Implementasi metode time synchronization one time password (OTP) menggunakan secure internet transaction

Pande K. Raka Susena H., author

Abstrak

Penggunaan internet sebagai media inforrnasi saat ini telah berkembang menjadi media penunjang kegiatan perekonomian. Terutama kegiatan perbankan sebagai sarana pembayaran perdagangan. Agar hanya orang yang memiliki hak atas rekeningnya yang melakukan kegiatan perekonomian, digunakan metode autentikasi untuk melindunginya. Metode ini menggunakan pasangan usemame dan password yang hanya diketahui oleh si pemilik account untuk proses pengesahan account sekaligus sebagai tanda pengenal dalam dunia maya. Untuk meningkatkan keamanan digunakan metode autentikasi One Time Password (OTP), password hanya dapat digunakan untuk satu kali proses autentikasi saja. Metode OTP yang banyak digunakan adaiah metode challenge response. Pemilik account akan mendapatkan password baru yang dapat digunakan unutk melakukan autentikasi setelah memasukkan challenge yang dikirimkan oleh server ke dalam suatu password generaton Password baru inilah yang dapat digunakan untuk melakukan proses autentikasi.

Pada skripsi ini dibahas pengembangan dari sistem OTP challenge response yang masih memitiki kelemahan adanya parameter tambahan berupa challenge, yang dapat membenkan infonnasi tambahan untuk pemecahan algoritma password itu sendiri. Aplikasi time synchronization authentication yang dibuat ini menggunakan metode time synchronous dengan menggunakan enkripsi ganda (BDES dan MD5), dimana client dan senrer akan sama-sama menghasilkan password baru untuk autentikasi setiap selang waktu satu menit. Untuk proses autentikasinya sendiri akan dilakukan pembandingan antara password baru yang dihasilkan oleh client dengan yang dihasilkan server. Sehingga tidak ada Iagi pengiriman informasi tambahan oleh server. Aplikasi dibuat dengan menggunakan bahasa pemrograman Java dan JBOSS (aplikasi database sekaligus server). Dari program yang dihasilkan dilakukan uji coba dan analisa terhadap OTP yang dinasilkan dari masukan berupa perubahan PIN dan waktu akses, serta analisa faktor keamanan Dari sini didapat data bahwa autentikasi aplikasi Iayanan perbankan dengan metode Time syncronizalion authentication ini dapat mengatasi masalah network snifling, replay attack, dan masquerade namun masih memiliki kelemahan terhadapa ancaman penangkapan identitas. Faktor keamanan yang dihasilkan cukup tinggi karena sangat kecil peluang untuk mengetahui password yang sebenamya dengan jalan mencoba-coba dalam selang waktu satu menit untuk berhasil.