ISSN 2460-1160

Rancang Bangun Sistem Informasi e-Payment Menggunakan RFID (Radio Frequency Identification) Berbasis Website (Studi Kasus : Kantin JTI Politeknik Negeri Malang)

Muchammad Iqbal Arief Pradana[1]

[1] Teknologi Informasi, Teknik Informatika, Politeknik Negeri Malang
[1] nyikdewo@gmail.com

Kemajuan ilmu pengetahuan tentang teknologi dan informasi di era sekarang ini sangatlah pesat baik dibidang Industri maupun dibidang Pemasaran. Saat ini dibidang pemasaran masih menggunakan pembayaran uang dalam bentuk fisik, mengakibatkan susahnya pengembalian uang lebih dan panjangnya antrian konsumen sehingga diperlukan metode pembayaran yang praktis dan cepat untuk mempersingkat waktu dalam transaksi. Pada kantin JTI Politeknik Negeri Malang terdapat permasalahan seperti yang ada diatas.

Maka dari itu dilakukannya penelitian "Rancang Bangun Sistem Informasi *e-Payment* Menggunakan RFID (*Radio Frequency Identification*) Berbasis Website**"** menggunakan metode Kriptografi Algoritma RSA. Agar pada kantin JTI Politeknik Negeri Malang tidak terjadi permasalahan antrian yang panjang dan proses transaksi yang lama.

Sistem Informasi *e-Payment* ini didukung dengan model algoritma RSA yang merupakan algoritma enkripsi maupun dekripsi dalam kriptografi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu yang bertujuan agar informasi tidak dapat terbaca oleh orang lain kecuali orang yang berhak.

Pada metode Kriptografi Algoritma RSA terbukti dari hasil pengujian yang dilakukan, metode RSA ini berjalan dengan baik untuk mengamankan data *customer*. Hasil dari perancangan sistem informasi menggunakan RFID ini terbukti dapat mempermudah dalam proses transaksi dan dapat di aplikasikan di kehidupan nyata

Kata kunci—Sistem Informasi e-Paymenmt, Kriptografi Algoritma RSA, RFID

I. PENDAHULUAN

Kemajuan ilmu pengetahuan tentang teknologi dan infromasi di era sekarang sangatlah pesat baik dibidang Industri maupun dibidang Pemasaran. Mau tidak mau kita haurs mengikuti perkembangan teknologi agar tidak tertinggal, Saat ini dibidang peasaran masih menggunakan pembayaran uang dalam bentuk fisik, mengakibatkan susahnya pengembalian uang lebih dan panjangnya antrian konsumen sehingga diperlukan metode pembayaran yang praktis dan cepat untuk mempersingkat waktu dalam transaksi.

Hadirnya teknologi RFID ini dapat membuat transaksi lebih raktis dan cepat dalam artian pelanggan tidak lagi membawa uang dalam bentuk fisik untuk melakukan transaksi. Transaksi ini juga membantu untuk mempercepat proses transaksi karena hanya perlu menempelkan *smart card* ke RFID *reader* yang terdapat di kasir. Pelanggan juga dapat melihat saldo di *website*.

Sistem informasi *e-payment* ini didukung dengan model Algoritma RSA yang merupakan algoritma enkripsi maupun dekripsi dalam kriptografi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu yang bertujuan agar informasi tidak dapat terbaca oleh orang lain kecuali orang yang berhak

II. LANDASAN TEORI

RFID menurut (GAO, 2005) merupakan salah satu bentuk perkembangan dari teknologi nirkabel (*wireless*) yang digunakan sebagai pengganti teknologi barcode.

Kantin menurut (Nuraida L, 2014) merupakan Keramik merupakan tempat yang menyediakan makanan dan minuman untuk memenuhi kebutuhan gizi siswa ketika berada di sekolah. Kantin sekolah mewujudkan pesan-pesan kesehatan dan menentukan perilaku makan siswa sehari-hari melalui penyediaan makanan jajanan di sekolah. Kantin sekolah dapat menyediakan makanan sebagai penggani makanan pagi dan makan siang serta camilan dan minuman yang sehat, aman dan bergizi.

Menurut penelitian (Dony Ariyus ,2008), Kriptografi sebenarnya adalah suatu metode yang sering sekali digunakan untuk melindungi berbagai macam data yang prosesnya disebut dengan encryption, yaitu suatu proses yang mengkonversi sebuah pesan plantext menjadi sebuah ciphertext yang bisa dibalik ke bentuk asli seperti semula, yang juga bisa disebut dengan proses decoding atau decryption

Sedangkan menurut (Antonius Wahyu Sudrajat, 2006), decryption adalah kebalikan dari encryption yaitu transformasi dari data yang dienkripsi (ciphertext) kembali kebentuk semula (plantext). Proses enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, yang sering disebut dengan kunci (key). Menurut Antonius Wahyu Sudrajat tahun 2006, bahwa transparent data encryption menawarkan dari sisi pengguna sehingga pengguna dapat langsung melakukan proses enkripsi data tampa melakukan coding dan kompleksitas manajemen key.

Kriptografi Algoritma RSA Menurut (Triorizka, 2010) RSA merupakan salah satu dari *public key cryptosystem* yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital. Langkah-langkah untuk menerapkan metode Kriptografi Algoritma RSA, yaitu :

1. Langkah Pertama : Pembangkit kunci dengan cara pilih 2 buah bilangan prima yang besar, p dan q untuk mendapatkan keamanan yang maksimum, dipilih bilangan p dan q kemudian dihitung :.

   $$N = pq \quad (2.1)$$

   Dimana :
   N = modulus yang digunakan
   Dmin = bilangan prima dari pembangkit kunci

   Kemudian dihitung :
   $\varphi = (p-1)\,(q-1)$

   lalu pilih kunci enkripsi e secara acak, kemudian dihitung kunci dekripsi d, sedemikian sehingga :
   $ed = 1 \bmod (p-1)(q-1)$
   Atau
   $ed - 1 = k\,(p-1)(q-1) \quad (2.2)$

   keterangan :
   e dan d = enkripsi dekripsi
   k = *key* atau kunci

2. Langkah Kedua : Proses Enkripsi
   Prosedur enkripsi pada algoritma rsa adalah dengan mengubah plainteks mencadi chiperteks dengan mengikuti aturan berikut :
   Bagi pesan menjadi beberapa kelompok mi, dengan i-1,2….| mi | = |n|-1. Kemudian setiap kelompok dengan

Ci = mi^e mod n **(2.3)**

Dimana :

Ci = proses enkripsi

Mi = proses dekripsi

Ingat bahwa proses dekripsi dilakukan dengan menggunakan kunci public

3. Langkah Ketiga : Proses Dekripsi
   Prosedur dekripsi merupakan kebalikan dari enkripsi, proses ini mengubah cipherteks menjadi plainteks, atau pesan asli. Prosedur ini proses dekripsi algoritma RSA adalah sebagai berikut :
   Bagi chiperteks c kedalam ci, dengan 1=1,2,…,| ei |=|n|-1
   Kemudian dekrip setiap ci dengan
   Mi = ci^d mod n **(2.4)**
   Dimana :
   Ci = Proses Enkripsi
   Mi = Proses Dekripsi

III. METODOLOGI PENELITIAN

Data untuk proses kriptografi diambil dari kode yang berada di RFID Card. Disetiap RFID Card memiliki kode unik yang berbeda-beda yang nantinya proses enkripsi dan dekripsi akan diolah pada saat proses penbacaan kode di RFID Reader dan akan di dekripsi pada website.

Metode Pengolahan Data dilakukan dengan melakukan perhitungan kunci, enkripsi, dekripsi dengan menggunakan metode Kriptografi Algoritma RSA

a. Pembuatan Kunci
   1. Langkah Pertama : menentukan bilangan prima p q dan dihitung untuk menentukan bilanan n
      Rumus :
      n = p . q
      Dimana nilai p = 3 dan q = 17
      Hitungan n = 3.17 = 51
      Kemudian mencari φ (n) dengan rumus :
      φ (n) = (p-1)(q-1)
      φ = 2.16 = 32
      kemudian dicari relative prima terhadap φ. Sehingga didapati e=5
      untuk mencari nilai d dengan rumus :
      Euclidean algorithm
      φ x + e y = 1
      32x + 5y=1
      32 = 6(5) + 2
      5 = 2(2) + 1
      2 = 1 (1) +1
      Proses selanjutnya adalah back substitution :
      1 = 2-1(1)
      1 = 2-1(5-2(2))
      1 = 1(2)-1(5)+2(2)
      1 = 3(2)-1(5)
      1 = 3(32-6(5))-1(5)
      1 = 3(32)-18(5)-1(5)
      1 = 3(32)-19(5)
      d = 32-19 = 13
      disini nilai d sudah ditemukan yaitu 13 yang berarti public key (5,51) dan private key (13,51)

   2. Langkah Kedua : Proses enkripsi
      Rumus :
      Pilih *plaintext* m, dengan 0≤m ≤ n-1
      Hitung ***c=m^e mod n***
      Diperoleh *chipertexts c,*

M= “49C514B3” m= “35 40 5 36 32 35 4 34”

TABEL 3. 1 PROSES ENKRIPSI

C	Nilai		Hasil
C1	35^5	Modulus 51	35
C2	40^5		7
C3	5^5		14
C4	36^5		15
C5	32^5		2
C6	35^5		35
C7	4^5		4
C8	34^5		34

   3. Langkah Ketiga : Proses Dekripsi
      Rumus :
      Hitung ***m = c^d mod n***
      Diperoleh *plaintext m ,* sebagai berikut :
      c = 35 7 14 15 2 35 4 34

TABEL 3. 2 PROSES DEKRIPSI

D	Nilai		Hasil
D1	35^13	Modulus 51	35
D2	7^13		40
D3	14^13		5
D4	15^13		36
D5	2^13		32
D6	35^13		35
D7	4^13		4
D8	34^13		34

IV. KESIMPULAN DAN SARAN

a. Kesimpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan dapat ditarik kesimpulan sebagai berikut:

a. Rancang dan bangun sistem informasi e-payment dan topup berhasil diterapkan sesuai dengan rancangan awal
b. Metode kriptografi algoritma RSA berhasil diterapkan pada sistem yang berfungsi untuk keamanan sistem
c. Memberikan fitur diskon pada sistem informasi e-payment

b. Saran

Saran yang dapat diberikan dari hasil penelitian untuk pengembangan sistem ini kedepan sebagai berikut:

a. Diharapkan sistem dapat membaca RFID Tag secara otomatis ketika ditempelkan RFID Reader
b. Diharapkan dapat menambah fitur print bukti transaksi dengan tambahan perangkat thermal printer
c. Dapat mencoba metode lain dalam sistem informasi transaksi seperti metode dicision tree

DAFTAR PUSTAKA

GAO (United States Government Accountability Office), Information Security : Radio Frequency Identification Technology in the Federal Government, GAO-05-551, May 2005.s

Nuraida L, Kusumaningrum H, Palup NS, Koswara S, Madanijah S, Zulaikhan, Madjij AS, Ariani, Triwahyunto A. 2014. Menuju Kantin Sehat. Direktorat Jendral Kementrian Pendidikan dan Kebudayaan, Jakarta

Triorizka, Andrianus, 2010., Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature Dengan .Net

Ariyus, Dony. 2008 "*pegantar ilmu kriptografi: teori analisis & implementasi"*. Yogyakarta

Sudrajat, Wahyu, Antonius. 2006. *"Implementasi Enkripsi Database Menggunakan Transparent Data Encryption Pada Database Engine Oracle"*. Palembang : Jurnal Ilmiah STMIK GI MPD Vol.2, No.3 Oktober 2006: 14-19.