DESAIN *E-VOTING* PILKADA KOTA BOGOR MENGGUNAKAN PROTOKOL *TWO CENTRAL FACILITIES* YANG DIMODIFIKASI

Fitrah Satrya Fajar Kusumah, Sugi Guritman, Endang Purnama Giri
Unversitas Ibn Khaldun Bogor
Jln. K.H Sholeh Iskandar Km. 2 Bogor
fitrah.satry@gmail.com, guritman@gmail.com, epgthebest@yahoo.com

Abstract-One of Indonesian election is the local elections for regional head that are still using conventional election type. The conventional election type still spend a lot of time and prone of mistakes made by humans, including frauds committed by certain parties. This research is based on two central facilities protocol in Schneier book (1996) and a continuation of previous research by Sireesha and Chakchai (2005) which has developed a secure election with two central facilities protocol that implement the development of Central Legitimization Agency (CLA) and the Central Tabulating Facilities (CTF) to create a secure virtual elections and Wardhani (2009) which implement the protocol Two central facilities at IPB online voting. This research collaboration with the KPU Bogor and Bogor Information and Communications, for the purposes of analyzing and studying the various elections policy of regional heads of Bogor. Through this study found a design system using a protocol e-voting Two central facilities modified. However, this design is still require further research to be applicable for Bogor Regional Head election.
Keywords: E-voting, E-voting Protocol, Voting Machine, Bogor e-voting.

I. PENDAHULUAN

A. Latar Belakang

Pemilihan Umum (Pemilu) secara harfiah, dapat dijelaskan sebagai sebuah kegiatan rutin di Indonesia yang diadakan lima tahun sekali guna memilih anggota pejabat daerah, parlemen, maupun presiden guna memilih figur yang dipercayai menduduki lembaga politik tertentu. Pemilu merupakan rangkaian sistematis dari pengembangan sistem negara yang menganut paham demokrasi. Pemilu pada negara yang memiliki jumlah penduduk yang banyak dilakukan melalui tahap *voting*. *Voting* adalah salah satu metode untuk mengambil keputusan penting dalam kehidupan manusia. *Voting* dapat digunakan mulai tingkat masyarakat kecil, yaitu keluarga hingga sampai dengan sebuah negara.

Salah satu bentuk penerapan Pemilu di Indonesia adalah pemilihan kepala daerah atau Pilkada. Pilkada umumnya masih menggunakan cara konvensional, yaitu cara coblos dan contreng pada lembar surat suara. Penggunaan cara

konvensional tersebut tidak jarang menghabiskan banyak waktu dan rentan terhadap kesalahan yang dilakukan oleh manusia, termasuk kecurangan-kecurangan yang dilakukan oleh pihak-pihak tertentu.

Perkembangan teknologi informasi saat ini telah membawa perubahan besar bagi manusia, termasuk cara untuk melaksanakan *voting*. Penggunaan teknologi komputer pada pelaksanaan *voting* ini lazim dikenal dengan istilah *electronic voting* atau lazim disebut *e-voting*. Teknologi *e-voting* telah menjadi isu yang hangat dibicarakan di beberapa negara maju. Hal ini disebabkan oleh kelebihan dari sistem e-*voting* dibandingkan pemilihan menggunakan kertas suara yang biasa dilakukan.

Pada tahun 2001, Dan DuFeu dan Jon Harris melakukan penelitian dengan mendeskripsikan bagaimana *online election system* bekerja. Penelitian ini mengimplementasikan pembangunan *Central Legitimization Agency* (CLA) dan *Central Tabulating Facilities* (CTF) untuk menerapkan pemilu yang aman [1]. Beberapa penelitian selanjutnya mengenai topik serupa kian terbuka lebar. Pada tahun 2005, Sireesha, Janga, dan So-In Chakchai melakukan penelitian dengan memodifikasi protokol *secure election* dengan *Two Central Facilities* [2]. Dengan lahirnya berbagai penelitian dalam bidang *election sistem*, penelitian ini diharapkan dapat terus menyempurnakan sistem *online voting* yang telah ada.

Penelitian ini merupakan penelitian berdasarkan protokol *two central facilities* [3] protokol *two cenral facilities* dengan mengimplementasikan pengembangan *Central Legitimization Agency* (CLA) dan *Central Tabulating Facilities* (CTF) untuk mewujudkan pemilu virtual yang aman dan protokol *two central facilities* juga diterapkan pada IPB *online voting* [4].

Penelitian ini bekerjasama dengan KPU Bogor dan Dinas Perhubungan, Komunikasi, dan Informatika Kota Bogor untuk menganalisis dan mempelajari berbagai keperluan pemilihan umum kepala daerah Kota Bogor, dan penyesuaian dengan protokol *two central facilities* [3].

B. Tujuan dan Manfaat Penelitian

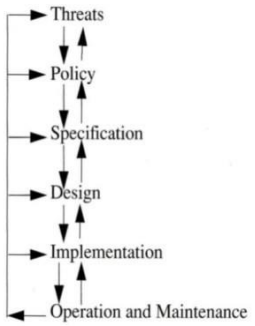
Penelitian ini bekerjasama dengan KPU Bogor dan Dinas Perhubungan, Komunikasi, dan Informatika Kota Bogor untuk menganalisis dan mempelajari berbagai keperluan pemilihan umum kepala daerah Kota Bogor, dan penyesuaian dengan protokol *two central facilities*.

II. METODOLOGI

Penelitian ini dikembangkan dengan metode *Security life cycle*. Terdapat 6 tahap utama yang diterapkan dalam *security life cycle* diantaranya [5]:

1. Ancaman (*Threats*),
2. Kebijakan (*Policy)*,
3. Spesifikasi (*Specification)*,
4. Perancangan (*Design)*,
5. Implementasi (*Implementation)*,
6. Operasi dan Pemeliharaan *(Operation and Maintenance)*.

Metode *security life cycle* dapat dilihat pada Gambar 1. Fokus peneliltian ini pada tahap (1) sampai (5)



Gambar 1 *The Security life cycle*.

III. HASIL DAN BAHASAN

A. Ancaman (*Threat*)

Sebuah sistem keamanan yang dibuat harus dipersiapkan agar mampu untuk melindungi sistem dari ancaman-ancaman yang mungkin terjadi. Pada situs yang dikembangkan, ancaman yang mungkin timbul antara lain:

1 *Modification* atau *alternation* yakni ancaman modifikasi yang mungkin terjadi dalam adalah pengubahan *Unique ID UID* dan (Nomor Induk KTP) NIK yang akan dikirimkan sistem ke pemilih serta status pemilih. Pengubahan ini mungkin dilakukan apabila *database server* CLA dapat ditembus oleh penyerang sehingga akun pemilih tidak lagi sama dan tidak dapat digunakan oleh pemilih. Pengubahan lain yang mungkin terjadi adalah terhadap konten dari situs ini sendiri. Hal ini dapat mengakibatkan penerimaan informasi yang salah oleh pengguna sistem.

2 *Snooping* yakni penangkapan informasi oleh pihak-pihak yang tidak berwenang. *Snooping* merupakan bentuk dari *disclosure*. Hal ini dapat bersifat aktif maupun pasif, bersifat pasif seperti penyadapan komunikasi dan bersifat aktif apabila pencarian informasi melalui sebuah berkas atau sistem. Ancaman yang mungkin terjadi adalah penyadapan komunikasi yang terjadi saat proses registrasi sehingga data yang dikirimkan pemilih dapat diketahui oleh pihak yang tidak berwenang.

3 Penyamaran (*masquering*) yakni peniruan terhadap suatu entitas terhadap entitas yang lain. Contohnya

yaitu saat pemilih akan mengirimkan kunci simetri kepada CLA atau CTF untuk melakukan komunikasi, pihak yang menerima kunci tersebut bukanlah CLA atau CTF yang resmi melainkan *server* lain yang mengaku sebagai CTF. Untuk menangani ancaman ini konsep otentifikasi (*authentication*) dapat digunakan untuk mencegah serangan. *Masquerading* termasuk ancaman dalam kelas *deception* dan *usurpation*. Pada komunikasi data sendiri perubahan dapat terjadi apabila penyerang dapat bertindak sebagai *man in the middle* diantara saat terjadi proses pertukaran data pada mesin *voting*, CTF, dan CLA.

4 *Disruption*, yakni penyerangan terhadap sistem untuk melemahkan sumberdaya sistem tersebut sehingga tidak dapat diakses atau sistem mengalami *crash*. Penyerangan ini dapat dilakukan melalui serangan *denial of service* (*DoS*) dengan mengeksploitasi kelemahan yang terdapat di dalam protokol TCP.

5 *Usurpation*, yakni pengaturan beberapa bagian dari sistem. Hal ini dapat dilakukan dengan cara merubah kode program agar terjadi kecurangan pada *e-voting*. Hal ini dapat dilakukan oleh orang luar ataupun orang dalam yang dapat mengakses *source code* dari program.

B. Kebijakan (*Policy*)

Secure voting yang dibangun secara komputerisasi akan digunakan jika terdapat protokol yang menjamin [3]:

1 Privasi individu.
2 Pencegahan terhadap kecurangan.

Suatu protokol *secure election* yang ideal harus memiliki 6 persyaratan sebagai berikut:

1 Hanya pemilih yang berhak yang dapat memberikan suara (otentifikasi).
2 Tidak boleh memberikan lebih dari satu suara.
3 Tidak boleh menentukan orang lain harus memilih untuk siapa.
4 Tidak ada yang bisa menduplikasi suara orang lain.
5 Tidak boleh mengubah pilihan orang lain.
6 Setiap pemilih dapat memastikan bahwa suara mereka sudah dikirimkan dan terhitung dalam penghitungan akhir.

Sebagai bagian awal dari *electronic voting*, sistem yang dibangun haruslah memenuhi sebagian dari persyaratan di atas. Persyaratan tersebut diantaranya:

1 Hanya pemilih yang berhak yang dapat memberikan suara. Status UID dan NIK pada *database* CLA yang

menjadi bukti bahwa orang tersebut merupakan pemilih yang sah dan dapat memberikan suaranya.

2 Tidak boleh memberikan lebih dari satu suara. Hal ini dapat pula diartikan pencegahan pemilih ganda. Pemilih ganda dapat dicegah jika terlebih dahulu dilakukan pengecekan apakah seseorang yang mendaftar sebagai pemilih sudah pernah mendaftarkan dirinya. Pengecekan ini dapat dilakukan pada UID dan NIK pemilih pada *server* CLA.

3 Setiap pemilih dapat memastikan bahwa suara mereka terhitung dalam perhitungan akhir. Menurut Undang (2011), diperlukan adanya tiga bentuk bukti pemilihan suara, yaitu:

- Bukti hasil pemilihan elektronik yang terakumulasi pada CTF,
- Bukti hasil pemilihan elektronik yang terdapat pada tiap-tiap mesin *voting*, dan
- Bukti fisik pemilih yang terdapat pada setiap mesin *voting* yang dapat dijadikan bukti apabila bukti hasil pemilihan elektronik suara tidak diterima.

4 Hanya komputer-komputer *server* dan mesin *voting* yang telah ditetapkan yang dapat mengakses sistem *e-voting*.

C. Spesifikasi (*Spesification*)

Sistem ini terdiri dari tiga entitas yaitu mesin *voting*, *server* CLA, dan *server* CTF. Pemilihan dilakukan pada mesin *voting*, pemeriksaan hak pemilih dilakukan pada CLA, dan proses penghitungan suara dilakukan pada mesin CTF. Sistem hanya dapat bekerja melalui entitas yang telah ditetapkan sebelumnya.

CTF maupun CLA harus dapat diakses oleh setiap mesin *voting* sehingga pemakaian *database*nya dapat dilakukan secara terpusat. Sistem yang dibangun diharapkan dapat terjamin keamanannya dan kerahasiaannya untuk memenuhi ketentuan pemilihan.

Secara umum, sistem yang dibangun haruslah memberikan jaminan bahwa informasi yang diakses pengguna tidak diganggu oleh pihak-pihak yang tidak berwenang dalam mengakses sistem, namun tetap mempertimbangkan sisi kecepatan pertukaran data, oleh karena itu digunakan jalur komunikasi VPN PPTP. Pengiriman data dalam setiap proses, misalnya registrasi juga haruslah terjamin keamanannya sehingga diperlukan pengenkripsian data sebelum pengiriman dilakukan.

D. Perancangan (*Design*)

Perancangan sistem yang dibangun terbagi menjadi dua bagian, yakni

perancangan sistem secara umum yang membahas keseluruhan sistem yang dibangun menggunakan protokol *two central facilities* yang dimodifikasi. Perancangan selanjutnya adalah perancangan secara khusus yang akan membahas perancangan alur *voting* dan pengamanan jaringan sistem *e-voting*. Perancangan otentifikasi pemilih pada *server* CLA dan proses pengiriman suara melalui *server* CTF masing-masing dilakukan oleh dua rekan penulis yaitu Alfian Prayanta dan Erick Prianggodo.

Modifikasi *two central facilities* ini bertujuan untuk menyesuaikan protokol *two central facilities* [3] dengan kebijakan-kebijakan yang didapatkan dari KPU kota Bogor, membuat protokol ini menjadi lebih efisien, dan lebih aman protokol dari *two central facilities* sebelumnya. Protokol *two central facilities* yang dimodifikasi ini memiliki empat lembaga penyelenggara pemilu yang diimplementasikan dalam dua *server* yang berbeda, yaitu mesin *voting*, dan pemilih seperti yang tergambar pada Gambar 3.

Server pertama yakni *Central Legitimization Agency* (CLA) merupakan badan sertifikasi pemilih yang memiliki tugas utama mengAutentikasi dan mengotorisasi pemilih. CLA mempunyai pangkalan data yang menyimpan data pemilih baik data diri maupun *ID* (*UID* dan NIK) pemilih. Pangkalan data ini tidak dapat diperlihatkan pada pihak lain, sekalipun CTF. Setiap proses yang membutuhkan data pemilih, contohnya *login* dan verifikasi pilihan, harus melakukan pengecekan langsung dengan CLA melalui mesin *voting*.

Server kedua yakni *Central Tabulating Facilities* (CTF) merupakan badan tabulasi/penghitungan suara. Pangkalan data yang terdapat pada CTF berisi suara atau pilihan pemilih dan perhitungannya untuk masing-masing kandidat.

a)* Skema *E-voting

Alur kerja *online voting* berdasarkan Gambar 3 tersebut terbagi menjadi empat tahapan dengan penjelasan sebagai berikut:

Tahap 1

1 Pengiriman kunci publik oleh masing-masing mesin *voting* kepada CLA.
2 CLA mengirimkan kunci simetri yang telah dienkripsi menggunakan kunci publik yang diterima dari masing-masing mesin *voting* dan diberikan kepada masing-masing mesin *voting* sesuai alamat IP *address* masing-masing mesin *voting*.

Tahap 2

1 Pemilih mengirimkan permintaan untuk memilih melalui mesin *voting* dengan cara menempelkan kartu identitasnya.
2 Mesin *voting* akan mengirimkan data kartu identitas pemilih yang telah dienkripsi kepada CLA.
3 CLA akan melakukan proses dekripsi terhadap data yang diterima.
4 CLA akan melakukan autentikasi pemilih dengan *database*.
5 Apabila pemilih dinyatakan berhak memilih dengan ketentuan pemilih telah terdaftar di *database* dan belum memilih sebelumnya, pemilih akan diarahkan kepada halaman pemilihan dan status pemilih akan diubah menjadi status telah melakukan autentikasi. Namun, apabila pemilih dinyatakan tidak berhak memilih, pemilih langsung diarahkan ke halaman gagal memilih.
6 Setelah pemilih melakukan pemilihan, pilihan pemilih akan disimpan pada mesin *voting* dan status pemilih akan diubah menjadi status telah melakukan pemilihan. Mesin akan terus menerus melakukan proses yang sama sampai pada waktu pemilihan usai.

Tahap 3

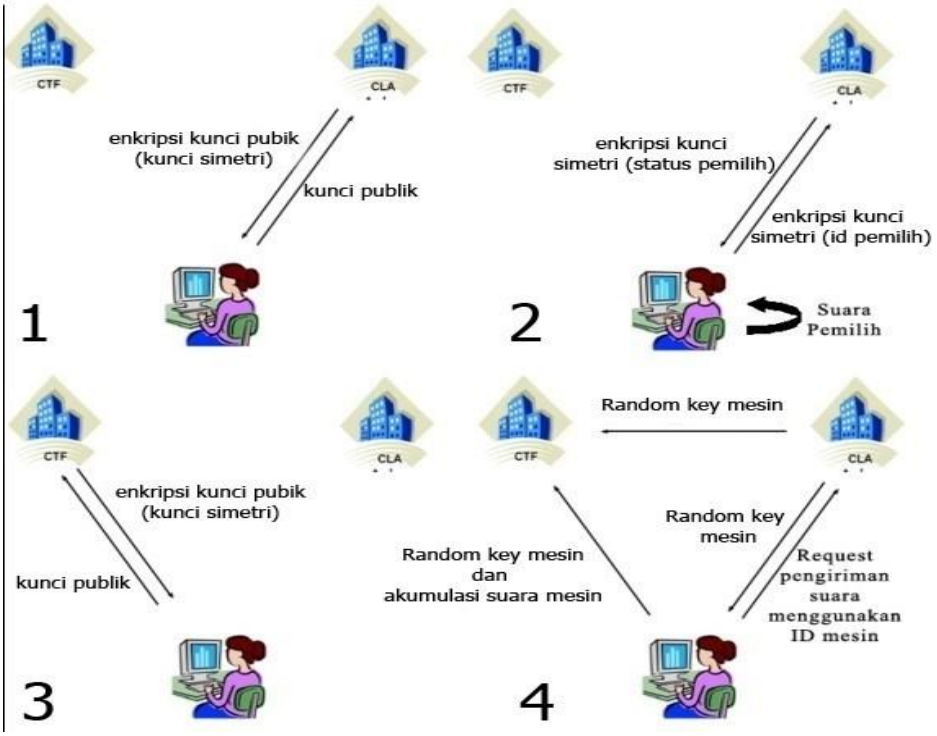
1 Pengiriman kunci publik oleh masing masing mesin *voting* kepada CTF.
2 CTF mengirimkan kunci simetri yang telah dienkripsi menggunakan kunci publik yang diterima dari tiap-tiap mesin dan dikirimkan kepada masing-masing mesin sesuai alamat IP *address* mesin.

Tahap 4

1 Mesin secara periodik akan melakukan permintaan kepada CLA untuk mengirimkan data ke CTF dengan mengirimkan informasi identitas mesin yang dienkripsi.
2 CLA akan melakukan proses autentikasi dan mengirimkan suatu *random key* mesin kepada mesin *voting* dan CTF yang dienkripsi.
3 Mesin *voting* akan mengirimkan identitas mesin, data hasil pemilihan, dan juga nilai *random* kepada CTF yang didapatkan dari CLA yang telah dienkripsi.
4 CTF melakukan pencocokan nilai *random key* yang diberikan mesin dengan *random key* yang diterima dari CLA untuk mesin tersebut.
5 Jika sah, CTF akan melakukan pengecekan data yang dikirim dari masing-masing mesin *voting*.

6 Apabila *random key* yang dikirimkan mesin dan CLA sesuai, jumlah suara yang diberikan mesin kepada CTF akan disimpan ke dalam CTF.
7 Mesin akan terus menerus melakukan proses yang sama sampai pada waktu pemilihan usai.

Proses pemilihan dengan *two central facilities* yang dimodifikasi ini memisahkan waktu pengiriman *ID* pemilih dari mesin ke CLA dan suara pemilih ke CTF.



Gambar 1 Skema Pemilihan dengan *Two Central Facilities* Dimodifikasi.

Kelebihan dari protokol *two central facilities* yang dimodifikasi ialah penggunaan jalur komunikasi untuk autentikasi pemilih pada CLA tidak akan terganggu oleh data yang dikirimkan ke CTF, sebab waktu pengirimannya yang berbeda.

Pemisahan waktu pengiriman mempermudah penyelenggara untuk mengecek kecurangan yang terjadi pada mesin CTF. Sebab suara pemilih akan dikirimkan pada waktu yang *random* ke CTF setelah waktu pemilihan selesai, sehingga apabila sebelum waktu pemilihan selesai pada CTF telah ditemukan suara pemilih dari mesin *voting* dapat dipastikan suara tersebut bukanlah suara yang sah.

Sistem ini tidak memenuhi salah satu kriteria *secure election* yang ideal [3]),

yaitu setiap pemilih dapat memastikan bahwa suara mereka sudah dikirimkan dan terhitung dalam penghitungan akhir sebab suara yang dikirimkan ke CTF bukanlah suara yang dikirimkan secara langsung oleh pemilih, melainkan suara yang diakumulasi terlebih dahulu pada mesin *voting*. Tidak ada seorang pun yang dapat mengetahui pemilih dan pilihan yang dipilihnya. Namun, di sisi lain, hal ini menjadi salah satu kekuatan dari sistem ini, sebab tidak akan dimungkinkan terjadi penelusuran ke belakang oleh pihak-pihak manapun yang mampu mengumpulkan *database* dari CLA, CTF, dan mesin *voting.*

Dari penerapan *e-voting* yang dilakukan KPU Bogor untuk pemilihan RW II Kelurahan Cipaku, didapatkan sebuah hasil perhitungan pemilih melakukan *voting* dalam waktu rata-rata satu menit untuk tiap pemilih. Asumsi yang digunakan yaitu waktu untuk melakukan pemilihan dilakukan selama 7 jam atau 420 menit. Dengan kata lain satu mesin *voting* dapat digunakan oleh 420 pemilih.

b) Tahapan-tahapan pemilihan

Terdapat beberapa tahapan pemilihan dalam *e-voting* ini yang berfungsi untuk mengarahkan pemilih dalam proses pemilihan. Tahapan-tahapan tersebut antara lain:

1. Tahap pemilihan surat suara

Pada tahapan ini pemilih diberikan waktu 20 detik untuk memilih calon kandidat yang tersedia. Kesempatan untuk memilih calon kandidat diberikan sebanyak-banyaknya dua kali kesempatan. Apabila pemilih tidak memanfaatkan kedua kesempatan tersebut, pemilih akan dinyatakan abstain.

2. Tahapan perpanjangan waktu

Perpanjangan waktu diberikan kepada pemilih yang belum sempat memilih pada kesempatan pertama. Pemilih diberikan 10 detik untuk memberikan keputusannya apakah ia akan memilih atau tidak. Jika pemilih memutuskan tidak, suara akan dinyatakan abstain. Namun, jika memutuskan memilih perpanjangan waktu, pemilih akan dihadapkan kembali dengan halaman surat suara.

3. Tahapan menanyakan keyakinan pemilih

Pemilih akan ditanyakan tentang keyakinannya akan kandidat yang akan dipilihnya dalam waktu 10 detik. Apabila pemilih yakin akan pilihannya, pilihannya akan segera disimpan di dalam *database* mesin *voting*. Namun, apabila tidak yakin pemilih diberikan satu kesempatan lagi untuk menentukan

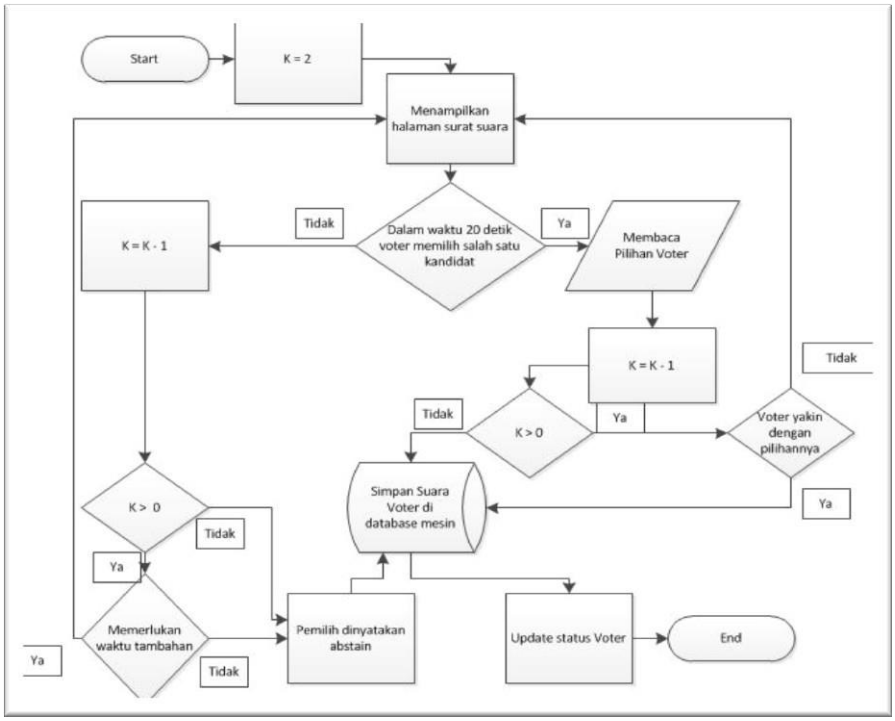
pilihannya melalui halaman surat suara. Pemilih yang tidak melakukan apa pun dalam waktu 10 detik dinyatakan yakin akan pilihannya.

4. Tahapan bukti suara elektronik

Pemilih yang telah memilih salah satu kandidat dan yakin ataupun pemilih yang dinyatakan abstain dengan pilihannya akan diarahkan pada halaman bukti suara elektronik pada mesin *voting*. Bukti suara ini hanyalah sebuah halaman yang menunjukkan pemilih telah memilih kandidat yang dipilihnya, yang diwakili dengan nomor kandidat yang dipilih.

c) *Flowchart* Pemilihan

Diagram alir Proses pemilihan pemilih digambarkan pada Gambar 4.



Gambar 4 Flowchart Proses Pemilihan Kandidat

Proses pemungutan suara dilakukan dengan ketentuan-ketentuan yang telah didiskusikan sebelumnya dengan pakar. Untuk mencegah hal-hal yang tidak diinginkan, waktu pemilihan tetap harus dibatasi dengan pembatasan satu menit untuk setiap pemilih. Berikut langkah-langkah pemungutan suara sebagai berikut seperti:

Kasus satu

Pemilih melakukan pilihan dan yakin akan pilihannya.

1 Inisialisasi batas kredit pemilih dengan nilai dua.
2 Mesin menampilkan halaman surat suara.
3 Dalam waktu 20 detik pemilih harus menentukan pilihan.
4 Jika pemilih telah menentukan pilihan, pemilih akan ditanyakan tentang keyakinannya memilih kandidat tersebut.
5 Kredit pemilih dikurangi satu.
6 Jika pemilih telah yakin akan pilihannya, sistem akan menyimpan pilihan pemilih.

Kasus dua

Pemilih melakukan pilihan dan tidak yakin akan pilihannya, lalu kembali memilih.

1 Inisialisasi batas kredit pemilih dengan nilai dua.
2 Mesin menampilkan halaman surat suara.
3 Dalam waktu 20 detik pemilih harus menentukan pilihan.
4 Jika pemilih telah menentukan pilihan, pemilih akan ditanyakan tentang keyakinannya memilih kandidat tersebut.
5 Kredit pemilih dikurangi satu.
6 Jika pemilih tidak yakin akan pilihannya, sistem akan mengarahkan pemilih untuk memilih satu kali lagi kandidat yang ingin dipilih.
7 Pemilih menentukan pilihan.
8 Sistem akan langsung memasukkan pilihan terakhir pemilih ke *database* tanpa menanyakan keyakinannya terlebih dahulu.

Kasus tiga

Pemilih tidak menentukan pilihan selama 20 detik. Namun menentukan pilihan pada kesempatan berikutnya.

1. Inisialisasi batas kredit pemilih dengan nilai dua.
2. Mesin menampilkan halaman surat suara.
3. Dalam waktu 20 detik, pemilih harus menentukan pilihan.
4. Jika pemilih tidak memilih selama 20 detik, pemilih akan ditanyakan apakah memerlukan waktu tambahan.
5. Kredit pemilih dikurangi satu.

6. Jika pemilih memerlukan waktu tambahan, pemilih akan kembali dihadapkan pada halaman surat suara.
7. Pemilih menentukan pilihan
8. Sistem akan langsung memasukkan pilihan terakhir pemilih ke *database* tanpa menanyakan keyakinannya terlebih dahulu.

Kasus empat

Pemilih tidak menentukan pilihan dalam waktu 20 detik dan pemilih tidak memerlukan waktu tambahan.

1 Inisialisasi batas kredit pemilih dengan nilai dua
2 Mesin menampilkan halaman surat suara.
3 Dalam waktu 20 detik pemilih harus menentukan pilihan.
4 Pemilih tidak memilih selama 20 detik dan pemilih akan ditanyakan apakah memerlukan waktu tambahan.
5 Kredit pemilih dikurangi satu.
6 Pemilih memilih untuk tidak memakai waktu tambahan dengan cara memilih tidak.
7 Sistem akan langsung memasukkan pilihan abstain pada *database* mesin.

Kasus lima

Pemilih tidak jadi memilih

1 Inisialisasi batas kredit pemilih dengan nilai dua
2 Mesin menampilkan halaman surat suara.
3 Dalam waktu 20 detik pemilih harus menentukan pilihan.
4 Jika pemilih telah menentukan pilihan, pemilih akan ditanyakan tentang keyakinannya memilih kandidat tersebut.
5 Kredit pemilih dikurangi satu.
6 Pemilih memilih untuk tidak yakin dengan pilihannya.
7 Pemilih tidak memilih pada kesempatan kedua.
8 Sistem akan langsung memasukkan pilihan abstain pada *database* mesin.

Kasus enam

Pemilih memakai waktu tambahan namun tidak tetap tidak memilih.

1 Inisialisasi batas kredit pemilih dengan nilai dua.
2 Mesin menampilkan halaman surat suara.
3 Dalam waktu 20 detik pemilih harus menentukan pilihan.
4 Pemilih tidak menentukan pilihan.
5 Pemilih memakai waktu tambahan.
6 Pemilih tetap tidak memilih.
7 Sistem akan langsung memasukkan pilihan abstain pada *database* mesin.

d) **Implementasi mesin *voting***

Idealnya mesin *voting* ialah satu perangkat komputer yang telah dirakit untuk menjadi mesin *voting.* Salah satu alternatifnya ialah mesin seperti yang

telah diterapkan sebelumnya pada *e-voting* RW 02 di kelurahan Cipaku, dengan kebijakan sebagai berikut:

a Mesin tidak menyediakan *keyboard* ataupun *mouse* selama proses *e-voting*. Hal ini dianjurkan agar interaksi antara manusia dengan mesin *voting* menjadi lebih terbatas dan untuk memperkecil kemungkinan *human error* ataupun tindakan-tindakan yang tidak diinginkan lainnya.

b Pemilih hanya berinteraksi dengan sistem *e-voting* menggunakan layar sentuh dengan *single touch screen* sehingga pemilih tidak dapat memilih dua kandidat sekaligus.

c Layar sentuh yang digunakan disarankan menggunakan layar *capasitive screen* agar pemilih dibatasi hanya dapat menggunakan anggota tubuhnya untuk memilih.

d Hasil *print out* dari surat suara pemilih di susun secara acak di dalam kotak khusus yang akan disegel oleh pihak yang berwenang.

IV. PENUTUP

Penerapan sebuah protokol harus sesuai dengan kebijakan-kebijakan yang berlaku protokol tersebut akan diterapkan agar dapat diterima dan diterapkan sesuai dengan keadaan.

Desain sistem *e-voting* menggunakan protokol *two central facilities* yang dimodifikasi untuk Pilkada Kota Bogor masih berupa rancangan dasar yang harus dikembangakan lebih lanjut agar dapat diterapkan secara langsung untuk Pilkada Kota Bogor, sebab masih banyak hal-hal yang harus dipertimbangkan untuk menyempurnakan sistem *e-voting* baik itu faktor *internal*, *eksternal* sistem maupun kebijakan yang mendasari sistem *e-voting*.

V. DAFTAR PUSTAKA

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

[2] Sireesha J, Chakchai S. 2005. *Secure Virtual Election Booth with Two Central Facilities.* Department of Computer Science Washington University, St. Louis, USA.

[3] Schneier B. 1996. *Applied Cryptography*. Ed ke-2, Jon Wiley & Sons.

[4] Wardhani EC. 2009. Analisis dan pengembangan IPB online *voting* center berbasis protokol *two central facilities* [skripsi]. Bogor: Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor

[5] Bishop M. 2003. *Computer Security Art and Science*. Pearson Education, Inc. Boston.