SISTEM PEMILU *ONLINE* BERBASIS PROTOKOL *TWO CENTRAL FACILITIES*

Muhammad Ilyas Sikki
Program Studi Teknik Elektro
Fakultas Teknik Universitas Islam "45" (UNISMA)
Jl. Cut Meutia No. 83 Bekasi, Indonesia
Telp. 021-88344436, 021-8802015 Ext.124

Abstract

An election is an simple example of a scenario where security and confidentiality of data between parties is critical. General election system that used in Indonesia as it long still use conventional trick that evokes a lot of problem as elector of double, voice distension and another fault and also long time for vote count. This conventional trick also require big costs and resources. To settle that thing, one of solution which can be done is use electronic voting (e-voting) with arrange general election system online that building to use a safe protocol.System that is made has default pock secure voting reguirements to get settles and secure security each threat which will happen. One of protocol which can accomplish partly criterion default secure voting reguirements and has security zoom that passably is Two Central Facilities Protocol , where consisting of Central Legitimazation Agency (CLA) for elector validation and Central Tabulating Facility (CTF) for vote count.

Keywords : *General election system, e-voting, Two Central Facilities, Central Legitimazation Agency, Central Tabulating Facility.*

1. PENDAHULUAN

Pemilu (Pemilu) disebut juga dengan "*Political Market*" (Dr. Indria Samego), artinya bahwa pemilu adalah pasar politik tempat individu/masyarakat berinteraksi untuk melakukan kontrak sosial (perjanjian masyarakat), antara peserta pemilu (partai politik) dengan pemilih (rakyat) yang memiliki hak pilih setelah terlebih dahulu melakukan serangkaian aktivitas politik yang meliputi kampanye, iklan politik melalui media massa cetak, audio (radio) maupun audio visual (televisi) serta media lainnya seperti spanduk, pamflet, selebaran bahkan komunikasi antar pribadi yang berbentuk *face to face* (tatap muka) atau lobi-lobi yang berisi penyampaian pesan mengenai program, platform, asas, ideologi serta janji-janji politik lainnya, guna meyakinkan pemilih sehingga pada pencoblosan dapat menentukan pilihannya terhadap salah satu partai politik yang menjadi peserta pemilu untuk mewakilinya dalam badan legislatif maupun eksekutif.

Sepanjang sejarah Indonesia, sejak meraih kemerdekaan 1945, Indonesia tercatat telah 10 kali menyelenggarakan pemilu yang dimulai dari tahun 1955 sampai tahun2009 dan masih bersifat konvensional. Banyak kendala dan permasalahan yang timbul pada penyelenggaraan pemilu secara konvensional, beberapa masalah yang ditimbulkan antara lain sebagai berikut :

- Banyak terjadi kesalahan dalam proses pendataan dan pendaftaran pemilih.
- Pemilih salah dalam memberi tanda pada kertas suara.
- Proses pengumpulan kartu suara yang berjalan lambat.
- Kurang terjaminya kerahasiaan dari pilihan yang dibuat oleh seseorang.
- Keterlambatan dalam proses tabulasi hasil perhitungan suara di daerah.

Sistem pemilu yang digunakan selama ini harus segera diperbaharui dan beralih ke sistem pemilu online menggunakan *e-voting* sebagai salah satu solusi untuk mengatasi permasalahan yang timbul.*E-voting* menawarkan beberapa keunggulan dibandingkan sistem konvensional, diantaranya mempercepat

perhitungan suara, memudahkan pengolahan suara, memudahkan verifikasi, menghemat biaya, dan meningkatkan efektifitas pelaksanaan pemilu.

Seperti halnya dengan sistem pemilu yang diadakan secara konvensional, pelaksanaan sistem pemilu secara *online* pun pasti tidak akan terhindar dari berbagai ancaman kecurangan yang mungkin terjadi. Oleh karena itu, sistem yang dibuat harus memenuhi standar *secure voting reguirements* menurut paparan Bruce Schneier (1996) untuk dapat mengatasi dan menjamin keamanan setiap ancaman yang akan terjadi. Salah satu protokol yang dapat memenuhi sebagian standar kriteria *secure voting reguirements* dan memiliki tingkat keamanan yang cukup baik adalah *Two Central Facilities Protocol*, dimana terdiri dari *Central Legitimazation Agency* (CLA) untuk pengesahan pemilih dan *Central Tabulating Facility* (CTF) untuk perhitungan suara (Bruce Schneier, 1996).

2.TINJAUAN PUSTAKA

2.1 Keamanan Komputer

Bishop (2003) mengemukakan bahwa keamanan komputer mencakup tiga aspek utama, yaitu kerahasian (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).Interpretasi dari setiap aspek pada lingkungan suatu organisasi ditentukan oleh kebutuhan dari individu yang terlibat, kebiasaan dan hukum yang berlaku dalam organisasi tersebut.

2.2 Kriptografi

Kriptografi berasal dari gabungan kata kripto yang berarti rahasia dan grafi yang berarti tulisan.Definisi kriptografi merupakan seni dan ilmu untuk menjaga keamanan pesan (Schneier, 1996). Terdapat empat tujuan utama dari kriptografi sebagai berikut :

a. **Kerahasiaan** adalah suatu layanan yang digunakan untuk menjaga isi informasi dari semua pihak yang tidak berwenang memilikinya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.
b. **Integritas** adalah suatu layanan yang berkaitan pengubahan data atau informasi dari pihak-pihak yang tidak berwenang. Untuk menjamin integritas data, harus mampu mendeteksi manipulasi data dari pihak-pihak yang tidak berwenang. Manipulasi data yang dimaksud disini diartikan sebagai hal-hal yang berkaitan dengan penghapusan, penyisipan, dan pergantian data.
c. **Otentikasi** adalah suatu layanan yang berhubungan dengan identifikasi entitas dan informasi itu sendiri. Dua pihak yang terlibat dalam komunikasi seharusnya mengidentikasi dirinya satu sama lain. Informasi yang disampaikan melalui satu saluran (*channel*) seharusnya dapat diidentifikasikan asalnya, isinya, tanggal dan waktunya. Atas dasar ini otentikasi terbagi menjadi dua kelas besar, yaitu otentikasi entitas dan otentikasi asal data.
d. **Non-repudiasi** adalah suatu layanan yang ditujukan untuk mencegah terjadinya pelanggaran kesepakatan yang telah dibuat sebelumnya oleh entitas. Apabila sengketa muncul ketika suatu entitas mengelak telah melakukan komitmen tertentu, maka suatu alat untuk menangai situasi tersebut diperlukan. Misalnya, suatu entitas mendapatkan wewenang dari entitas lainnya untuk melakukan aksi tertantu, kemudian mengingkari wewenang yang diberikan, maka suatu prosedur yang melibatkan pihak ketiga yang dipercaya untuk menyelesaikan sengketa itu.

2.2 Protokol Kriptografi

Suatu protokol adalah serangkaian langkah-langkah yang melibatkan dua pihak atau lebih dan dirancang untuk menyelesaikan suatu tugas (Schneier, 1996). Protokol memiliki beberapa karakteristik sebagai berikut :

a. Protokol memiliki urutan dari awal hingga akhir.
b. Setiap langkah harus dilaksanakan secara bergiliran.
c. Suatu langkah tidak dapat dikerjakan apabila langkah sebelumnya belum selesai.
d. Melibatkan dua pihak atau lebih untuk melaksanakan protokol.
e. Protokol dirancang untuk mencapai suatu hasil
f. Setiap orang yang terlibat dalam protokol harus mengetahui terlebih dahulu mengenai protokol dan semua langkah yang akan dilaksanakan.
g. Setiap orang yang terlibat dalam protokol harus menyetujui untuk mengikutinya.

h. Protokol tidak boleh menimbulkan kerancuan (ambigu) dan tidak boleh timbul kesalahpahaman.
i. Protokol harus lengkap, harus terdapat aksi yang spesifik untuk setiap kemungkinan situasi.

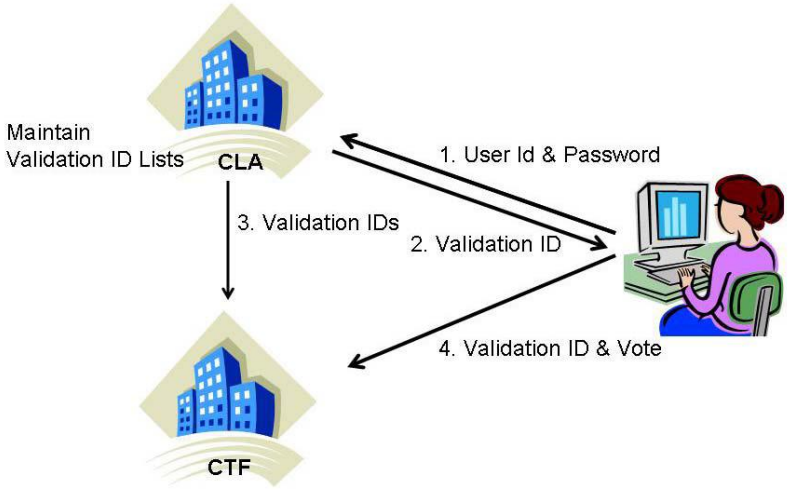
2.4 Protokol Two Central Facilities

Pemilihan menggunakan protokol *Two Central Facilities* dilakukan dengan membagi CLA dan CTF menjadi dua bagian yang berbeda. Menurut Sireesha dan Chakchai (2005) pemilihan dengan *Two Central Facilities* adalah sebagai berikut :

a. Setiap pemilih mengirim pesan kepada CLA dan meminta nomor validasi.
b. CLA mengirim nomor validasi acak kepada pemilih dan menyimpan daftar setiap nomor validasi. CLA juga menyimpan sebuah daftar dari nomor validasi penerima

c. untuk mengantisipasi seseorang memilih dua kali.
d. CLA mengirim daftar nomor validasi kepada CTF.
e. Setiap pemilih memilih nomor identifikasi secara acak lalu membuat pesan dengan nomor tersebut, yaitu nomor validasi yang diperoleh dari CLA dan suaranya. Pesan ini kemudian dikirimkan kepada CTF.
   CTF memeriksa dan membandingkan nomor validasi dengan daftar yang diterima dari CLA. Jika nomor validasi terdapat pada daftar maka nomor tersebut akan disilang untuk menghindari pemilih memilih dua kali. CTF menambahkan nomor identifikasi pada daftar pemilih yang telam memberikan suara pada kandidat tertentu dan menambahkan satu suara pada kandidat tersebut.
f. Setelah semua suara diterima, CTF mempublikasikan keluaran seperti daftar nomor identifikasi dan untuk siapa suara tersebut diberikan.

Skema pemilihan dengan komunikasi *Two Central Facilities* dapat dilihat pada Gambar 1.



Gambar 1. Skema pemilihan *Two Central Facilities*

Pada sistem ini setiap pemilih dapat melihat daftar nomor identifikasi dan mencari nomor miliknya untuk membuktikan bahwa pilihannya telah dihitung. Tentu saja semua pesan yang keluar/masuk telah dienkripsi dan ditandatangani untuk menghindari peniruan terhadap identitas orang lain atau menghindari adanya penangkapan transmisi.

CTF tidak dapat memodifikasi suara karena setiap pemilih akan melihat nomor identifikasi yang dimilikinya. Jika seseorang pemilih tidak berhasil menemukan nomor identifikasinya, atau ditemukan nomor identifikasi pada kandidat yang tidak dipilih, pemilih akan menyadari bahwa telah terjadi kecurangan. CTF tidak dapat memanipulasi kotak perhitungan suara karena kegiatan tersebut berada

dalam pengawasan CLA. CLA mengetahui berapa banyak pemilih yang telah terdaftar dan nomor validasinya, dan akan mendeteksi jika terdapat modifikasi.

CLA dapat menyatakan pemilih yang tidak memiliki hak pilih.CLA juga dapat mengawasi pemilih yang melakukan kecurangan seperti memilih lebih dari satu kali. Hal ini dapat diantisipasi dengan cara menerbitkan daftar pemilih yang telah disertifikasi. Jika nomor pemilih dalam daftar tidak sama dengan jumlah suara, maka dicurigai telah terjadi kesalahan atau kecurangan. Sebaliknya jika jumlah peserta yang ada pada daftar lebih banyak dari hasil tabulasi artinya beberapa pemilih tidak menggunakan hak suaranya (Fadhliy, Wardhani, dan Nuras, 2009).

2.5 Central Legitimization Agency (CLA)

Central Legitimization Agency (CLA) merupakan bagian yang bertugas untuk melakukan sertifikasi pemilih.Fungsi utama dari CLA adalah untuk melakukan otentikasi dan otorisasi pemilih. Setiap pemilih akan mengirim sebuah pesan aman kepada CLA untuk meminta sebuah *ValidationID*. CLA akan membangkitkan sebuah *ValidationID*, mendaftarkannya secara aman kepada CTF, dan mengembalikannya secara aman kepada pemilih. *ValidationID* bernilai sangat kompleks sehingga secara komputasi tidak memungkinkan seorang penyerang untuk memproduksi sebuah ID yang valid.CLA memiliki daftar sejumlah *ValidationID* yang valid serta daftar identifikasi pemilih dari setiap *ValidationID* dalam rangka untuk mencegah pemilih menerima lebih dari satu *ValidationID* dan melakukan pemilihan lebih dari satu kali (DuFeu dan Harris, 2001).

2.6 Central Tabulating Facility

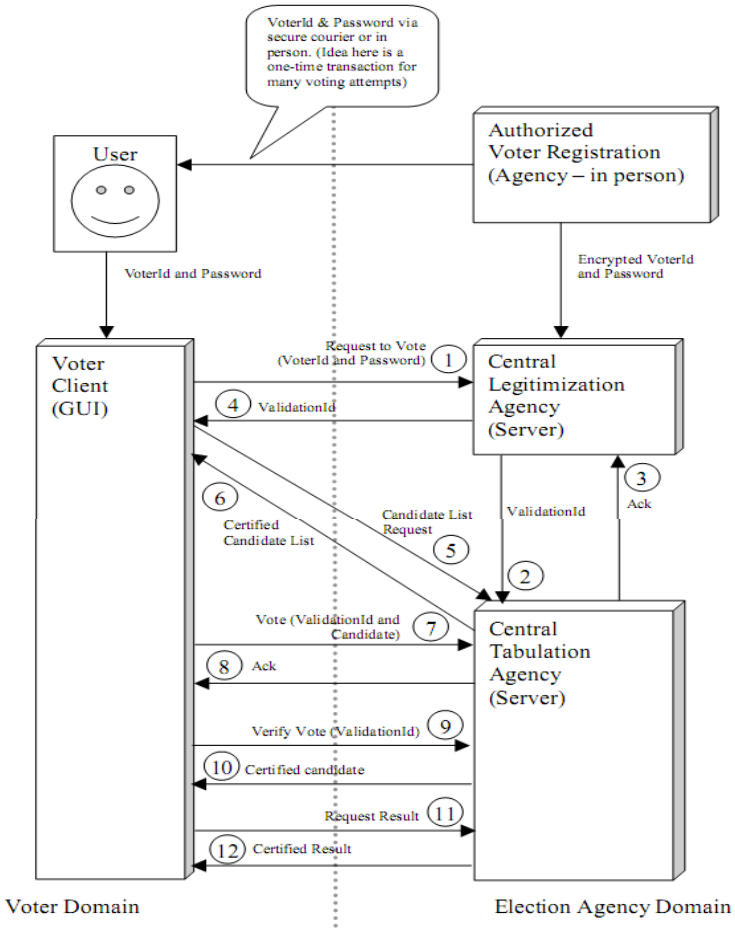
Central Tabulating Facility (CTF) merupakan bagian yang bertugas untuk melakukan perhitungan suara dan berfungsi sebagai berikut :

- Mengizinkan pemilih meminta sertifikasi daftar kandidat.
- Menerima *secure ValidationID* yang telah disertifikasi dan ditandatangani dari CLA.
- Menerima *secure vote* dari pemilih yang berwenang/sah (dengan *ValidationID*).
- Secara aman meminta kembali surat suara kandidat terpilih dari pemilik suara yang berwenang untuk verifikasi.
- Mengizinkan pemilih untuk meminta sertifikasi hasil pemilihan.

Dalam rangka otorisasi pemilih, CTF melakukan pengecekan *ValidationID* terhadap daftar yang telah diterima dari CLA.Jika *ValidationID* adalah valid, CTF memberi tanda (untuk mencegah dari perubahan pemilihan) dan menetapkan pemilihannya kepada kandidat yang telah dipilih, suara pemilih diamsukkan ke dalam kotak suara.Sebagaimana suatu desain dari sebuah sistem (untuk tujuan demonstrasi), CTF dapat memproduksi sertifikasi hasil pemilihan setiap saat (DuFeu dan Harris, 2001).

3.ANALISA DAN PEMBAHASAN

Gambar 2 berikut merupakan gambaran diagram komponen-komponen dan data flow dari sistem pemilu online.



Gambar 2. Diagram komponen dan data flow system pemilu online

1) *Voter* meminta *ValidationID* dari CLA.
   a. *Voter* memulai koneksi dengan mesin yang mengasumsikan sebagai CLA.
   b. CLA segera mengirim kunci publik dan sertifikat.
   c. *Voter* membaca kunci publik dari CLA dan memverifikasi sertifikat menggunakan kunci publik CA.
   d. *Voter* membangkitkan kunci simetrik dan mengenkripsi dengan kunci publik CLA kemudian mengirimkannya ke CLA. *Voter* kemudian mengirimkan *login* (*VoterID, password,* dan kunci publik) pada CLA menggunakan chiper simetrik.
   e. CLA mendeskripsi kunci simetrik menggunakan kunci privat dan mendeskripsi *login* menggunakan kunci simetrik.
   f. CLA membangkitkan *ValidationID.*

2) CLA meminta untuk menambahkan *ValidationID* yang sah kepada CTF.
   a. CLA memulai koneksi dengan mesin yang mengasumsikan sebagai CTF.
   b. CTF segera mengirim kunci publik dan sertifikat.
   c. CLAmembaca kunci publik dari CTF dan memverifikasi sertifikat menggunakan kunci publik CA.
   d. CLAmembangkitkan kunci simetrik dan mengenkripsi dengan kunci publik CTF kemudian mengirimkannya ke CTF. CLAkemudian mengirimkan permintaan (kunci public, sertifikat,

ValidationID) pada CTF menggunakan chipersimetrik. CLA kemudian mengirimkan tanda tangan dari permintaan kepada CTF.

e. CTF mendeskripsi kunci simetrik menggunakan kunci privat dan mendeskripsi permintaan dengan kunci simetrik. Sebelum menambahkan *ValidationID* pada badan yang sah, CTF memastikan bahwa CLA benar-benar telah mengirim pesan dengan :
   - Memverifikasi kunci publik CLA dengan sertifikat menggunakan kunci publik CA. Hal ini menjamin bahwa hanya CLA yang sebenarnya mengetahuim kunci privat untuk menandatangani pesan.
   - CTF memeriksa tanda tangan yang dikirim oleh CLA menggunakan kunci publik CLA bersertifikat.

f. Jika tanda tangan sesuai, maka *ValidationID*akan ditambahkan ke sistem.

3) CTF mengembalikan *ValidationID* baru yang sah ke CLA.
   a. Menggunakan chiper simetrik dan kunci yang telah ditetapkan sebelumnya pada step 2, CTF mengenkripsinya dengan sebuah pengakuan "OK" untuk CLA. CLA juga menandatangani pesan. Dalam kasus kesalahan, respon ("ERROR", ErrorMessage) akan dikirim kembali ke CTF.
   b. CLA memverifikasi respon sebelum mengembalikan *ValidationID* ke *Voter*. Sebelumnya telah menerima kunci publik CTF dan sertifikat pada step 2.

4) CLA mengembalikan *ValidationID* ke *Voter*.
   a. Menggunakan chiper simetrik dan kunci yang telah ditetapkan sebelumnya pada step 1, CLA mengenkripsinya dengan sebuah pengakuan "NEW" atau "REPEAT" bersama dengan pemilihan *ValidationID* kembali ke *Voter*. CLA juga menandatangani pesan. Dalam kasus kesalahan, respon yang dienkripsi ("ERROR", ErrorMessage) akan dikirim kembali ke *Voter*.
   b. *Voter* memverifikasi respon sebelum meminta daftar kandidat dari CTF. Sebelumnya telah menerima kunci publik CLA dan sertifikat pada step 1.

5) *Voter* meminta daftar kandidat dari CTF.
   a. *Voter* memulai koneksi dengan mesin mengasumsikan sebagai CTF.
   b. CTF segera mengirim kunci publik dan sertifikat.
   c. *Voter* membaca kunci publik dari CTF dan memverifikasi sertifikat menggunakan kunci publik CA.
   d. *Voter* membangkitkan kunci simetrik dan mengenkripsi kunci publik CTF dan mengirimkannya ke CTF.*Voter* kemudian mengirimkan permintaan dari "LIST" kepada CTF menggunakan chiper simetrik.
   e. CTF mendeskripsi kunci simetrik menggunakan kunci privat dan mendeskripsi permintaan dengan kunci simetrik. Untuk daftar kandidat, otentikasi tidak diperlukan dari pengguna.

6) CTF mengembalikan daftar kandidat ke *Voter*.
   a. Menggunakan kunci simetrik yang dikembangkan pada step 5, CTF mengenkripsi daftar kandidat dan mengirimkannya ke *voter*. CTF kemudian menandatangani daftar kandidat dan mengirimkan ke *voter*.
   b. *Voter* mendeskripsi daftar kandidat dan memverifikasi tanda tanga dari CTF. Sebelumnnya telah menerima kunci publik CTF dan sertifikat pada step 5.

7) *Voter* meminta untuk memilih pada CTF.
   a. *Voter* memulai koneksi dengan mesin mengasumsikan sebagai CTF.
   b. CTF segera mengirim kunci publik dan sertifikat.
   c. *Voter* membaca kunci publik dari CTF dan memverifikasi sertifikat menggunakan kunci publik CA.
   d. *Voter* membangkitkan kunci simetrik dan mengenkripsi kunci publik CTF dan mengirimkannya ke CTF. *Voter* kemudian mengirimkan permintaan memilih yang terdiri dari ("*VOTE*", *ValidationId*, kandidat) kepada CTF menggunakan chiper simetrik.

e. CTF mendeskripsi kunci simetrik menggunakan kunci privat dan mendeskripsi permintaan dengan kunci simetrik.
f. Sebelum pemungutan suara dilakukan, CTF memverifikasi bahwa *ValidationID* berada dalam system, tetapi belum digunakan dan kandidat ada. Setelahnya, CTF mencatat pemilihan dan mengembalikan konfirmasi kandidat kepada *voter*.

8) CTF mengembalikan pemilihan yang sah kepada *voter*.
   a. Menggunakan kunci simetrik yang dikembangkan pada step 7, CTF mengenkripsi dengan sebuah pengesahan ("OK") dan mengirimkannya ke *voter*. Dalam hal kesalahan, respon dienkripsi menjadi ("ERROR", ErrorMessage). CTF kemudian menandatangani pesan dan mengerimkan ke *voter*.
   b. *Voter* mendeskripsi hasil pemilihan dan memverifikasi tanda tangan dari CTF. Sebelumnya telah menerima kunci publik CTF dan sertifikat pada step 7.

9) *Voter* meminta untuk memverifikasi pemilihannya.
   a. *Voter* memulai koneksi dengan mesin mengasumsikan sebagai CTF.
   b. CTF segera mengirim kunci publik dan sertifikat.
   c. *Voter* membaca kunci publik dari CTF dan memverifikasi sertifikat menggunakan kunci publik CA.
   d. *Voter* membangkitkan kunci simetrik dan mengenkripsi kunci publik CTF dan mengirimkannya ke CTF. *Voter* kemudian mengirimkan konfirmasi permintaan yang terdiri dari ("*CHECK*", *ValidationId*) kepada CTF menggunakan chiper simetrik.
   e. CTF mendeskripsi kunci simetrik menggunakan kunci privat dan mendeskripsi permintaan dengan kunci simetrik.
   g. CTF memverifikasi bahwa *ValidationID* berada dalam sistem dan dapat digunakan. CTF mengembalikan konfirmasi kandidat kepada *voter*.

10) CTF mengembalikan status verifikasi pemilihan dan kandidat terpilih kepada *voter*.
   a. Menggunakan kunci simetrik yang dikembangkan pada step 9, CTF mengenkripsi dengan sebuah pengesahan ("OK", suara kandidat) dan mengirimkannya ke *voter*. Dalam hal kesalahan, respon dienkripsi menjadi ("ERROR", ErrorMessage). CTF kemudian menandatangani pesan dan mengerimkan ke *voter*.
   b. *Voter* mendeskripsi hasil pemilihan dan memverifikasi tanda tangan dari CTF. Sebelumnya telah menerima kunci publik CTF dan sertifikat pada step 9.

11) *Voter* meminta hasil pemilihan dari CTF.
   a. *Voter* memulai koneksi dengan mesin mengasumsikan sebagai CTF.
   b. CTF segera mengirim kunci publik dan sertifikat.
   c. *Voter* membaca kunci publik dari CTF dan memverifikasi sertifikat menggunakan kunci publik CA.
   d. *Voter* membangkitkan kunci simetrik dan mengenkripsi kunci publik CTF dan mengirimkannya ke CTF. *Voter* kemudian mengirimkan permintaan dari "*RESULT*" kepada CTF menggunakan chiper simetrik.
   e. CTF mendeskripsi kunci simetrik menggunakan kunci privat dan mendeskripsi permintaan dengan kunci simetrik.

12) CTF mengembalikan hasil pemilihan.
   a. Menggunakan kunci simetrik yang dikembangkan pada step 11, CTF mengenkripsi hasil pemilihan dan mengirimkannya ke *voter*. CTF kemudian menandatangani hasil dan mengerimkan ke *voter*.
   b. *Voter* mendeskripsi hasil pemilihan dan memverifikasi tanda tangan dari CTF. Sebelumnya telah menerima kunci publik CTF dan sertifikat pada step 11.

1. KESIMPULAN

Pemilihan umum secara online dirancang tidak hanya untuk membuat nyaman bagi orang untuk memilih, tetapi juga efisien terhadap waktu dan biaya dibanding dengan memberikan suara berbasis kertas (secara konvensional). Dengan kemajuandan perkembangan teknologi yang menakjubkan saat ini, dapat membuat *online e-voting* memungkinkan untuk diimplementasikan.Namun demikian, skema *e-voting* ini tidak akan pernahdigunakanjika tidak dapat menjaga privasi individu dan mencegah terhadap kecurangan.

Sistem *e-voting* secara online yang dibuat harus memenuhi standar *secure voting reguirements* untuk dapat mengatasi dan menjamin keamanan setiap ancaman yang akan terjadi. Protokol *Two Central Facilities Protocol* merupakan protokol yang dapat memenuhi sebagian standar kriteria *secure voting reguirements* dan memiliki tingkat keamanan yang cukup baik, dimana terdiri dari CLA untuk pengesahan pemilih dan CTF untuk perhitungan suara.

Daftar Pustaka

Bishop M. 2003. *Computer Security : Art and Science*, Boston : Addison-Wesley, Pearson Educaation, Inc.

DuFeu D, Harris J. 2001. *Online Election System*, 95.413 Project Report, Carleton University.

Fadhliy B. 2009. *Analisis dan Pengembangan Sistem Tabulasi CTF Berbasis Protokol Two Central Facilities*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.

Guritman S. 2003. *Handout Mata Kuliah Pengantar Kriptografi*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.

Hardhienata, Medria Kusuma Dewi. 2009. *Pengembangan Sistem Pengiriman Suara Voter Menuju Central Tabulating Facility (CTF)*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.

Munir R. 2004. *Bahan Kuliah Protokol Kriptografi*, Departemen Teknik Informatika, Institut Teknologi Bandung, Bandung.

Neyman SN. 2007. *Perancangan Protokol Penyembunyian Informasi Terotentikasi*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.

Nuras HF. 2009. *Analisis dan Pengembangan GUI dan Protokol Kriptografi Voter CLA Berbasis Two Central Facilities Protocol*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.

Schneier B. 1996. *Applied Cryptography*, second edition : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc.

Sireesha J, Chakchai SI. 2005. *Secure Virtual Election Both with Two Central Facilities*, Department of Komputer Science Washington University in St. Louis, USA.

Stallings W. 2011.*Network Security Essentials : Applicatiuons and Standard*, Fourth Edition, Prentice Hall, Pearson Education, Inc.

Wardhani CE. 2009. *Analisis dan Pengembangan IPB Online Voting Berbasis Protokol Two Central Facilities*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.