Studi dan Implementasi Kriptografi pada Pemungutan Suara dalam Pemilihan Umum Secara Online

Muhammad Ihsan (13504120)[1)]

1) Program Studi Teknik Informatika ITB, Bandung 40132, email: if14120@students.if.itb.ac.id

Abstract – *Makalah ini membahas studi kasus dan implementasi kriptografi dalam pengamanan pemungutan suara secara online dalam pelaksanaan Pemilihan Umum(Pemilu). Dalam pelaksanaan pemilu, pemilih akan memberikan suatu status dipilih atau tidak terhadap kandidat yang bakal dipilih.*

Kriptografi berperan dalam menangani permasalahan pemungutan suara konvensional dan modern yang terintegrasi dalam sistem pemungutan suara secara online dalam rangka pemilihan umum.

Penanganan authentifikasi dan verifikasi pemilih diperankan oleh public key. Untuk protokol penverifikasi pemilih, menggunakan Blind Signature Protokol.

Dalam pemungutan suara secara online ini, ada 4 kebutuhan yang harus terpenuhi yaitu anonimyty, completeness, uniqueness dan correctnes. Selain itu, juga adanya third party seperti authority of certification, authority of authentication, authority of collection. Tiga hal ini, yang berperan dalam menjamin terpenuhinya kebutuhan tadi.

Kata Kunci *: pemilu, protokol, kriptografi.*

1. PENDAHULUAN

Perkembangan penggunaan internet sejalan dengan perkembangan layanan yang mampu didukungnya, membuat banyak pengguna bisa melakukan banyak hal melalui internet. Mulai dari perdagangan dengan elektronik ini, kerja jarak jauh, pencarian data, dan banyak hal lainnya.

Akibatnya banyak pekerjaan yang biasanya menyita waktu dan tempat menjadi pekerjaan yang bisa dilakukan dimanapun dan kapanpun. Bahkan kadang tanpa perlu keluar dari rumah.

Semua itu dapat dilakukan dengan syarat, cukup memiliki sebuah “komputer” dan terhubung dengan internet. Kenapa disebut “komputer” karena sekarang ini, komputer bukan hanya sebuah monitor dengan CPU dan *keyboard*, tapi bisa saja cukup dengan sebuah telepon seluler dengan kemampuan hampir menyamai sebuah komputer sederhana.

Dengan melihat penggunaan internet yang semakin meluas dan mampu melayani banyak hal, seharusnya pemerintah bisa memanfaatkan media ini dalam melayani masyarakat. Beberapa program yang telah mulai digunakan adalah e-government. Program ini didesain agar lebih mudah untuk melayani masyarakat, dan masyarakat juga akan lebih mudah dalam mengurus administrasi dengan pemerintah.

Salah satu permasalahan lain yang mungkin dapat memanfaatkan internet adalah pemilihan umum dengan metode pemungutan suara secara online. Dengan penggunaan internet diharapkan penghitungan suara menjadi jauh lebih cepat dan pengawasan penggunaan hak pilih pemilih juga lebih mudah.

Ada beberapa syarat yang harus dipenuhi oleh pemungutan suara secara online, yaitu ;

a. Setiap pemilih hanya boleh memilih satu kali
b. Setiap pemilih hanya bisa memilih dalam satu tempat saja dalam satu waktu
c. Setiap pemilih bisa memilih dimana saja
d. Pemilih yang masuk ke sistem memang benar pemilih yang bersangkutan
e. Pemilih yang berhak yang memilih
f. Sistem harus siap dari serangan

Untuk studi kasus dibidang kriptografi sendiri akan mengambil posisi di beberapa bagian dalam menangani syarat-syarat diatas.

Selain itu, kriptografi sangat berperan penting dalam sistem ini. Karena banyak data yang perlu disembunyikan, dijamin dalam sistem ini.

Beberapa persoalan yang muncul dalam metode konvensional adalah dalam penghitungan suara membutuhkan waktu yang lama, kecurangan penggunaan hak suara.

Selain permasalahan tradisional tersebut, persoalan modern sejalan dengan penggunaan internet juga

harus diatasi. Inilah peran kriptografi.

Ada pendapat menyebutkan :

"The image is that it was a successful process. [It was] successful only if you compare it to nothing. If you compare it to any official election held in the country, it would have been labeled a disaster."- Election Center director Doug Lewis [Bu00]

"Lacking clear and explicit guidelines, we therefore went to great lengths in Arizona to implement rigorous procedures and protocols to ensure ballot sanctity and universal accessibility"-election.com CEO Joe Mohen [MG01]

2. Kriptografi dalam Sistem

2.1. Authentifikasi dan Verifikasi Pemilih

Setiap pemilih akan memiliki kartu identitas sendiri dan juga memiliki sebuah kata sandi, kata sandi ini yang harus diingat setiap pemilih. Dan dengan menggunakan protokol kunci publik, authentifikasi pemilih dilakukan. Dengan menggunakan kartu yang dimiliki pemilih authentifikasi ini dilakukan, dimana di dalam kartu tersimpan suatu kunci. Kunci ini akan didenkrip menjadi suatu plainteks, dan kunci yang telah dalam bentuk plainteks ini dikirim ke server sistem. Dalam server terdapat basisdata pemilih dan kunci masing-masing. Sehingga tidak ada user lain yang bisa mengakses selain yang terdaftar pada basisdata dan dengan kunci yang ada pada basisdata.

Untuk memverifikasi bahwa pemilih yang berhak yang melakukan pemilihan, maka setiap pemilih akan memasukkan kunci yang diketahui oleh pemilih sendiri. Kunci ini lah yang akan digunakan sistem untuk mencek apakah sesuai pemilih tersebut memang benar pemilih yang bersangkutan.

2.2. Blind Signature

Blind signature skema berupa suatu protokol kriptografi antara user, U dan Signer, S sehingga S akan memberikan sign pada pesan yang dikirim U tanpa perlu mengetahui isi pesan.

Tujuan utama dari tipe protokol kriptografi ini adalah untuk menjaga S dari observasi pesan dan tanda tangan yang diberikan. Setiap protokol blind digital membutuhkan 2 komponen, yaitu ;

a. Suatu protokol yang dibangun oleh S misalkan S(m) merupakan tanda tangan dari pesan m.
b. Dua fungsi, f dan g yang hanya diketahui oleh S, dimana g(S(f(m))) = S (m)

Fungsi f ini disebut *blinding function*. Sedangkan fungsi g disebut unblinding function. Untuk lebih mengamankan lagi, digunakan RSA sebagai basis dari protokol blind signature ini.

Pada RSA, misalkan n = p.q yang merupakan dua bilangan prima besar. Misalkan tanda tangan digital ini digunakan oleh S dengan kunci publik (n,e) dan kunci privat d. Misalkan k suatu bilangan integer sehingga gcd(n,k) = 1.

Sehingga fungsi blinding adalah :

$$f : Z_n \rightarrow Z_n$$

$$f(m) = m \cdot k^e \pmod n$$

Sedangkan fungsi unblinding :

$$g : Z_n \rightarrow Z_n$$

$$g(m) = k^{-1} \cdot m \pmod n$$

Dan juga harus memenuhi :

$$\begin{aligned} g(S(f(m))) &= g(S(mk^e \pmod n)) \\ &= g(m^d k \pmod n) \\ &= m^d \pmod n \\ &= S(m) \end{aligned}$$

Protokol Blind Signature ini berupa :

a. Fase Inisialisasi
   Misalkan
   $0 \le m \le n-1$
   yang merupakan pesan dari U yang akan disign oleh S. Dan suatu himpunan k yang dipilih oleh S
   $0 \le k \le n-1$
   $gcd(n,k) = 1$

b. Fase Blinding
c. U mengkomputasi
   $m^* = f(m) = mk^e \pmod n$ dan ini dikirim pada S.

d. Fase Signing
   S mengkomputasi
   $s^* = S(m^*) = (m^*)^d \pmod n$ dan dikirim kepada V

e. Fase Unblinding
   U mengkomputasi

$s = S(m) = g(S(m^*)) = k^{-1} s^* (\text{mod } n)$
Ini lah tanda tangan digital yang akan digunakan dalam pesan m.

3. Protokol Pemungutan Suara Online

Untuk membangun pemilihan kita menggunakan operasi XOR, validasi sangat dibutuhkan dengan menggunakan protokol Blind Signature.

Ada empat bagian yang akan di-*handle :*

a. Pemilih (P_1, P_2, ..., P_N)
Mereka yang menjadi pemain utama dalam sistem ini. Setiap pemilih harus memilih satu pilihan.

b. Authority of certification (A_0)
Fungsi utama yaitu menyediakan sertifikat digital untuk pemilih yang terdaftar dan untuk mengeluarkan tanda tangan digital blind.

c. Authority of authentication(A_1)
Fungsi utamanya adalah untuk mengautentikasi pemilih yang terdaftar dan menyediakan *tool* dalam pelaksanaan pemungutan suara

d. Autority of collection(A_2)
Bertanggung jawab dalam mengumpulkan hasil pemungutan suara, untuk memberifikasi kevalidan data tersebut, menyimpan dan menghitung kembali.

Berikut protokol dalam pemungutan suara secara online :

a. A_0 memberikan sertifikat digital kepada setiap pemilih yang terdaftar dan sah.
b. Setiap P_i diidentifikasi oleh A_1 dengan memvalidasi sertifikat digital dan mengirimkan secara berurutan suatu bit acak $B_i \in F_2^N$ kepada pemilih
c. Setiap pemilih memilih, $v_i \in F_2^N$ dimana ;
   - Jika V_i memilih pilihan 1, maka :
     $V_i = B_i \oplus (0, \ldots, 1, 0, \ldots 0)$
   - Jika V_i memilih pilihan 2, maka :
   - $V_i = R_i \oplus (0, \ldots, 0, 0, \ldots 0)$

d. Setiap pemilih V_i memilih secara acak satu bit
$C_i \in F_2^N$
Dan mengkomputasi
$P_i = v_i \oplus c_i$

e. A_0 membuat suatu blind signature dari P_i, P_i^* dan memberikan kepada V_i dan memberikan nilai $S(P_i)$
Setiap pemilih V_i mengirimkan kepada A_0 sekumpulan bit $C_i \in F_2^N$
f. Setiap V_i mengirimkan A_2 pilihannya yang telah disign oleh A_0 : $S(P_i)$
g. A_0 mengkomputasi :
$C = C_1 \oplus C_2 \oplus C_3 \oplus \ldots \oplus C_N$
Dan mengirimkannya kepada A_2
h. A_1 mengkomputasi :
$B = B_1 \oplus B_2 \oplus B_3 \oplus \ldots \oplus B_N$ $B_i \in F_2^N$
i. A_2 memverifikasi keabsahan setiap pilihan $S(P_1),\ldots,S(P_n)$ dengan mengambil nilai $P_1,..,P_N$
j. A_2 mengkomputasi
$P = P_1 \oplus P_2 \oplus P_3 \oplus \ldots \oplus P_N$
$P \oplus C = v_1 \oplus v_2 \oplus v_3 \oplus \ldots \oplus v_N = v$

k. A_2 mengkalkulasi jumlah pemilih yang memilih pilihan 1.
Pilihan 1 : d_H (v, B)
Pilihan 2 : N – d_H (v, B)
l. Terakhir A_2 menampilkan bit $P_1,\ldots,P_N$ bersama dengan C.

4. Analisis Properti dari protokol

Hasil analisis kebutuhan dalam suatu pemilihan sesuai dengan protokol yang diajukan

a. Tidak ada satupun Authority yang bisa menentukan bahwa Pemilih siapa yang memilih apa. Walaupun bisa mengetahui bit C_i namun sulit untuk menentukan bit itu dari siapa. Karena A tidak mengetahui B_i.
b. Completeness
Properti ini menjamin keberlangsungan secara utuh, mulai dari pemberian sertifikat digital oleh A_0 sampai membuat blind signature yang berbeda untuk setiap pemilih
c. Correctness
Setiap pemilih dapat memverifikasi pilihannya.
d. Uniqueness
Setiap pemilih hanya bisa memilih satu yang valid.

5. KESIMPULAN

Dalam pemungutan suara secara online ini mengharuskan setiap pemilih memilih di antara dua pilihan.

Skema yang dimunculkan disini amat sederhana hanya dengan menggunakan operasi biner XOR untuk pemilihan itu sendiri.

Disamping itu, kebutuhan lain seperti authority of certification yang memberikan sertifikat digital juga mendukung sistem ini. Semua itu untuk mendukung kebutuhan Anonimyty, completeness, uniqueness dan correctness.

DAFTAR REFERENSI

[1] R. Munir, "Catatan Kuliah Kriptografi", 2006.

[2] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, A. Vaccarelli. << SEAS, a secure e-voting protocol : Design and Implementation" Comput. Secur., vol. 24 (8), pp. 642-652, 2005