SISTEM PEMBAYARAN ONLINE MENGGUNAKAN STEGANOGRAFI DAN KRIPTOGRAFI VISUAL

Penulis: Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar, A. M. Bagul

Reviwer: Putu Bayu Baskara, Luh Ristiari, Made Yayang Eka Prananda

1. PENDAHULUAN

Belanja online juga disebut sebagai e-tail adalah cara pembelian produk melalui internet. Dalam belanja online ancaman umum adalah phishing dan pencurian identitas. Phishing adalah metode mencuri informasi rahasia pribadi seperti username, password dan rincian kartu kredit dari korban. Metode yang diusulkan dalam makalah ini menggunakan steganografi dan kriptografi visual. Ini mengurangi berbagi informasi antara pelanggan dan server pedagang dan melindungi informasi pelanggan.

2. STEGANOGRAFI DAN KRIPTOGRAFI VISUAL

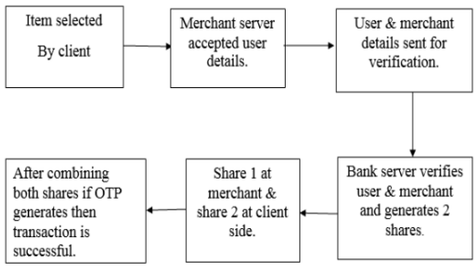
Steganografi adalah seni menyembunyikan pesan di dalam pesan lain. Ini adalah teknik menyembunyikan informasi ke dalam gambar. Steganografi terbuat dari dua kata steganos dan graphein. Teknik steganografi menggunakan teks, gambar, dan video, audio sebagai media penutup untuk menyembunyikan data. Kriptografi adalah studi tentang teknik untuk komunikasi yang aman di hadapan pihak ketiga. Ini adalah teknik enkripsi khusus di mana informasi visual dienkripsi sedemikian rupa sehingga dekripsi tidak memerlukan komputer. Kriptografi visual berisi dua gambar transparan. Satu gambar berisi piksel acak dan gambar lain berisi informasi rahasia.

3. TRANSAKSI BELANJA ONLINE

Dalam belanja online pelanggan memilih produk dari portal belanja online dan kemudian pelanggan diarahkan ke halaman pembayaran. Pedagang online dapat menggunakan sistem pembayaran pihak ketiga seperti PayPal, Web Money dan lain-lain. Di portal pembayaran online, pelanggan mengirimkan detail kartu kredit atau debitnya. Rincian informasi yang diberikan kepada pedagang online bervariasi dari satu gateway pembayaran yang lain. Menurut Standar Keamanan Data PCI, pedagang tidak diperbolehkan menyimpan informasi CVV atau data PIN. Pedagang online hanya dapat menyimpan informasi kartu seperti nama, nomor kartu, dan tanggal kedaluwarsa.

4. PEDAGANG DAN SERVER BANK

Dalam tulisan ini terdapat satu aplikasi admin dan satu produk admin. Fungsi dari aplikasi admin adalah untuk menambahkan server dan pengguna. Mungkin ada n jumlah pengguna tetapi hanya dua server yang kami gunakan yaitu satu server pedagang dan satu server palsu. Tujuan utama dari admin produk adalah untuk menambahkan berbagai kategori dan produk yang berbeda ke dalam kategori tersebut. Aplikasi klien adalah aplikasi android. Pada dasarnya klien mengakses berbagai produk yang ada di server pedagagng melalui aplikasi android.



Gambar 1 Server Merchant dan Bank

Gambar di atas menggambarkan apa peran server pedagang dan server bank dalam seluruh transaksi. Pengguna pertama-tama masuk ke situs pedagang kemudian akan memilih produk yang diinginkan. Informasi pengguna seperti: id pengguna, nama pengguna, kata sandi, dll akan dikirim ke server pedagang kemudian bersama dengan detail pengguna dan detail pedagang juga kirim ke server bank untuk verifikasi seperti id server pedagang, nama server pedagang, kata sandi dll. Server bank akan memberikan dua cara otentikasi dalam memverifikasi pengguna dan server pedagang.

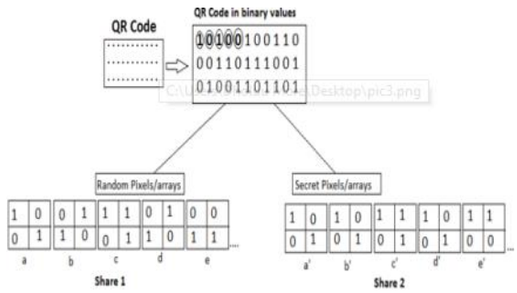
Pengguna memiliki login password dan password transaksi yang unik, sehingga jika ada pengguna palsu maka akan diverifikasi juga oleh server bank. Saat detail pengguna dan detail pedagang dikirim ke server bank, akan menghasilkan OTP. Dengan menggunakan steganografi, OTP yang dihasilkan dikonversi menjadi kode QR. Kemudian dengan menggunakan visual kriptografi kode QR akan dibagi menjadi dua bagian. Bagian pertama dikirim ke server pedagang dan bagian kedua dikirim ke pengguna melalui mail.

Nantinya, pada sisi pengguna akan disediakan fitur untuk menggabungkan dua bagian kode QR tersebut. Server pedagang akan mengirimkan bagian pertama dari kode QR ke pengguna, sedangkan bagian kedua didapatkan melalui email pengguna. Setelah berhasil digabungkan, maka akan menghasilkan kode QR lengkap. Kemudian setelah kode QR discan, akan didapat kembali OTP asli yang berasal dari server bank. Pengguna akan mengirimkan kembali OTP yang didapat ke server bank untuk verifikasi, kemudian akan diminta password transaksi dan jika password telah benar maka transaksi dapat dilakukan.

5. STEGANOGRAFI DAN ALGORITMA VISUAL KRIPTOGRAFI

Steganografi adalah teknik menyembunyikan pesan rahasia di dalam yang lain dan ekstraksi pesan rahasia di tempat tujuannya. Visual kriptografi adalah teknik khusus enkripsi untuk menyembunyikan informasi ke dalam gambar yang dapat didekripsi oleh penglihatan manusia jika gambar kunci yang benar digunakan.

Tujuan dari proyek pada paper ini adalah untuk memberikan keamanan yang lebih baik selama transaksi. Pada projek ini berfokus pada pembuatan dua share/gambar OTP melalui visual kriptografi. Dengan menggunakan steganografi, OTP akan menghasilkan sebuah kode QR. Gambar kode QR ini memiliki nilai 0 dan 1. Untuk membuat dua gambar dari OTP akan menggunakan matriks acak dua dimensi. Visual kriptografi menggunakan dua gambar tranparan, gambar pertama mengandung piksel/array acak dan gambar kedua mengandung pesan atau piksel/array rahasia.



Gambar 2 Algoritma Visual Kriptografi

Untuk membuat dua bagian dari kode QR, diperlukan proses XOR dan untuk menggabungkannya kembali diperlukan proses AND. Pertama, piksel pertama dari gambar kode QR di XOR dengan piksel/array yang dihasilkan secara acak dari matriks dua dimensi (a dalam Random Pixels/arrays) yang akan menghasilkan matriks baru (a' dalam Secret Pixels/arrays). Begitu seterusnya pada array (b), (c), (d), (e) akan menghasilkan array (b'), (c'), (d'), (e'). Sedangkan untuk menggabungkan kembali kode QR, proses AND dilakukan pada piksel (a) dan (a') maka akan dapatkan piksel asli dalam kode QR. Demikian pula jika melakukan AND dari (b) dan (b') dan seterusnya. Akan dapat mengambil kembali piksel asli dari kode QR.

6. KEUNTUNGAN

a) Sistem yang diusulkan menyediakan dua cara otentikasi.
b) Pencegahan phishing.
c) Menggunakan visual kriptografi untuk membuat dua bagian dari OTP untuk membuat sistem lebih aman.
d) Sistem mencegah pencurian identitas.
e) Ini juga memberikan keamanan data pribadi pengguna.

7. KESIMPULAN

Dalam paper ini digunakan dua metode yaitu Steganografi dan Visual Kriptografi untuk menyediakan transaksi aman selama belanja online. Ini mengamankan informasi rahasia pelanggan serta pedagang dan mencegah penyalahgunaan data di bank. Metode ini terutama menyangkut dengan mencegah pencurian identitas dan menyediakan pelanggan keamanan data. Ini juga mencegah phishing. Sistem mengotentikasi pengguna serta server pedagang (yaitu dua otentikasi).