| No. Komputer | Jenis Komputer | Jumlah Trasaksi | Jumlah Keberhasilan | Keterangan |
|---|---|---|---|---|
| 1 | Kasir | 10 | 10 | |
| 2 | kasir | 15 | 13 | Terjadi 2 kali kegagalan penyimpan data transaksi disebabkan kartu yang digunakan salah. |
| 3 | Kasir | 13 | 10 | Terjadi 3 kali kegagalan karena driver RFID *reader* error.. |
| 4 | Penjual Saldo | 10 | 8 | Terjadi 2 kali kegagalan pengisian saldo dikarenakan saldo yang diisikan lebih dari 1000000 dan system belum dapat memproteksinya |

## 4. Kesimpulan

Dari hasil pengujian sistem disimpulkan bahwa reliabilitas jaringan komputer pada LAN merupakan infrastuktur yang vital bagi berjalannya sistem *e-money*. Apabila jaringan komputer terganggu/terputus belum ada mekanisme untuk melakukan *backup* dan *recovery*. Kegagalan sistem transaksi *e-money* dapat disebabkan oleh beberapa faktor antara lain penggunaan kartu yang salah atau bukan sesuai dengan pemiliknya, belum adanya proteksi jumlah saldo maksimal yang dapat diisikan seharusnya disesuaikan dengan tipe data yang digunakan, dan kegagalan sistem RFID *reader*.

Dengan keterbatasan fitur pada versi prototipe ini, maka direncanakan untuk mengembangkan sistem dengan beberapa fitur seperti menambahkan printer pada kasir untuk mencetak hasil transaksi, mengganti aplikasi desktop berbasis form windows menjadi aplikasi web agar tidak memerlukan proses instalasi di setiap komputer dan memperluas jangkauan sistem, penggunaan sistem *e-money* pada transaksi lain seperti kartu perpustakaan dan absensi perkuliahan, penggunaan metode keamanan data lain, dan pengujian sistem keamanan data baik secara formal matematis maupun praktis.

## Daftar Pustaka

[1] Finkenzeller, K. *RFID Handbook: Fundamentals and Application in Contactless Smart Card and Identification, Second Edition*, John Willey and Sons Ltd. Munich. 2003.

[2] Sandy, A.M. *Aplikasi Radio Frequency Identification* (*RFID*) *pada tiket busway*, Skripsi, Fakultas Teknik Elektronika dan Komputer, UKSW, Salatiga, 2008.

[3] Stallings, W. *Cryptography and Network Security, Principles and Practice, Fifth Edition*, Prentice Hall, 2011.

[4] Philips. *Mifare® MF1ICS50 Functional Specification Rev. 5.3*, January 2008.