

RANCAN BANGUN SISTEM E-VOTING MENGGUNAKAN PROTOKOL TWO CENTRAL FACILITIES

Asep Taufik Muharram¹, Fitrah Satrya²

¹Fakultas Sains Dan Teknologi, UIN Syarif Hidayatullah Jakarta
JL. Ir. H. Juanda, No. 95, Ciputat, Jakarta - Indonesia
Telp. 021 74019 25, Fax. 749 3315
e-mail : a.taufikmuharram@uinjkt.ac.id

ABSTRACT

General election of regional head, governor or regent, in Indonesia is conducted conventionally. This kind of election is prone of human errors and also black campaigns committed by certain parties. This research aims to build an e-voting system in Tasikmalaya City using Two Central Facilities Protocol, i.e.: Central Legitimization Agency (CLA), for the approval of voters, and Central Tabulating Facility (CTF) for counting. This system is purposed to facilitate the general elections, so that the election will be run effectively and efficiently. However, there are some factors to be considered to polish the system in order to implement it in real general elections.

Keywords: *E-voting, Protocol Two Central Facilities, Tasikmalaya General Election*

ABSTRAK

Salah satu pelaksanaan pemilu di Indonesia adalah pemilu untuk kepala daerah (pilkada), yang masih menggunakan jenis pemilu konvensional. Jenis pemilu konvensional masih menghabiskan banyak waktu dan rawan kesalahan yang dibuat oleh manusia, termasuk penipuan yang dilakukan oleh pihak-pihak tertentu. Penelitian ini merupakan rancangan untuk membangun sistem e-voting pilkada Kota tasikmalaya dengan menggunakan Two Central Facilities Protocol, dimana terdiri dari Central Legitimization Agency (CLA) untuk pengesahan pemilih dan Central Tabulating Facility (CTF) untuk perhitungan suara, yang dapat mewujudkan sistem e-voting yang aman, efektif, dan efisien. Agar dapat di terapkan secara langsung untuk Pilkada Kota Tasikmalaya, masih banyak hal-hal yang harus dipertimbangkan untuk menyempurnakan sistem baik itu faktor internal maupun eksternal sistem.

Kata Kunci : *E-voting, Protocol Two Central Facilities, Pilkada Kota Tasikmalaya.*

1. PENDAHULUAN

Pemilihan umum (pemilu) merupakan bagian penting dalam sistem demokrasi Indonesia. Sejak meraih kemerdekaan 1945, Indonesia tercatat telah 11 kali menyelenggarakan pemilu yaitu pada

tahun 1955, 1971, 1977, 1982, 1987, 1992, 1997, 1999, 2004, 2009 dan 2014. Secara umum terdapat 4 aspek yang dapat diamati dari pemilu sebelumnya, yaitu sumber daya manusia, biaya, waktu, dan keamanan.

Banyak kendala dan permasalahan yang timbul pada penyelenggaraan pemilu hingga tahun 2009 yang lalu. Pada tahun 2011, diadakan dialog nasional yang diprakarsai oleh KPU yang bertemakan “Menuju Pemilu Elektronik di Indonesia” menyimpulkan beberapa masalah yang ditimbulkan pemilu konvensional.

Di Indonesia salah satu bentuk pemilu adalah pemilihan kepala daerah atau Pilkada. Pilkada umumnya masih menggunakan cara konvensional, yaitu cara coblos dan conteng pada lembar surat suara. Tidak jarang menghabiskan banyak waktu dan rentan terhadap kesalahan yang dilakukan oleh manusia, termasuk kecurangan-kecurangan yang dilakukan oleh pihak-pihak tertentu.

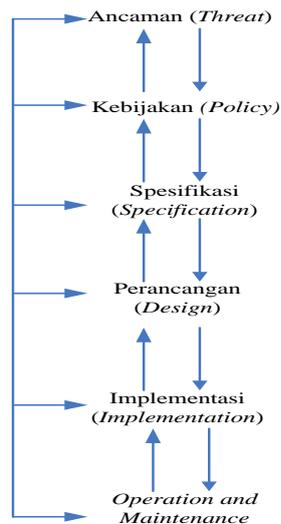
Perkembangan teknologi informasi saat ini telah membawa perubahan besar bagi manusia, termasuk cara untuk melaksanakan *voting*. Penggunaan teknologi computer pada pelaksanaan *voting* ini lazim dikenal dengan istilah *electronic voting* atau lazim disebut *e-voting*. Teknologi *e-voting* telah menjadi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

Seperti halnya dengan sistem pemilu yang diadakan secara konvensional,

pelaksanaan sistem pemilu secara *e-voting* pun pasti tidak akan terhindar dari berbagai ancaman kecurangan yang mungkin terjadi. Oleh karena itu, sistem yang dibuat harus memenuhi standar *secure voting requirements* 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 requirements* dan memiliki tingkat keamanan yang cukup baik adalah *Two Central Facilities Protocol*, dimana terdiri dari *Central Legitimization Agency* (CLA) untuk pengesahan pemilih dan *Central Tabulating Facility* (CTF) untuk perhitungan suara [1].

2. METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah metode *Security Life Cycled* [2] Berdasarkan Bishop (2003) ada 6 tahap utama yang diterapkan dalam *Security Life Cycle* diantaranya: dapat dilihat pada Gambar 1.



Gambar 1. Metode Security Life Cycle

3. HASIL DAN PEMBAHASAN

Protokol ini memiliki tiga komponen utama dalam implementasi penyelenggaraan pemilu yakni mesin *voting*, *Central legitimization Agency* (CLA), dan *Central Tabulating Facilities* (CTF). Mesin *voting* merupakan komponen yang berinteraksi langsung dengan pemilih, dimana pemilih dapat melakukan proses pemberian suara untuk kandidat yang dipilihnya. *Central Legitimization Agency* (CLA) adalah *server* pertama yang merupakan badan sertifikasi pemilih yang memiliki tugas utama mengotentikasi dan mengotorisasi pemilih, CLA mempunyai pangkalan data yang menyimpan data. Pangkalan data ini tidak dapat diperlihatkan pada pihak lain sekalipun *Central Tabulating Facilities*(CTF). Setiap proses yang membutuhkan data pemilih, contohnya

login dan verifikasi pilihan, harus melakukan pengecekan langsung dengan *Central legitimization Agency* (CLA) melalui mesin *voting*. *Central Tabulating Facilities* (CTF) adalah *server* kedua yang merupakan badan tabulasi atau penghitungan suara. Pangkalan data yang terdapat pada *Central Tabulating Facilities* (CTF) berisi suara atau pilihan pemilih dan perhitungannya untuk masing-masing kandidat.

3.1 Ancaman (Threats)

Sebuah sistem e-voting yang dibuat harus dipersiapkan agar mampu untuk melindungi sistem dari ancaman-ancaman yang mungkin terjadi. Ancaman yang mungkin timbul antara lain:

1. *Modification or alternation* Ancaman modifikasi yang mungkin terjadi dalam adalah perubahan UID dan NIK yang akan dikirimkan sistem ke pemilih serta status pemilih. Perubahan ini mungkin dilakukan apabila database server CLA dapat ditembus oleh penyerang sehingga akun pemilih tidak lagi sama dan tidak dapat digunakan oleh pemilih. Perubahan lain yang mungkin terjadi adalah terhadap konten dari situs ini sendiri. Hal ini dapat mengakibatkan penerimaan informasi yang salah oleh pengguna sistem. *Snooping* yakni

penangkapan informasi oleh pihak-pihak yang tidak berwenang. *Snooping* merupakan bentuk dari *disclosure*.

2. Penyamaran (*masquering*) yakni peniruan terhadap suatu entitas terhadap entitas yang lain. Sebagai contoh, 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.
3. *Disruption*, yakni penyerangan terhadap sistem untuk melemahkan sumber daya sistem tersebut sehingga tidak dapat diakses atau sistem mengalami *crash*. Penyerangan ini dapat dilakukan melalui serangan DoS atau Denial Of Service dengan

mengeksploitasi kelemahan yang terdapat di dalam protokol TCP.

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

3.2 Kebijakan (*Policy*)

Kebijakan yang diterapkan dalam membangun sistem *e-voting*. [3]*Secure voting* yang dibangun secara komputerisasi dapat digunakan jika terdapat protokol yang menjamin dua hal dibawah ini, yaitu :

- 1 Privasi individu
 - 2 Pencegahan terhadap kecurangan.
- Suatu protokol yang ideal harus memiliki 6 persyaratan sebagai berikut :
- 1 Hanya pemilih yang berhak yang dapat memberikan suara (otentikasi);
 - 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;

Setiap pemilih dapat memastikan bahwa suara mereka sudah dikirimkan dan terhitung dalam penghitungan akhir.

3.3 Spesifikasi (*Specification*)

Secara Umum sistem pengiriman hasil suara mesin *voting* menuju CTF yang dibangun dapat memenuhi spesifikasi umum sebagai berikut:

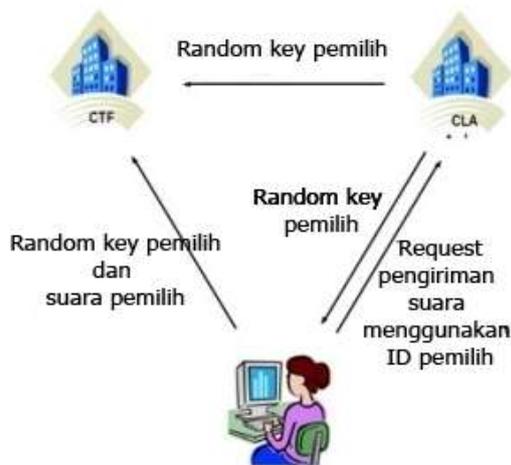
1. Hanya mesin *voting* yang terdaftar yang dapat mengirimkan suara.
 - Terdapat *validation ID* yang acak dan unik untuk setiap mesin *voting*.
 - Seluruh mesin *voting* aktif didaftarkan pada VPN dengan IP tertentu, sehingga IP asing tidak akan bisa mengakses jaringan tersebut.
2. Tidak boleh mengirimkan lebih dari satu hasil suara.
 - Jika mesin *voting* telah melakukan pengiriman dan kembali melakukan pengiriman maka CTF akan mengembalikan pesan “Mesin *voting* tersebut sudah melakukan pengiriman sebelumnya”.
3. Setiap pemilih dapat memastikan bahwa suara mereka sudah dikirimkan dan terhitung dalam penghitungan akhir.

Jika sebuah mesin *voting* mengirimkan hasil suara, CTF akan mengakumulasi dan menghitung kandidat dan

mengembalikan hasil penghitungan sementara. Hal ini menyebabkan mesin *voting* dapat memastikan bahwa hasil suaranya benar telah dihitung oleh CTF.

3.4 Perancangan (*Design*)

Protokol *two central facilities* memiliki dua lembaga penyelenggara pemilu yang diimplementasikan dalam dua *server* yang berbeda[4]. Server pertama yakni *Central Legitimization Agency* (CLA) merupakan badan sertifikasi pemilih yang memiliki tugas utama mengotentikasi 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 *votin*, berikut ini gambar yang merupakan skema dari sistem *e-voting* dapat dilihat pada Gambar 2.



Gambar 2. Skema sistem e-voting

Server pertama yakni *Central Legitimization Agency* (CLA) merupakan badan sertifikasi pemilih yang memiliki tugas utama mengotentikasi dan mengotorisasi pemilih. *Central Legitimization Agency* (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 *Central Tabulating Facilities* (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.

Adapun alur kerja sistem *e-voting* berdasarkan gambar tersebut terbagi menjadi empat tahapan dengan penjabaran sebagai berikut:

➤ Tahap 1

1. Pengiriman kunci public oleh masing-masing mesin voting kepada CLA.
2. CLA mengirimkan kunci simetri yang telah di enkripsi menggunakan kunci publik yang di terima dari masing-masing mesin voting dan diberikan kepada masing-masing mesin voting sesuai alamat IP address masing-masing mesin voting.

➤ Tahap 2

1. Pemilih (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. Selanjutnya CLA akan melakukan autentikasi pemilih dengan database.
5. Apabila pemilih dinyatakan berhak memilih dengan ketentuan pemilih telah terdaftar di database dan belum memilih sebelumnya maka pemilih

akan diarahkan kepada halaman pemilihan dan status pemilih akan diubah menjadi status telah melakukan autentikasi. Namun apabila pemilih dinyatakan tidak berhak memilih maka pemilih langsung diarahkan ke halaman gagal memilih.

6. Setelah pemilih melakukan pemilihan, pilihan pemilih akan di simpan pada mesin *voting*, dan status pemilih akan diubah menjadi status telah melakukan pemilihan
7. Mesin akan terus menerus melakukan proses yang sama sampai pada waktu pemilihan usai.

➤ Tahap 3

1. Pengiriman kunci public oleh masing-masing mesin *voting* kepada CTF.
2. CTF mengirimkan kunci simetri yang telah di enkripsi menggunakan kunci public yang di terima 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 membuat suatu tanda tangan digital dari jumlah suara yang di hash menggu
4. Mesin *voting* akan mengirimkan identitas mesin, data hasil pemilihan, tanda tangan digital, dan juga nilai random kepada CTF yang didapatkan dari CLA yang telah di enkripsi.
5. CTF melakukan pencocokan nilai random key yang diberikan mesin dengan random key yang diterima dari CLA untuk mesin tersebut.
6. Jika sah, CTF akan melakukan pengecekan data yang dikirim dengan tanda tangan digital yang dikirimkan.
7. Apabila tanda tangan digital dan data yang dikirimkan sesuai maka nilai yang diberikan mesin kepada CTF akan di-store ke dalam CTF.
8. Mesin akan terus menerus melakukan proses yang sama sampai pada waktu pemilihan usai.

Terdapat beberapa tahapan pemilihan dalam sistem *e-voting* ini yang berfungsi untuk mengarahkan pemilih dalam proses pemilihan, tahapan-tahapan tersebut ialah

1. Tahap pemilihan surat suara

Pada tahapan ini pemilih diberikan waktu 20 detik untuk memilih calon kandidat yang tersedia. Kesempatan

untuk memilih calon kandidat hanya diberikan sebanyak-banyaknya adalah dua kali kesempatan. Apabila pemilih tidak memanfaatkan kedua kesempatan tersebut maka 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 maka suara akan dinyatakan abstain namun jika memutuskan memilih perpanjangan waktu maka 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 maka 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 apapun 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 maka pemilih tersebut 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.

3.4.1 Perancangan Basis Data

Basis data dibagi menjadi tiga bagian utama, yaitu basis data pada masing-masing mesin *voting*, basis data CLA sebagai basis data otentikasi dan basis data CTF yang digunakan untuk perhitungan suara total.

1. Basis Data mesin *voting* dapat dilihat pada Tabel 1.

Tabel 1. Basis Data mesin voting

Nama Tabel	Jumlah Kolom	Deskripsi
Kandidat	4	Tabel yang berisi data calon dan jumlah perolehan suara masing-masing calon
Waktu	2	Tabel yang berisi waktu mulai dan waktu akhir dari <i>voting</i>

2. Basis Data CLA dapat dilihat pada Tabel 2.

Tabel 2. Basis Data CLA

Nama Tabel	Jumlah Kolom	Deskripsi
Pemilih	5	Tabel yang berisi data pemilih dan status pemilih
Validasi_mesin	2	Tabel yang berisi id mesin dan nomor validasi mesin
Waktu	2	Tabel yang berisi waktu mulai dan waktu akhir dari voting

3. Basis Data CTF dapat dilihat pada Tabel 3.

Tabel 3. Basis Data CTF

Nama Tabel	Jumlah Kolom	Deskripsi
Mesin_voting	4	Tabel yang berisi data surat suara yang berasal dari mesin voting.
Validasi_mesin	4	Tabel yang berisi id mesin dan nomor validasi mesin
Waktu	2	Tabel yang berisi waktu mulai dan waktu akhir dari voting
Keterangan_pemilih	4	Tabel yang berisi keterangan pemilih yang berasal dari CLA

3.5 Implementasi (*Implementation*)

Idealnya mesin *voting* ialah satu perangkat komputer yang telah dirakit untuk menjadi mesin *voting*, dengan kebijakan sebagai berikut :

a. Mesin tidak menyediakan keyboard ataupun mouse selama proses *e-voting*. Hal ini di anjurkan agar interaksi antara manusia dengan mesin *voting* menjadi lebih terbatas, 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 *capacitive 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.

Adapun spesifikasi *hardware* komputer yang dijadikan mesin *e-voting* pada sistem *e-voting* ialah sebagai berikut

- Processor : intel dual core 2,6 Ghz
- Main Memory : Ram 2 Gb
- Storage Disk : HD SATA 8 Gb
- Layar sentuh *single touch* LG 17 inc

3.5.1 Antarmuka Halaman Surat Suara Evoting

Perancangan antarmuka halaman untuk sistem *e-voting* juga harus memenuhi berbagai ketentuan, sebab perancangan ini terkait erat dengan calon kandidat yang akan dipilih oleh pemilih. Berikut ini ada tampilan dari halaman sistem *e-voting*.

a. Tampilan otentikasi pemilih

Tampilan halaman pertama adalah otentikasi pemilih untuk bias melakukan proses pemilihan, dapat dilihat pada Gambar dibawah ini dimana nomor UID yang menjadi fungsi otentikasi pemilih berdasarkan kode NIK.



Gambar 4. Halaman otentikasi pemilih

b. Tampilan Surat suara

Tampilan halaman surat suara dapat dilihat pada Gambar 5 dimana terdapat tiga calon kandidat yang dapat dipilih.



Gambar 5. Halaman surat suara

c. Tampilan perpanjangan waktu

Tampilan Halaman perpanjangan waktu ditunjukkan pada Gambar 6 dimana pemilih diberikan pertanyaan dengan jawaban “Ya” atau “Tidak” untuk menjawab “Perpanjangan waktu pemilih”.



Gambar 6. Halaman perpanjangan waktu

d. Tampilan surat suara kesempatan kedua

Apabila pemilih menggunakan kesempatan keduanya untuk memilih, maka akan diberikan halaman surat suara dengan peringatan kesempatan terakhir seperti pada Gambar 7.



Gambar 7. Halaman surat suara kesempatan kedua

e. Tampilan memastikan pemilih

Halaman yang memastikan pemilih yakin akan pilihannya ditunjukkan pada Gambar 8. Pada halaman ini ditulis nomor urut kandidat yang telah dipilih

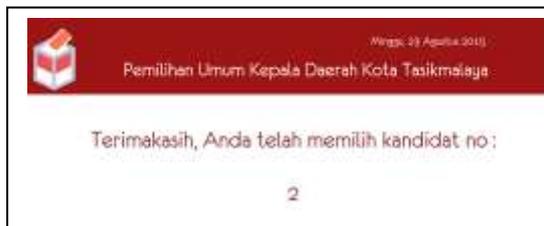
melalui halaman surat suara. Pemilih tinggal menentukan jawaban “Ya” atau “Tidak” untuk kepastian pilihannya..



Gambar 8. Halaman memastikan pemilih

f. Tampilan bukti selesai pemilih.

Pemilih yang benar-benar yakin akan pilihannya dan menjawab “Ya” akan diarahkan pada halaman bukti suara elektronik seperti pada Gambar 9.



Gambar 9. Halaman bukti selesai memilih

g. Tampilan bukti tidak memilih.

Pemilih yang dinyatakan abstain maka pada bukti suara elektronik akan ditampilkan tulisan “Anda tidak memilih siapapun” seperti pada Gambar 10.



Gambar 9 Halaman bukti tidak memilih.

4. SIMPULAN

Beberapa kesimpulan yang dapat diambil pada penelitian ini antara lain:

- Rancang bangun sistem *e-voting* pilkada Kota Tasikmalaya dengan menggunakan *protocol two central facilities* yang mengimplementasikan pengembangan *Central Legitimization Agency (CLA)* dan *Central Tabulating Facilities (CTF)* yang dapat mewujudkan sistem *e-voting* yang aman, efektif, dan efisien.
- Dalam otentikasi pemilih hanya nomor NIK yang sudah di daftarkan yang dapat melakukan proses pemilihan.
- Berdasarkan waktu yang telah ditentukan, pemilih hanya dapat diberikan waktu 20 detik untuk dapat melakukan proses pemilihan.

PENELITIAN LANJUTAN

Hal-hal yang dapat disarankan berdasarkan hasil penelitian ini di antaranya:

- Sistem harus memiliki pengamanan database baik itu pengamanan

menggunakan database mirror ataupun pengenkripsian setiap nilai-nilai yang ada di dalam database tersebut.

- Dilakukannya penelitian mengenai rekayasa sosial yang dapat terjadi pada sistem *evoting*.
- Penelitian mengenai perhitungan-perhitungan arus lalu lintas data yang harus diperdalam.

DAFTAR PUSTAKA

- [1] Bruce, Schneier. 1996. *Applied Cryptography*. Second Edition, Jon Wiley & Sons.
- [2] Bishop, Matt. 2003. *Computer Security Art and Science*. Addison-Wesley.
- [3] Schneier B. 1996. *Applied Cryptography, second edition : Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc.
- [4] Sireesha, Janga & So-In Chakchai .2005. *Secure Virtual Election Booth with Two Central Facilities*. Department of Computer Science Washington University in St. Louis, USA. 2007.