PROGRAM KEAMANAN PADA TRANSAKSI E-PAYMENT DENGAN MENGGUNAKAN METODA ONE-TIME PASSWORD (OTP) DENGAN MENGGUNAKAN ALGORITMA AES-128 SEBAGAI PASSWORD GENERATOR

Arieldo Meizul Zuki[1], Yudha Purwanto[2], Sofia Naning Hertiana[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

---

Abstrak

Kata Kunci :

Abstract

The most important aspect that has to be paid attantion on e-payment services is the security level of that services. With a lot of data transfer that happened on that services, some information data became most likely be vurnerable toward some attack form some unauthorized parties. The other problem is that, how would the user as well as the bank server knows that the identity that entering their system is a valid user. In other word, the authentificities of the data transmitted on the e-payment service became a factor that decides the outcome of the transaction between both parties.

The current securities procedures always using password as the authentification procedures on the e-payment transcation, for example if a user want to login on an e-payment or banking server, users have to enter their PIN (personal Identification Number) as their password. But, if the password/PIN always the same (static password) and the user continuesly re-entering the PIN, then it makes it most likely an easy mark for carders and sniffers to obtain those PIN.

This program has yet to reach the perfection, because theres still a bug that could be found at the main program, and this particular bug is the biggest obstackle that render this project failure because its shaking the very foundation of Rijndael Algorithm, which could only process 8 bits on each column of the state array. Because of there's a limitation on Java Programming Library which do not support the calculation of checksum and carry, so the exclusive library is needed. That's why this project can't be finished.

Keywords : Personal Identification Number, One-Time Password, AES 128 dan Carding

---

BAB I
PENDAHULUAN

1.1. Latar Belakang

Pada saat ini, Internet sudah menjadi sarana yang dapat dinikmati oleh semua orang. Banyak kemudahan yang bisa kita dapatkan dari *internet*. Salah satunya adalah kemudahan bertransaksi. Dengan adanya internet, kita dapat bertransaksi secara elektronik (baik pembayaran maupun transfer), atau lebih dikenal dengan *e-payment.* Pada metoda pembayaran ini yang perlu dilakukan hanya memberikan nomor *credit card* atau *debit card* pada *web* tempat belanja tersebut dan transaksi dapat dilaksanakan dengan cepat dan mudah.

Tetapi *internet* bukanlah suatu sarana yang selalu aman, ada banyak orang-orang yang tidak bertanggung jawab di luar sana yang menggunakan kemudahan *Internet* untuk manjahili dan mempersulit orang lain. Dan terkadang mereka melakukan tindakan illegal dan merusak seperti melakukan *hacking, cracking, sniffing,* dan banyak hal lain yang dapat merugikan orang lain. Dan salah satu tindakan yang sangat merugikan itu adalah *pencurian password* dan juga nomor *credit card* seseorang dan menggunakannya untuk kepentingan pribadi. Atau yang lebih dikenal dengan istilah *carding*.

Modus operandi yang paling sering digunakan dalam *carding* ini adalah dengan menyisipkan halaman web belanja palsu pada suatu situs perbelanjaan dan menunggu seseorang untuk melakukan pembelian (purchase) untuk item tersebut. Dan sewaktu seseorang melakukan *purchase* dan memasukkan nomor *credit card* serta *password*nya kedalam halaman *web*, halaman web palsu yang dibuat oleh *hacker* tersebut akan mengopi *password* dan juga nomor *credit card* orang tersebut. Dan pada akhirnya setelah *hacker* tersebut mendapatkan nomor *credit card* dan juga *password*nya, *hacke*r tersebut dapat melakukan transaksi eletronik menggunakan *credit card* orang yang malang tersebut.

Salah satu faktor yang membuat *carding* ini dapat dilakukan dengan mudah adalah karena orang-orang yang melakukan transaksi elektronik tersebut jarang mengganti *password* mereka. Dan juga ketidak-tahuan orang-orang mengenai *cyber crime* yang sering terjadi, baik modus operandil-nya maupun tanda-tandanya.

1.2. Tujuan Penelitian

Tujuan penelitian tugas akhir ini adalah untuk merancang suatu program yang dapat membantu menangani masalah *carding* dan juga beberapa *cyber crime* lainnya, seperti *direct attack* pada *server* dan juga *cracking* program pada server itu sendiri. Selain itu penelitian ini juga bertujuan untuk menganalisa performansi dari program ini sendiri. Performansi ini akan diuji dengan melakukan serangan-serangan seperti *carding*, *sniffing* dan juga *direct attack*.

1.3. Rumusan Masalah

Permasalahan yang dijadikan objek penelitian dan pengembangan tugas akhir ini adalah:

a. Pemodelan program pengamanan server *e-payment* dengan system *one-time password*, menggunakan *algoritma Rijndael*.
b. Pemodelan system database pada server *e-payment*.
c. Bagaimana simulasi program terhadap serangan *cyber* seperti *carding*, *sniffing* dan juga *direct attack*.
d. Bagaimana hasil dari simulasi program terhadap serangan tersebut, parameter yang dilihat adalah *success rate* dari serangan, *crash*, dan juga analisa kelayakan program.

1.4. Batasan Masalah

Batasan masalah dalam penelitian dan pengembangan tugas akhir ini adalah:

a. Implementasi pada jaringan internet.
b. Analisa performansi didapatkan dengan metoda *trial and error* dari serangan-serangan yang akan dilakukan, seperti *carding*, *sniffing*, dan juga direct *attack*.
c. Bahasa yang digunakan pada program adalah bahasa *Java-Script*.
d. *Hanya sistem keamanan yang diperhitungkan, dengan kata lain delay, jitter, dan packet loss* tidak diperhitungkan.
e. Hanya membahas pada jaringan IPv4.

1.5. Metoda Penelitian

Metodologi yang digunakan dalam menyelesaikan masalah dalam tugas akhir ini adalah:

a. Studi Literatur
   Merupakan kegiatan pembelajaran dan pemahaman materi mengenai konsep dan teori melalui berbagai sumber pustaka yang berkaitan dengan penelitian dan dapat mendukung proses perancangan system.

b. Desain dan Implementasi Sistem
   Pada tahap ini akan dilakukan perancangan dan implementasi system.

c. Pengujian dan Analisis Sistem
   Menganalisis performansi program yang ditekankan pada keberhasilan memblock serangan *cyber* seperti *carding*, *sniffing*, dan juga *direct attack*.
d. Penarikan Kesimpulan

1.6. Sistematika Penulisan

Penulisan tugas akhir ini akan dibagi dalam beberapa bagian, sebagai berikut:

1. **Bab I Pendahuluan**

   Berisi tentang latar belakang pembuatan tugas akhir, maksud dan tujuan pembuatan tugas akhir, pembatasan masalah, metodologi penulisan serta sistematika yang dilakukan dalam penulisan laporan tugas akhir.

2. **Bab II Dasar Teori**

   Berisi tentang penjelasan teoritis dalam berbagai aspek yang akan mendukung ke arah analisis tugas akhir yang dibuat.

3. **Bab III Perancangan dan Implementasi**

   Berisi penjelasan mulai dari proses desain hingga konfigurasi untuk implementasi system, serta skenario yang digunakan untuk melakukan pengujian.

4. **Bab IV pengujian dan Analisis**

   Berisi analisis dari implementasi sistem sesuai skenario yang telah ditetapkan.

5. **Bab V Kesimpulan dan Saran**

   Berisi kesimpulan yang diperoleh dari serangkaian kegiatan terutama pada bagian pengujian dan analisis. Selain itu juga memuat saran-saran pengembangan lebih lanjut yang mungkin dilakukan.

BAB V
KESIMPULAN DAN SARAN

1. Kesimpulan

Program ini belum berhasil diselesaikan dengan sempurna, karena masih terdapat bug (error) yang terjadi, dan bug tersebut merupakan halangan terbesar karena benar-benar menyalahi landasan teori dari algoritma Rijndael ini sendiri yang mana hanya boleh dan hanya dapat memproses 8 bit dalam satu kolom pada array state. Hal dikarenakan adanya checksum dan carry overflow yang ikut terproses dalam algoritma dan tidak bisa dihilangkan. Menurut analisa lebih lanjut diperlukan 4 library tambahan yang tidak terdapat pada progran Java standar (exclusive library) untuk mensupport program ini agar dapat berjalan dengan sempurna. Keempat exclusive library tersebut adalah:

- Adler32, diperlukan untuk memproses modulo dan pengaturan checksum serta carry overflow.
- Padding, diperlukan untuk memproses penambahan dan pengurangan bit pada array.
- Base64 Encoder, diperlukan untuk mengubah inputan menjadi byte dan bit yang akan diproses dalam program.
- Base64 Decoder, diperlukan untuk mengubah outputan program menjadi password yang bisa dikenali dan dipergunakan.

Dikarenakan tidak adanya 4 exclusive library tersebutmaka program ini belum bisa dilanjutkan.

2. Saran

Program ini masih perlu dilakukan penelitian lebih lanjut untuk menyelesaikan masalah *bug* dimana terdapat 9 bit pada satu kolom *array state*, yang mana sangat diharapkan dan dipercaya dapat diwujudkan apabila ada waktu dan *resources* yang mencukupi. Apabila akan dilakukan research lebih lanjut, sangat disarankan untuk mecari dan mempelajari lebih lanjut mengenai 4 exclusive library tersebut.

DAFTAR PUSTAKA

- FIPS 197: Federal Information Processing Standards Publication 197, "Announcing The Advanced Encryption Standard (AES)", NIST, 26 November 2001.
- Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael, Document version 2", NIST, 03 September 1999.
- Budi Raharjo, Imam Heryanto, Arif Haryono, "Mudah Belajar Java", Informatika, Januari 2009.
- M. Shalahuddin, Rosa A. S., "belajar Pemrograman dengan Bahasa C++ dan Java", Informatika, Maret 2009.
- Advanced Encryption Standard:
  - http://en.wikipedia.org/wiki/Advanced_encryption_standard.
- One-Time Password:
  - http://en.wikipedia.org/wiki/One_time_password.
- Wedagama, Made Bayu, "Desain dan Implementasi Sistem Keamanan Algoritma Rijndael (AES) dengan One-Time Password untuk Optimasi Layanan SMS Banking.", Tugas Akhir IT Telkom.