

PERANCANGAN DAN IMPLEMENTASI SISTEM FAKTUR DAN PEMBAYARAN OTOMATIS PADA TOKO SWALAYAN BERBASIS RFID

Angger Widya Sulaiman¹, Erwin Susanto², Unang Sunarya³

^{1,2,3}Fakultas Teknik Elektro, Universitas Telkom

¹angger@gmail.com, ²erwinelektro@telkomuniversity.ac.id, ³unangsunarya@telkomuniversity.ac.id

Abstrak

Pada saat ini, antrean panjang di kasir toko swalayan merupakan pemandangan yang biasa. Pada umumnya antrean yang terjadi di kasir disebabkan oleh dua faktor, yaitu petugas kasir harus menembak satu per satu *barcode* pada barang yang dibeli oleh pengunjung sekaligus harus menghitung uang yang dibayarkan dan yang dikembalikan. Oleh karena itu, pada penelitian ini dirancang suatu sistem faktur otomatis berbasis RFID yang dapat mengurangi panjang antrean di kasir toko swalayan. Sistem kerja RFID pada sistem ini menyerupai fungsi *barcode* pada barang, tetapi karena RFID memiliki kemampuan untuk mengirim dan menerima data maka barang-barang belanjaan tidak perlu dikeluarkan dari keranjang belanja untuk mengidentifikasinya. Untuk menyelesaikan faktor antrean, RFID juga digunakan sebagai alat pembayaran elektronik dengan algoritma kriptografi RSA sebagai pengaman komunikasi data antara komputer *merchant* dan *server*. Dari hasil pengujian system, diperoleh tingkat rata-rata akurasi deteksi barang adalah 92,23%, kecepatan rata-rata *scanning* barang 5,19 detik/keranjang, serta kecepatan rata-rata komunikasi data antara komputer *merchant* dan *server* melalui sms 17,41 detik/transaksi.

Kata Kunci: RFID, kriptografi, RSA, *barcode*

Abstract

A long queue at the checkout supermarket is a general condition at this time. It is generally caused by two factors, the cashier has to check the barcode on consumer goods, all at once the clerk also must calculate the money paid and count the cash change money. Therefore, this study designs an RFID-based automated invoicing system that can reduce the long queues at the supermarket checkout. RFID system works with barcode process. Because RFID has the ability to send and receive data, the grocery items do not need to be picked from the shopping cart to identify it. To overcome the queue difficulties, RFID is also used as a means of electronic payment with RSA cryptographic algorithm as a safety data communication between the merchant and the server computer. From the test results obtained by the system, it can be shown that average level of detection accuracy is 92.23% of goods, the average speed is 5.19 seconds scanning items/baskets, and average speed data communication between the merchant and the server computer via sms is 17.41 seconds/transaction.

Keywords: RFID, cryptography, RSA, barcode

1. Pendahuluan

Dengan memanfaatkan perkembangan teknologi dan informasi khususnya teknologi *Radio Frequency Identification* (RFID), masalah antrean pada toko swalayan sangat mungkin untuk diatasi karena teknologi *reader* RFID saat ini sudah memungkinkan untuk membaca kumpulan *tag* RFID dalam sekali waktu. Dengan memanfaatkan kemampuan tersebut, *tag* RFID dapat digunakan sebagai *barcode* pada barang-barang yang dijual di toko swalayan sehingga pembeli dengan keranjang belanjanya hanya perlu melewati *gate* pembayaran dan secara otomatis faktur belanja ditampilkan dilayar monitor. Metro Group dan IBM telah bekerjasama dalam melakukan riset untuk bekerja sama mewujudkan implementasi teknologi ini [1].

Untuk menyelesaikan masalah pembayaran di toko swalayan yang seringkali memakan waktu lama, teknologi RFID diharapkan juga mampu mengatasi masalah tersebut dengan dimanfaatkan sebagai alat pembayaran elektronik (*e-payment*) karena dengan metode *e-payment* ini pembeli cukup memasukkan PIN untuk menyelesaikan transaksi jual beli dan untuk mengamankan PIN dari serangan "*Man in the middle attack*", PIN dienkripsi menggunakan algoritma kriptografi RSA. Pada umumnya algoritma kriptografi RSA ini digunakan untuk mengamankan transaksi keuangan berbasis *card* [2, 6], sehingga diharapkan algoritma kriptografi RSA ini mampu memberikan tingkat keamanan dan keotentikan data hingga 100%.

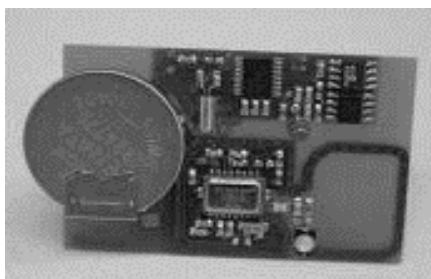
Pada penelitian ini, dirancang dan diimplementasikan sebuah sistem faktur

otomatis sekaligus sebagai pembeda dari teknologi yang dikembangkan oleh Metro Group dan IBM sistem ini ditambahkan sistem pembayaran berbasis RFID yang menggunakan algoritma kriptografi RSA sebagai sistem keamanannya.

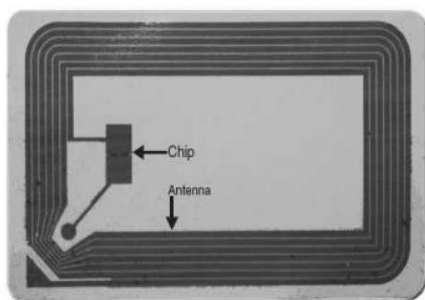
2. Sistem RFID

Sistem RFID terdiri dari empat komponen utama [1, 6]:

- a. *Tag: device* bermemori yang dibuat dari rangkaian elektronika dan antena yang terintegrasi di dalam rangkaian tersebut. Berdasarkan catu dayanya, *tag* dapat digolongkan menjadi:
 - 1) *Tag* aktif: yaitu *tag* yang catu dayanya diperoleh dari baterai (Gambar 1).
 - 2) *Tag* pasif: yaitu *tag* yang catu dayanya diperoleh dari medan yang dihasilkan oleh pembaca RFID (Gambar 2).
- b. Antena: untuk mentransmisikan sinyal frekuensi radio antara pembaca RFID dan *tag* RFID.
- c. Modul RFID: *device* yang memiliki kemampuan untuk membaca atau menulis data pada *tag* yang kompatibel (Gambar 3).
- d. *Software* aplikasi: aplikasi pada sebuah *work station* atau komputer yang dapat membaca data dari *tag* melalui pembaca RFID.



Gambar 1. Tag Aktif



Gambar 2. Tag Pasif [6]



Gambar 3. Modul RFID Reader/Writer

3. Kriptografi

Kriptografi secara umum adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [4]. Beberapa istilah penting yang perlu diketahui dalam kriptografi, antara lain:

- a. Pesan/*plaintext/cleartext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya oleh manusia.
- b. *Chiphertext/cryptogram* adalah pesan yang tersandi.
- c. *Chiper/code* adalah algoritma matematis yang digunakan untuk enkripsi dan dekripsi.
- d. Kunci/*key* adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi.
- e. Enkripsi/*encrypt* adalah proses mengubah atau menyandikan *plaintext* menjadi *chiphertext*.

3.1. Teknik Kriptografi

Pada umumnya teknik kriptografi ada dua macam yaitu algoritma sandi kunci simetris dan asimetris. Perbedaan mendasar dari kedua teknik ini adalah algoritma sandi kunci simetris menggunakan kunci yang sama untuk melakukan proses enkripsi dan dekripsi, sedangkan algoritma sandi kunci asimetris menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsi.

3.2. RSA

Dari sekian banyak algoritma kriptografi asimetri yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA [2] [5]. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT pada tahun 1976, yaitu: Ron Rivest, Adi Shamir, dan Leonard Adleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan maka selama itu pula keamanan algoritma RSA tetap terjamin. Algoritma RSA memiliki besaran-besaran sebagai berikut:

- a. p dan q bilangan prima (rahasia)
- b. $n = p \cdot q$ (tidak rahasia)
- c. $\phi(n) = (p - 1)(q - 1)$ (rahasia)
- d. e (kunci enkripsi) (tidak rahasia)
- e. d (kunci dekripsi) (rahasia)
- f. m (*plaintext*) (rahasia)
- g. c (*chiphertext*) (tidak rahasia)

3.3. Perumusan Pembangkitan Kunci

Untuk pembangkitan kunci RSA langkah yang harus dilakukan adalah:

- a. Pilih dua bilangan prima p dan q dengan syarat $p \neq q$ dan nilai p atau q tidak sama dengan 2.
- b. Hitung nilai $n = p \cdot q$
- c. Hitung nilai $\phi(n) = (p-1)(q-1)$
- d. Pilih nilai e dari $1 < e < \phi(n)$ dengan syarat e relatif prima terhadap n atau $\text{gcd}(e, \phi(n)) = 1$ dan $\phi(n)$ tidak kelipatan dari e .
- e. Cari nilai d yang integer positif sehingga $d \cdot e \equiv 1 \pmod{n}$ atau dapat ditulis $d \cdot e - 1 = k \phi(n)$ dengan nilai $k = \{1, 2, \dots, n-1\}$.
- f. Untuk melakukan enkripsi dan dekripsi *plaintext* dapat menggunakan formula berikut:

$$E_e(m) = m^e \pmod{n}$$

$$D_d(c) = c^d \pmod{n}$$

3.4. Raspberry Pi

Raspberry Pi adalah sebuah mini komputer yang menggunakan sistem operasi linux dan CPU [3] menggunakan 700 MHz ARM1176JZF-S core. Ada dua model Raspberry Pi yang sekarang beredar di pasaran yaitu model A dan model B yang membedakan dari kedua model ini adalah model A memiliki satu port USB dan tanpa port ethernet sedangkan model B memiliki dua port USB dan memiliki port ethernet (Gambar 4).

4. Mikrokontroler ATmega 16

Mikrokontroler merupakan suatu komponen elektronika yang didalamnya terdapat rangkaian mikroprosesor, memori (RAM/ROM) dan I/O. Rangkaian tersebut terdapat dalam level chip atau biasa disebut *single chip micro computer*. Pada mikrokontroler sudah terdapat komponen-komponen mikroprosesor dengan bus-bus internal yang saling berhubungan. Komponen-komponen tersebut adalah RAM, ROM, *Timer*, komponen I/O paralel dan serial, dan *interrupt controller*. Dengan harga yang terjangkau memungkinkan mikrokontroler digunakan pada berbagai sistem elektronik, seperti pada robot, sistem alarm, peralatan telekomunikasi, hingga sistem otomatisasi industri [7].

5. Perancangan Sistem

Gambar 5 menggambarkan sistem kerja faktur otomatis dan sistem pembayaran secara umum. Untuk penjelasan per bagian sistem sebagai berikut (Gambar 6):

- a. Deteksi keranjang belanja
 Pada subsistem ini proses yang dijalankan adalah mendeteksi keranjang belanja yang akan memasuki area baca keranjang belanja. Proses ini diperlukan untuk tanda deteksi tag RFID mulai dilakukan.
- b. Deteksi barang belanjaan
 Pada subsistem ini proses yang dijalankan adalah mendeteksi setiap barang yang akan dibeli oleh pembeli. Pendeteksian dilakukan sebanyak 30

kali secara otomatis, hal ini dilakukan untuk meningkatkan keakuratan pendeteksian tag yang ditempelkan pada barang walaupun semakin banyak jumlah deteksi yang dilakukan akan semakin lama waktu proses yang diperlukan.

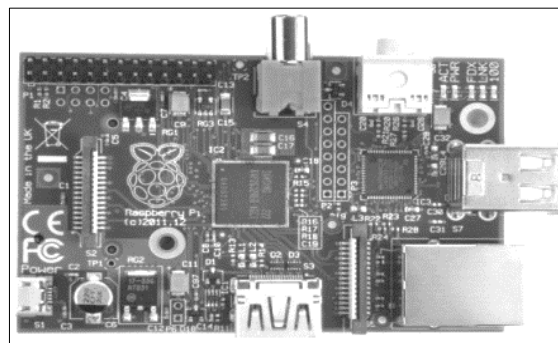
- c. Tampilkan faktur
 Pada subsistem ini hasil deteksi akan ditampilkan dilayar monitor dan dilengkapi informasi harga serta jumlah barang yang dibeli.
- d. Deteksi metode pembayaran
 Pada subsistem ini akan dijalankan proses deteksi ID yang tertempel pada perangkat pembeli misalkan *handphone*, dompet. Jika ID terdeteksi maka pembayaran akan dilakukan secara *e-payment* dan jika ID tidak terdeteksi maka pembayaran dilakukan secara manual atau tunai.

6. Analisis Waktu dan Ketepatan Pembacaan Tag

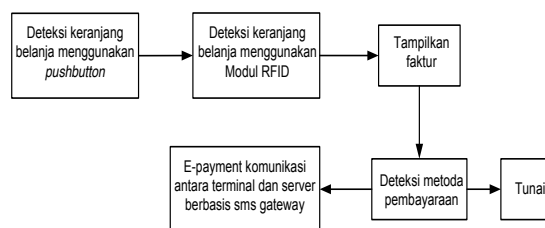
Pada bagian ini percobaan dikelompokkan menjadi dua macam yaitu analisis waktu dan ketepatan pembacaan tag tanpa proses pembayaran dan analisis waktu dan ketepatan pembacaan tag dengan proses pembayaran.

7. Analisis Waktu dan Ketepatan Pembacaan Tag Tanpa Proses Pembayaran

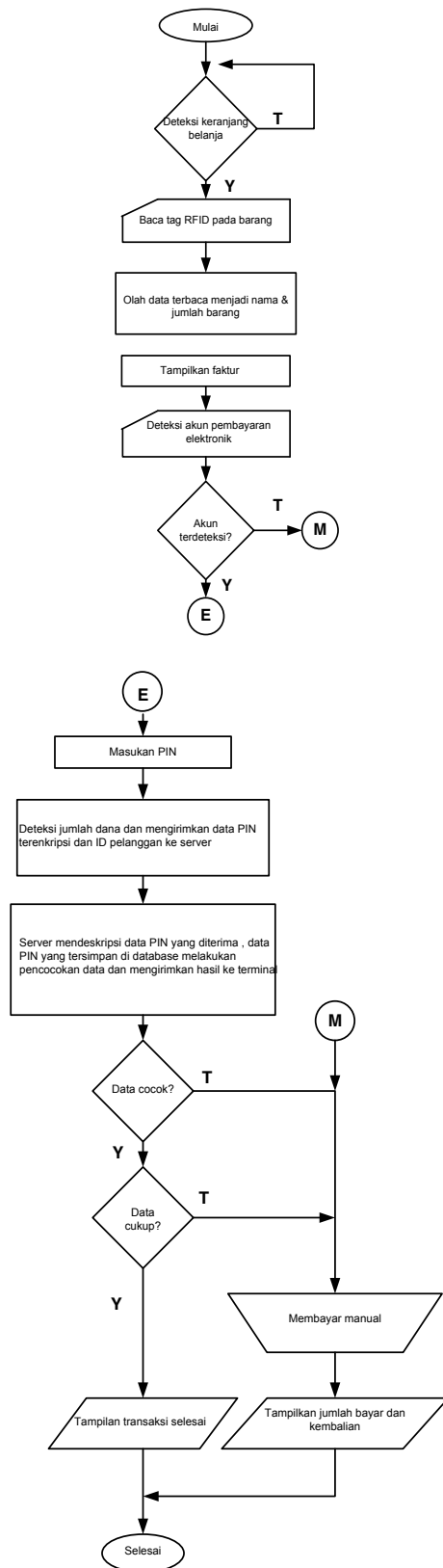
Prosedur yang dilakukan dalam percobaan ini adalah pengukuran waktu dilakukan manual menggunakan *stopwatch* dan jarak antara *reader*, *mode* perintah *scan*, *mode* manual dan *scan* manual, dan untuk jumlah barang yang dideteksi telah ditentukan jumlahnya yaitu 5, dan 10 macam dengan jarak pembacaan 1 meter.



Gambar 4. Raspberry Pi Model-B



Gambar 5. Blok Diagram Sistem



Gambar 6. Diagram Alir Sistem

Tabel 1. Data Sebenarnya dari Lima Macam Barang

No.	Nama Barang	Jumlah
1	Gucci Tshirt	2
2	Parfum Bvlgari	1
3	Jaya Amplop	1
4	Earphones	1

Tabel 2. Hasil Pembacaan dari Lima Macam Barang

No.	Nama Barang	Jumlah
1	Jaya Amplop	1
2	Gucci Tshirt	2
3	Earphones	1
4	Parfum Bvlgari	1

Tabel 3. Data Sebenarnya dari Sepuluh Macam Barang

No.	Nama Barang	Jumlah
1	Parfum Bvlgari	1
2	Omrom Walking Style	2
3	Jaya Amplop	1
4	Earphones	1
5	Gucci Tshirt	1
6	Essential Underwear	1
7	Rizome Tshirt	2
8	Nikita Slimming Magnetic	1

Tabel 4. Hasil Pembacaan dari Sepuluh Macam Barang

No.	Nama Barang	Jumlah
1	Nikita Slimming Magnetic	1
2	Gucci Tshirt	1
3	Earphones	1
4	Rizome Tshirt	2
5	Omrom Walking Style	2
6	Essential Underwear	1
7	Jaya Amplop	1
8	Parfum Bvlgari	1

Pada Tabel 1 ditunjukkan daftar barang di dalam keranjang yang akan dilakukan proses *scanning* untuk mengidentifikasi jenis dan banyaknya barang dalam keranjang. Dari 10 kali percobaan proses identifikasi barang di dalam keranjang tanpa proses pembayaran didapatkan waktu identifikasi selama 6,76 detik dengan tingkat ketepatan identifikasi pembacaan sebesar 100% seperti terlihat pada Tabel 2.

Pada Tabel 3 ditunjukkan 10 macam barang di dalam keranjang yang akan dilakukan proses *scanning* untuk mengidentifikasi jenis dan banyaknya barang dalam keranjang.

Dari 10 kali percobaan proses identifikasi barang di dalam keranjang tanpa proses pembayaran didapatkan waktu identifikasi selama 6,17 detik dengan tingkat ketepatan identifikasi pembacaan sebesar 100% seperti terlihat pada Tabel 4.

8. Analisis Waktu dan Ketepatan Pembacaan Tag dengan Proses Pembayaran

Prosedur yang dilakukan dalam percobaan ini adalah pengukuran waktu dilakukan manual menggunakan *stopwatch* terhadap lama pembacaan dan lama pengiriman sms antara komputer *server* dengan komputer *merchant* dalam proses pembayaran. Jarak antara *reader* dan keranjang belanja kurang dari 1 meter, mode perintah *scan* menggunakan mode manual, dan untuk jumlah barang yang akan dideteksi telah ditentukan jumlahnya yaitu 2 dan 5 macam. Pada Tabel 5 ditunjukkan daftar barang di dalam keranjang yang akan dilakukan proses *scanning* untuk mengidentifikasi jenis dan banyaknya barang dalam keranjang.

Tabel 5. Data Sebenarnya dari Dua Macam Barang

No.	Nama Barang	Jumlah
1	Jaya Amplop	1
2	Essential Underwear	1

Tabel 6. Data Hasil Pembacaan dari Dua Macam Barang

No.	Nama Barang	Jumlah
1	Jaya Amplop	1
2	Essential Underwear	1

Tabel 7. Data Sebenarnya dari Lima Macam Barang

No.	Nama Barang	Jumlah
1	Jaya Amplop	2
2	Essential Underwear	2
3	Earphones	1

Tabel 8. Data Hasil Pembacaan dari Lima Macam Barang

No	Nama Barang	Jumlah
1	Jaya Amplop	2
2	Essential Underwear	2
3	Earphones	1

Dari 10 kali percobaan proses identifikasi barang di dalam keranjang dengan proses pembayaran didapatkan waktu identifikasi selama 4,72 detik dan proses komunikasi pembayaran melalui sms dibutuhkan waktu 17,84 detik dengan tingkat ketepatan identifikasi pembacaan sebesar 100% (Tabel 6). Dari 10 kali percobaan proses pembacaan *tag* barang di dalam keranjang (Tabel 7) dengan proses pembayaran didapatkan waktu identifikasi selama 4,85 detik dan proses komunikasi pembayaran melalui SMS dibutuhkan waktu 15,35 detik dengan tingkat ketepatan identifikasi pembacaan sebesar 100% (Tabel 8).

9. Kesimpulan

Dalam penelitian ini, telah berhasil diimplementasikan sistem faktur dan pembayaran otomatis yang dilengkapi algoritma kriptografi RSA sebagai keamanannya. Keunggulan sistem yang dikembangkan ini dibandingkan dengan sistem konvensional yang sudah ada adalah mampu mendeteksi barang dalam jumlah banyak dalam waktu yang sangat cepat bila dibandingkan dengan sistem konvensional sehingga tujuan penyelesaian masalah antrean yang disebabkan oleh faktor pertama yaitu lamanya waktu yang diperlukan untuk mengidentifikasi barang dapat diatasi.

Sistem ini juga mampu mempercepat proses transaksi keuangan apabila menggunakan metode *e-payment* sehingga tujuan penyelesaian masalah antrean yang disebabkan oleh faktor kedua yaitu lamanya proses penghitungan uang bayar dan uang kembalian dapat diatasi. Selain itu, proses pembacaan *tag* RFID memiliki akurasi 100% pada jumlah barang untuk 10 macam barang.

Daftar Pustaka

- [1] Agustina, Yeni, “*Sistem Absensi Kepegawaian Menggunakan Radio Frequency Identification (RFID) dengan Multi Reader*”, Bandung: 2009.
- [2] Coutinho, S. C., “*The Mathematics of Ciphers, Number Theory and RSA Cryptography*”, Massachusetts: A K Peters, LTD., 1999.
- [3] Gay, Warren, “*Mastering The Raspberry Pi*”, Technology in Action, Apres, 2014.
- [4] Munir, Rinaldi, “*Kriptografi*”, Bandung: Informatika, 2006.
- [5] RSA Laboratories, “*Is the RSA cryptosystem currently in use?*”, <http://www.rsa.com/rsalabs/node.asp?id=2222> (diakses tanggal 11 Februari 2013).
- [6] Susanti, Roza dan Budi Bakhtiar, “*Pengaturan Portal Pada Pengurutan Parkir Mobil dengan Menggunakan RFID dan PC*”. Padang: Elektron Vol. 1 No. 2, 2009.
- [7] Winoto, Ardi, “*Mikrokontroler AVR Atmega8/32/16/8535 dan Pemrogramannya dengan Bahasa C pada WinAVR*”, Bandung: Informatika, 2008.