Penerapan Sistem *E-Voting* pada Pemilihan Kepala Daerah di Indonesia (The Application of E-Voting Systems in the Local Elections in Indonesia)

Shelvie Nidya Neyman[1], Muhammad Fikri Isnaini[2], Sri Nurdiati[3]
[1,2, 3]Departemen Ilmu Komputer FMIPA IPB, JL. Meranti Wing 20 Lv V, Kampus Dramaga, Bogor, 16680, [1] shelvie@ipb.ac.id ; [3]nurdiati@ipb.ac.id

Diterima 7 Oktober 2013/ Disetujui 21 Oktober 2013

ABSTRACT

On this research, the protocol and simulation of e-voting system were designed for the local election. The functions on this system were tailored to the e-voting scheme which must meet several criterias: Eligibility, Unreusability, Anonymity, Accuracy, Fairness, Vote and Go, and Public Verifiability. The protocol which was made in this research was a system for voter registration, validation and activation voters, the election system, and the election calculation system. To maintain the security of data, the e-voting system used public key algorithm and symmetric key algorithm. The result of this research was a web-based e-voting system which runs on the computer network that meets the criteria of e-voting scheme. The result of this research showed that the e-voting process can accelerate the vote calculation and decrease human errors.

Keywords: voting, e-voting, the public key cryptography algorithm, pilkada

PENDAHULUAN

Indonesia adalah negara penganut sistem politik demokrasi, dengan menggunakan *voting* untuk pengambilan keputusan dalam pemilihan wakil-wakil rakyat ataupun kepala daerah. Dalam pelaksanaan voting saat ini masih terdapat kelemahan-kelemahan baik dari sistem pemilihan kepala daerah (pilkada) itu sendiri ataupun *human error*.

Perkembangan teknologi informasi saat ini telah membawa perubahan yang besar bagi manusia, termasuk cara untuk melaksanakan *voting*. Penggunaan teknologi komputer pada pelaksanaan *voting* ini dikenal dengan istilah *electronic voting* atau lazim disebut dengan *e-voting*. Pengertian dari *electronic voting(e-voting)* secara umum adalah penggunaan teknologi komputer pada pelaksanaan *voting*. Pilihan teknologi yang digunakan dalam implementasi dari *e-voting* sangat bervariasi, seperti penggunaan *smart card* untuk autentikasi pemilih, penggunaan internet sebagai sistem pemungutan suara, penggunaan *touch screen* sebagai pengganti kartu suara, dan masih banyak variasi teknologi yang digunakan (Azhari 2005).

Pada sistem *e-voting* penggunaan kertas sudah diminimalkan karena sistem ini sudah berbasis teknologi digital. Secara sederhana dalam sistem *e-voting*, pada saat pilkada pemilih yang terdaftar hanya menunjukkan tanda pemilih lalu *login* menggunakan *id* dan *password* masing-masing, setelah itu pemilih melakukan pemilihan calon hanya dengan melakukan tindakan klik pada pilihan yang disediakan sistem ini, lalu sistem akan menghitung pilihannya secara digital. Untuk perhitungan total pun dilakukan oleh sistem secara digital menggunakan fungsi aritmatika sederhana, yaitu penjumlahan yang dapat dilakukan dalam hitungan detik. Dengan sistem *e-voting* sudah melakukan efisiensi waktu dan tenaga yang digunakan dalam melakukan perhitungan suara.

Algoritme kunci publik merupakan salah satu teknik kriptografi yang dapat melakukan enkripsi dan dekripsi data serta penandaan digital. Metode enkripsi disebut dengan skema enkripsi kunci publik jika untuk setiap pasangan kunci (*e,d*), satu kunci *e* dibuat tersedia untuk umum (publik) dan kunci pasangannya *d* dibuat untuk pribadi dan dijaga kerahasiaannya. Skema tersebut dikatakan aman, jika secara perhitungan tak-layak menentukan *d* dari *e* (Guritman 2003). Penggunaan algoritme kunci publik RSA pada sistem *e-voting*ini untuk melakukan enkripsi pada transaksi data sehingga menambah fitur jaminan keamanan dan kerahasiaan data. RSA dipilih dalam penelitian ini karena algoritma tersebut banyak digunakan untuk aplikasi yang membutuhkan keamanan data digital (Boneh 1999). Algoritma kiriptograsi kunci simetri juga dipergunakan dalam sistem ini untuk enkripsi kunci privat sistem menggunakan Algoritme Twofish. Desain fungsi *round* dan penjadwalan kunci pada algoritma ini mengakibatkan adanya *tradeoffs* antara kecepatan, ukuran perangkat lunak, waktu *setup key,* jumlah gerbang, dan memori (Schneier *et al* 1998).

Penelitian ini bertujuan untuk mengembangkan sistem e-voting pada pemilihan kepala daerah di Indonesia dengan melakukan simulasi pada lingkungan terbatas. Hasil dari penelitian ini diharapkan dapat menjadi bahan masukan bagi pemerintah atau pihak terkait dalam penerapan e-voting di Indonesia. Pada penelitian ini simulasi sistem dibatasi pada pembuatan sistem berbasis *desktop*, dan belum melakukan keamanan pada kerahasiaan isi basisdata sistem. Bagian selanjutnya dari tulisan ini membahas tentang skema E-voting yang diusulkan dalam penelitian ini, implementasi sistem E-Voting pada pilkada di Indonesia, pembahasan fitur keamanan dalam sistem ini dan ditutup dengan kesimpulan.

METODOLOGI

Metode Kajian

Skema e-voting

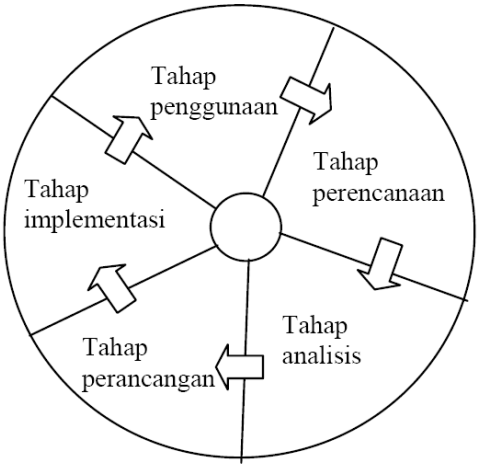
Skema *e-voting* adalah satu set protokol yang menjaga keamanan atau kerahasiaan pemilih dalam melakukan pemilihan serta interaksi dengan penitia pemilihan dan perhitungan suara. *E-voting* biasanya dibedakan menjadi dua tipe, yaitu *online* (misalnya via internet) dan *offline* (menggunakan mesin perhitungan suara atau kertas suara).

Tujuan dari keamanan sistem *e-voting* adalah untuk menjamin privasi atau kerahasiaan pemilih dan keakuratan pilihan. Keamanan sistem ini memiliki beberapa kriteria, yaitu:

1. *Eligibility:* hanya pemilih yang terdaftar yang dapat melakukan pemilihan.
2. *Unreusability:* setiap pemilih hanya bisa memberikan satu kali pilihan.
3. *Anonymity:* pilihan pemilih dirahasiakan.
4. *Accuracy:* pilihan tidak bisa diubah atau dihapus selama atau setelah pemilihan dan juga tidak bisa ditambahkan setelah pemilihan ditutup.
5. *Fairness:* perhitungan suara sebelum pemilihan ditutup tidak bisa dilakukan.
6. *Vote and Go:* pemilih hanya dapat melakukan pemilihan saja.
7. *Public Verifiability:* setiap orang dapat melakukan pengecekan pada berjalannya proses pemilihan (Canard & Sibert 2001).

Metode Pengembangan Sistem

Metode yang digunakan untuk implementasi e-voting system ini adalah System Life Cycle (SLC) seperti pada Gambar 1. Berdasarkan McLeod (2004) System Life Cycle (SLC) terdiri dari fase perencanaan, analisis sistem, desain sistem, implementasi, pengujian, evaluasi, dan penggunaan.



Gambar 1 Metode Kajian.

HASIL DAN PEMBAHASAN

Sistem E-Voting pada Pilkada Indonesia

Tahap Perencanaan dan Analisis

Pada tahap ini dilakukan perencanaan dan analisis terhadap kebutuhan sistem dari data dan literatur yang didapat dengan hasil sebagai berikut:

1. Hasil analisis skema *e-voting*

Berdasarkan *paper* yang ditulis Canard & Sibert (2001), sistem *e-voting* harus memenuhi beberapa kriteria dengan tujuan keamanan sistem dan kerahasiaan pemilih. Pada penelitian ini, sistem *e-voting* yang dibuat sudah memenuhi kriteria sebagai berikut:

a. Hanya pemilih yang sudah melakukan pendaftaran dan telah divalidasi dan dipengaktifan pendaftarannya oleh panitia pemilihan yang dapat masuk ke sistem *e-voting* dan melakukan pemilihan kepala daerah.
b. Setiap pemilih yang sudah melakukan pemilihan tidak dapat melakukan pemilihan lagi atau memperbaiki pilihannya. Pemilih hanya dapat memberikan satu kali pilihannya pada satu pasangan calon.

c. Pilihan dari pemilih dirahasiakan. Setelah melakukan pemilihan, hasil pilihan pemilih dienkripsi menggunakan algoritme RSA dengan kunci publik pemilih dan disimpan dalam basis data. Hanya pemilih yang tahu pilihannnya dengan mendekripsi pilihannya menggunakan kunci privat.
d. Pemilihan baru bisa dilakukan pada jangka waktu yang sudah ditentukan panitia. Setelah melakukan pemilihan, pemilih tidak dapat melakukan pemilihan lagi atau mengganti pilihannya.
e. Perhitungan suara tidak dapat dilakukan sebelum pemilihan selesai. Setelah pemilihan selesai, panitia masing-masing kelurahan mengirimkan hasil perhitungan di tempatnya ke pusat perhitungan dengan mengenkripsi data perhitungan yang dikirimkan.
f. Pemilih hanya dapat melakukan pemilihan saja. Pemilih tidak dapat mengubah data calon, waktu pemilihan, dan data dirinya.
g. Setiap pemilih dapat mengecek kembali pilihannya dengan memasukkan *password* ke sistem, setelah itu pilihan pemilih akan ditampilkan. Pemilih juga dapat melihat langsung hasil pemilihan setelah pemilihan selesai.

Pada sistem ini, setiap pemilih diberikan kartu pemilih ketika pendaftaran yang dilakukan benar dan dinyatakan *valid* oleh panitia pemilihan. Kartu pemilih akan digunakan ketika akan melakukan pemilihan pada tempat yang sudah ditentukan oleh panitia sebagai bukti bahwa pemilih sudah terdaftar dengan benar.

2. Deskripsi umum sistem

Sistem *e-voting* ini adalah sistem berbasis *web* dengan tiga modul utama, yaitu:

a. Modul pendaftaran pemilih

Modul ini digunakan untuk pendaftaran pemilih, pengaktifan pemilih, dan pemberian kartu pemilih.

b. Modul pemilihan

Modul ini merupakan modul utama pada sistem. Pada modul ini terdapat sistem pemilihan pasangan calon dimana tiap pemilih hanya dapat melakukan satu pilihan dan tidak dapat mengubah pilihannya. Hasil pilihan akan dienkripsi menggunakan algoritme kunci publik dan disimpan dalam basis data. Pada modul ini pun pemilih dapat mengecek kembali hasil pilihannya. Pada modul ini juga terdapat fungsi untuk autentikasi pemilih, dan *captcha*.*Captcha* bukan sekedar gambar dengan susunan teks, ia adalah tes atau banyak tes yang dapat berubah secara otomatis yang sebagian besar orang dapat melaluinya, tetapi program komputer saat ini tidak bisa melaluinya (Ahn 2004). *Captcha* biasa digunakan oleh Yahoo, Hotmail, Paypal, dan banyak *website* yang populer menggunakannya untuk mencegah pendaftaran secara otomatis. Hal ini bekerja karena tidak ada program komputer yang bisa membaca susunan teks seperti manusia

c. Modul perhitungan suara

Modul ini adalah modul untuk melakukan perhitungan suara. Modul ini terdiri dari dua bagian, yaitu perhitungan suara pada tiap kelurahan dan perhitungan suara total. Perhitungan suara di kelurahan baru dapat dilakukan setelah data perhitungan pada masing-masing TPS dienkripsi terlebih dahulu telah masuk ke basis data di kelurahan. Setelah itu tiap kelurahan mengirimkan hasil perhitungannya ke pusat perhitungan dengan terlebih dahulu mengenkripsi data perhitungan yang akan dikirim.

3. Analisis kebutuhan pengguna

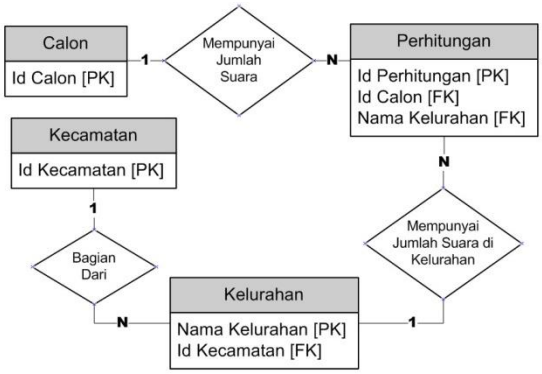
Kebutuhan pengguna terhadap aplikasi ini adalah sebagai berikut:

a. Terdapat fungsi untuk pendaftaran pemilih sehingga untuk melakukan pemilihan pemilih harus melakukan pendaftaran dengan benar.
b. Terdapat fungsi untuk pengaktifan pemilih sehingga hanya pemilih yang datanya *valid* yang dapat masuk ke sistem *e-voting*.
c. Terdapat fungsi autentikasi pemilih sehingga hanya pemilih yang berhak saja yang dapat masuk ke sistem *e-voting.*
d. Terdapat fungsi pemilihan calon yang terjaga keamanan dan kerahasiaannya.
e. Terdapat fungsi pengecekan hasil pilihan pemilih oleh pemilih. Pada fungsi ini pemilih memasukkan *password* untuk mengetahui pilihannya.
f. Terdapat fungsi perhitungan suara di tiap TPS dan kelurahan.
g. Terdapat fungsi perhitungan suara total dari seluruh kelurahan. Pada fungsi ini hasil perhitungan di tiap kelurahan dikirimkan ke pusat perhitungan yang sebelumnya data perhitungan tiap kelurahan dienkripsi terlebih dahulu.

Pengguna dari sistem ini adalah pemilih dan panitia pemilihan.

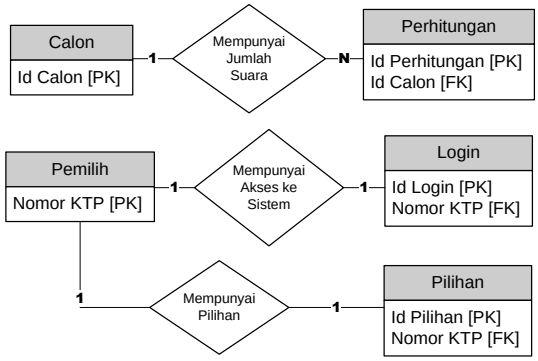
4. Analisis desain basis data sistem

Basis data pada sistem *e-voting* ini dibagi menjadi tiga bagian, yaitu basis data pusat, kelurahan, dan TPS. Pada basis data pusat disimpan data calon, hasil perhitungan suara tiap kelurahan, nama kecamatan, dan nama kelurahan. Tabel hasil perhitungan akan disimpan berdasarkan jumlah suara yang diperoleh calon pada tiap kelurahan. Dalam basis data juga disimpan data kecamatan yang terdiri dari beberapa kelurahan. *Entity Relationship Diagram* (ERD) untuk basis data pusat dapat dilihat pada Gambar 2.



Gambar 2. ERD basis data pusat.

Pada basis data kelurahan dan TPS disimpan data calon, hasil perhitungan suara, pemilih dan *login*-nya, dan pilihan dari pemilih. Pada tabel perhitungan disimpan jumlah suara dari calon. Tiap pemilih hanya memiliki satu akun untuk *login* dan basis data juga menyimpan pilihan dari pemilih dengan syarat tiap pemilih hanya memiliki satu pilihan. ERD dari basis data kelurahan dan TPS dapat dilihat pada Gambar 3.



Gambar 3. ERD basis data kelurahan dan TPS.

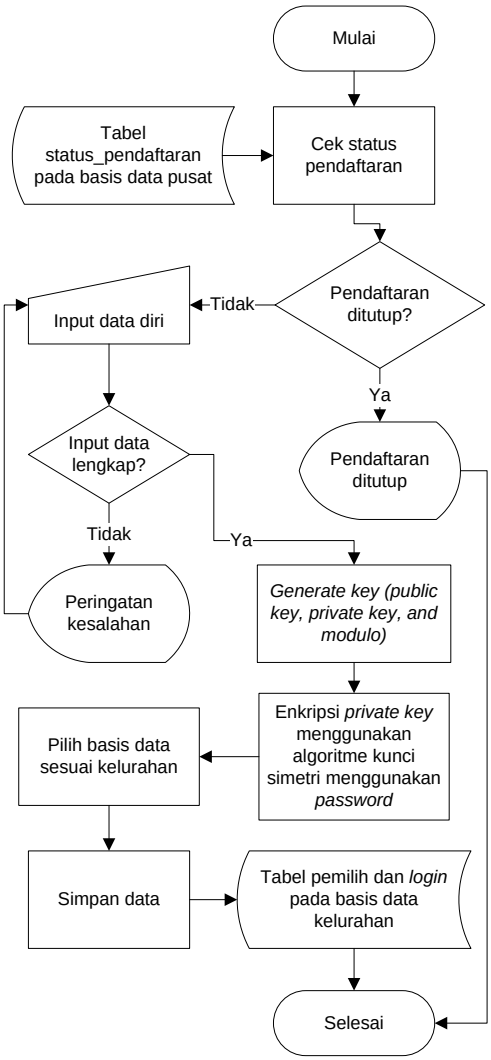
Desain basis data TPS sama dengan basis data kelurahan, perbedaannya hanya isi basis data TPS yang lebih sedikit. Isi basis data TPS adalah pembagian pemilih berdasarkan tempat pemilih akan memilih sesuai RT dan RW-nya. Jadi pemilih akan melakukan pemilihan di lokasi TPS yang sudah ditentukan oleh panitia.

Tahap Perancangan Sistem

1. Perancangan Sistem Pendaftaran Pemilih

Salah satu kriteria sistem *e-voting* adalah setiap pemilih yang akan melakukan pemilihan (masuk ke sistem) harus terdaftar di basis data masing-masing kelurahan, oleh karena itu fungsi pertama yang dijalankan oleh sistem adalah fungsi pendaftaran. Hasil dari perancangan sistem pendaftaran pemilih bisa dilihat pada *flowchart* pendaftaran pemilih pada Gambar 4.

Pendaftaran hanya bisa dilakukan pada saat pendaftaran dibuka oleh panitia. Data yang dimasukkan adalah data diri pemilih sesuai dengan KTP pemilih ditambah *captcha* dan *password* yang digunakan ketika *login*. Jika input data lengkap, maka sistem akan membuatkan kunci publik, privat, dan modulo menggunakan algoritme kunci publik. Untuk kunci privat sistem akan melakukan enkripsi menggunakan algoritme kunci simetri menggunakan *password* yang dimasukkan tadi. Tujuan dari enkripsi ini agar pemilih tidak harus menghafal kunci privat yang diberikan sistem tapi hanya menghafal *password* yang dimasukkan ketika pendaftaran.



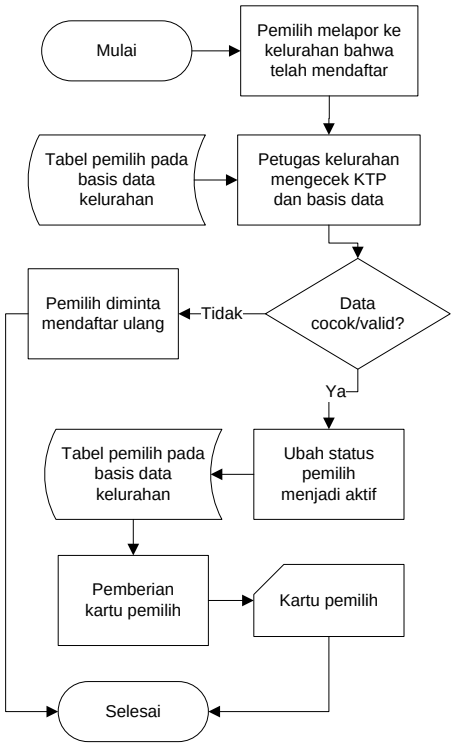
Gambar 4. *Flowchart* pendaftaran pemilih.

2. Perancangan Validasi dan Pengaktifan Pemilih

Fungsi selanjutnya setelah pendaftaran adalah perancangan untuk validasi dan pengaktifan pemilih. Fungsi ini dijalankan oleh panitia pemilihan yang mengecek data pendaftaran pemilih, jika data *valid* maka pemilih akan dipengaktifan dan diberikan kartu pemilih yang menandakan pemilih sudah terdaftar dan berhak melakukan pemilihan. Hasil perancangan validasi dan pengaktifan pemilih dapat dilihat pada *flowchart* validasi dan pengaktifan pemilih pada Gambar 5.

3. Perancangan *Login* ke Sistem

Perancangan pada fungsi ini digunakan untuk masuk ke dalam sistem dengan nomor KTP, *password* pemilih, dan *captcha*. Setelah *login*, maka pemilih dapat melakukan pemilihan. Fungsi *login* ini dilakukan oleh pemilih pada saat pemilihan telah dimulai di masing-masing TPS yang telah ditentukan panitia. *Flowchart* untuk fungsi *login* dapat dilihat pada Gambar 6.



Gambar 5. *Flowchart* validasi dan pengaktifan pemilih.

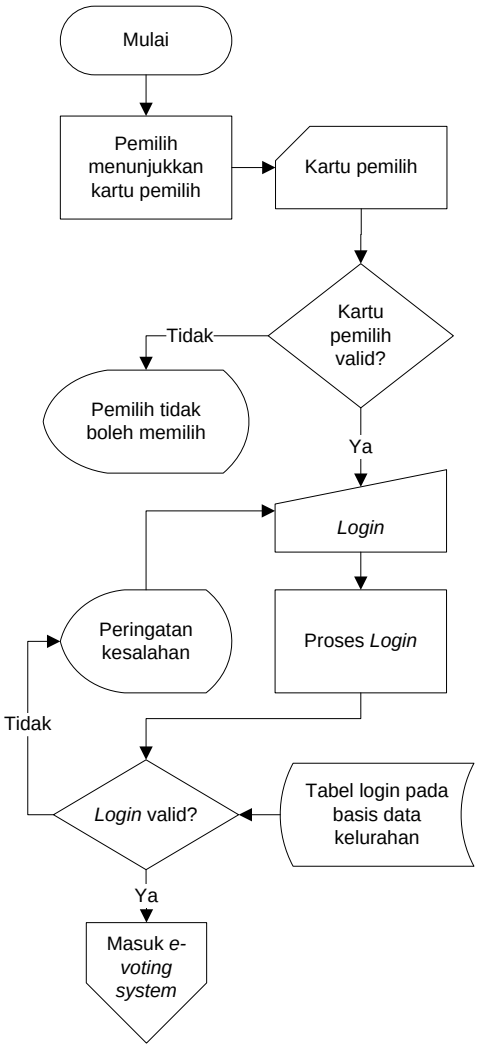
4. Perancangan Sistem Pemilihan

Fungsi ini merupakan fungsi utama dari sistem *e-voting* dimana sistem ini menggunakan enkripsi-dekripsi algoritme kunci publik dan algoritme kunci simetri. Fungsi ini harus memenuhi kriteria sistem *e-voting*, yaitu pemilih hanya bisa memberikan satu kali pilihannya dan tidak bisa mengubah pilihannya setelah melakukan pemilihan. Pemilihan hanya bisa dilakukan pada waktu yang sudah ditentukan panitia. Fungsi ini digambarkan pada *flowchart* sistem pemilihan pada Gambar 7.

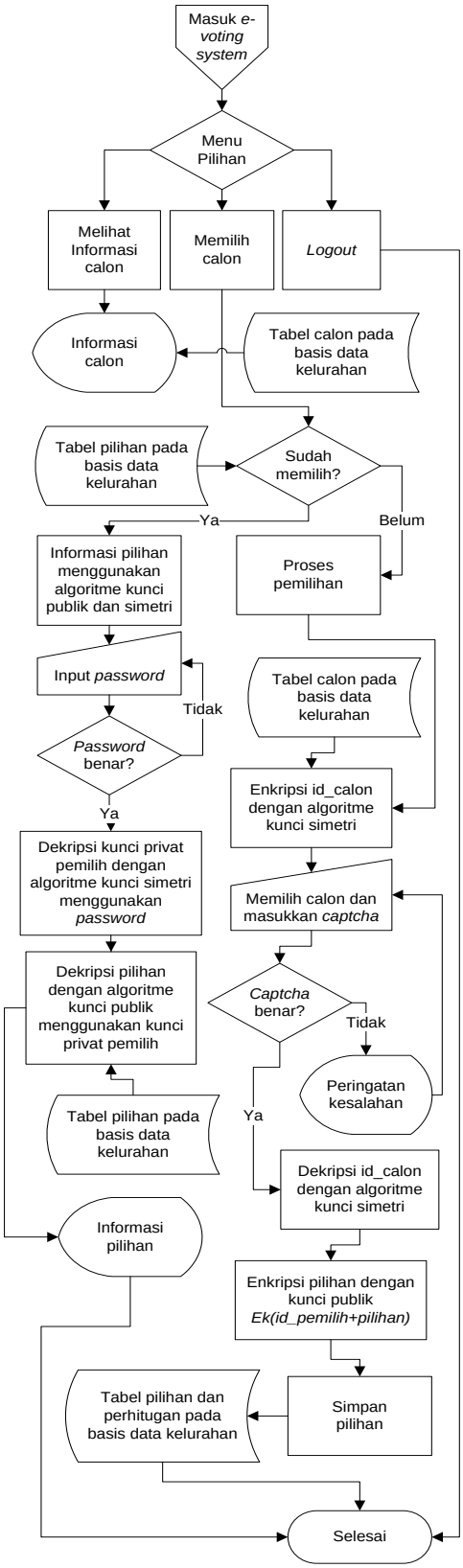
5. Perancangan Sistem Perhitungan Suara

Fungsi perhitungan suara digunakan setelah pemilihan selesai. Fungsi ini ada dua bagian, yaitu fungsi perhitungan suara di kelurahan dan fungsi perhitungan suara pusat atau total. Fungsi perhitungan suara di kelurahan merupakan penjumlahan dari hasil perhitungan suara di masing-masing TPS. Setelah proses pemilihan sistem *e-voting* di masing-masing TPS akan melakukan perhitungan secara otomatis, lalu jumlah hasil perhitungan di enkripsi dan dikirimkan oleh panitia di TPS ke kelurahan. Di kelurahan sistem *e-voting* akan mendekripsi hasil perhitungan di TPS yang telah dikirimkan dan menjumlahkannya. *Flowchart* sistem perhitungan suara di kelurahan dapat dilihat pada Gambar 8.

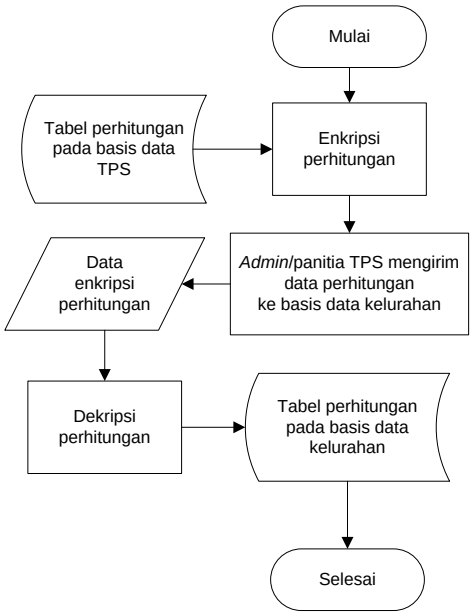
Fungsi perhitungan suara total merupakan hasil penjumlahan dari perhitungan suara di masing-masing kelurahan. Setelah perhitungan suara di kelurahan selesai, panitia di kelurahan mengirimkan hasil perhitungan suara yang sudah di enkripsi ke perhitungan pusat. Pada sistem *e-voting* pusat data yang dikirimkan oleh kelurahan akan didekripsi lalu dijumlahkan. *Flowchart* sistem perhitungan suara total dapat dilihat pada Gambar 9.



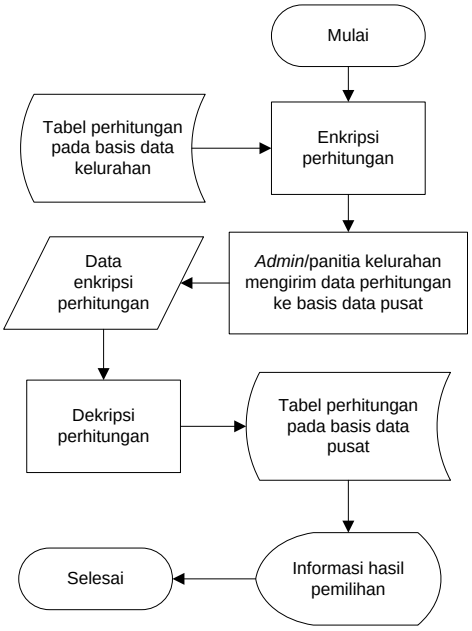
Gambar **6.** *Flowchartlogin* ke sistem *e-voting*.



Gambar 7*Flowchart* sistem pemilihan.



Gambar 8. *Flowchart* sistem perhitungan suara di kelurahan.



Gambar 9. *Flowchart* sistem perhitungan suara total.

6. Perancangan Basis Data

Basis data pada sistem ini dibagi menjadi dua bagian utama, yaitu basis data pada masing-masing TPS dan kelurahan dan basis data pusat yang digunakan untuk perhitungan suara total.

a) Basis Data di TPS dan Kelurahan

Basis data di TPS dan kelurahan memiliki desain yang sama, yaitu terdiri dari enam tabel yang digambarkan pada Tabel 1.

Tabel 1 Basis Data di TPS dan Kelurahan

Nama Tabel	Jumlah Atribut	Deskripsi
Calon	7	Tabel yang berisi data pasangan calon
pemilih	13	Tabel yang berisi data pemilih yang diisi pada saat melakukan pendaftaran
Login	8	Tabel yang berisi kunci publik, kunci privat, *password*, dan modulo pemilih
perhitungan	2	Tabel yang berisi jumlah perhitungan suara tiap pasangan calon pada kelurahan
Pilihan	3	Tabel yang berisi pilihan dari pemilih yang dienkripsi oleh kunci publik pemilih
pemilihan	1	Tabel yang berisi status pemilihan untuk membuka atau menutup pemilihan

b) Basis Data di Pusat
Basis data di pusat terdiri dari lima tabel yang digambarkan pada Tabel 2.

Tabel 2 Basis Data di Pusat

Nama Tabel	Jumlah Atribut	Deskripsi
Calon	7	Tabel yang berisi data pasangan calon
kecamatan	2	Tabel yang berisi data kecamatan pada kabupaten Bogor
kelurahan	6	Tabel yang berisi data kelurahan pada tiap kecamatan dan juga berisi nama basis data pada tiap kelurahan
perhitungan	4	Tabel yang berisi hasil perhitungan suara pada masing-masing kelurahan
status_pendaftaran	1	Tabel yang berisi status pendaftaran untuk membuka atau menutup pendaftaran

Tahap Implementasi Sistem

1. Implementasi Sistem Pendaftaran Pemilih

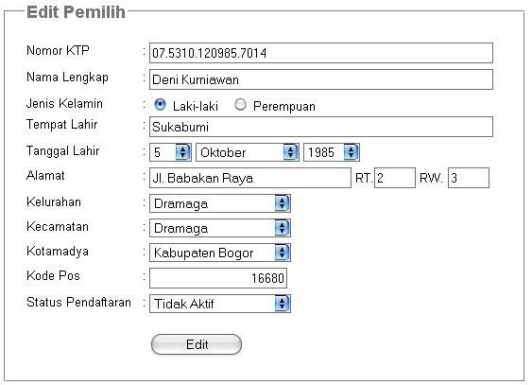
Halaman untuk pendaftaran pemilih dapat dilihat pada Gambar 10.Setelah pemilih mengisi *form* pendaftaran dengan benar, maka sistem akan memasukkan data pendaftaran ke dalam basis data kelurahan sesuai dengan kelurahan yang dimasukkan oleh pemilih.

Gambar 10. Halaman pendaftaran pemilih.

2. Implementasi Validasi dan Pengaktifan Pemilih

Halaman untuk validasi dan pengaktifan pemilih dapat dilihat pada Gambar 11 dan 12.

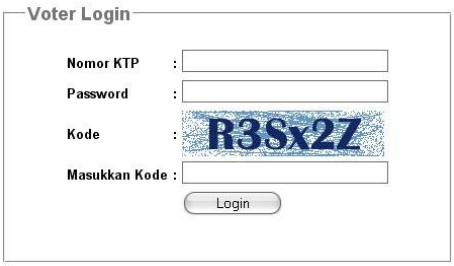
Gambar 11. Menu pengaktifan pemilih.



Gambar 12. Halaman edit pemilih.

3. Implementasi *Login* ke Sistem

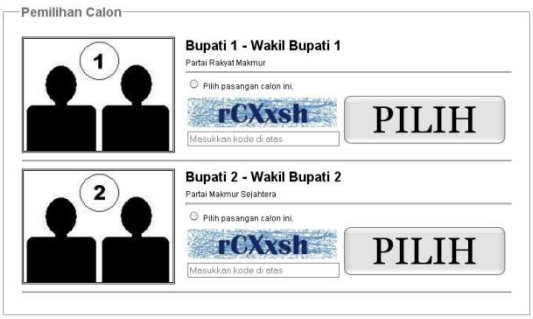
Halaman untuk *login* dapat dilihat pada Gambar 13. Proses *login* setelah pemilih menekan tombol *login* adalah membuat *session* berdasarkan tingkatan pengguna.



Gambar 13. Halaman *login*.

4. Implementasi Sistem Pemilihan

Halaman untuk pemilihan dapat dilihat pada Gambar 14. Setelah melakukan pemilihan, maka pemilih tidak dapat melakukan pemilihan kembali atau memperbaiki hasil pilihannya tetapi hanya dapat mengecek siapa calon yang dipilih dengan memasukkan *password* pemilih yang tampilannya dapat dilihat pada Gambar 15.

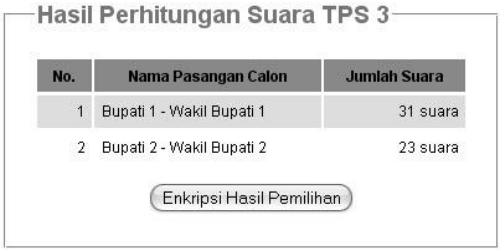


Gambar 14. Halaman pemilihan.

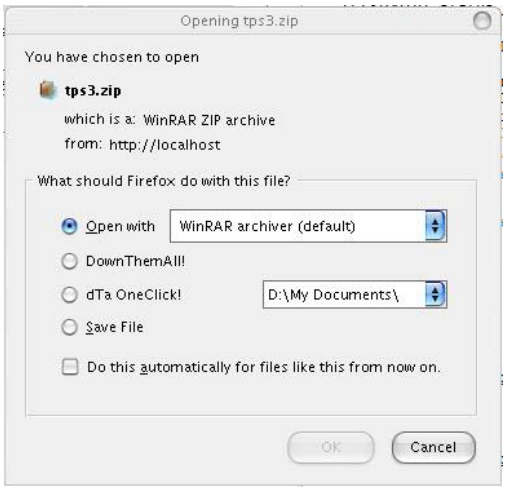
Gambar 15. Pilihan pemilih.

5. Implementasi Sistem Perhitungan Suara

Implementasi sistem perhitungan suara dibagi menjadi dua, yaitu perhitungan pada TPS ke kelurahan dan perhitungan kelurahan ke pusat. Halaman untuk perhitungan suara di TPS dapat dilihat pada Gambar 16. Setelah panitia menekan tombol “Enkripsi Hasil Pemilihan”, maka sistem akan membuat file hasil perhitungan yang dapat diunduh seperti pada Gambar 17. Setelah file enkripsi hasil perhitungan di masing-masing TPS diunduh oleh panitia, selanjutnya file tersebut akan dibawa ke perhitungan kelurahan yang akan didekripsi terlebih dahulu oleh sistem yang dapat dilihat pada Gambar 18.

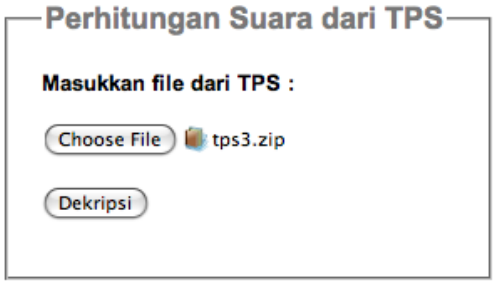


Gambar 16. Halaman perhitungan suara di TPS.



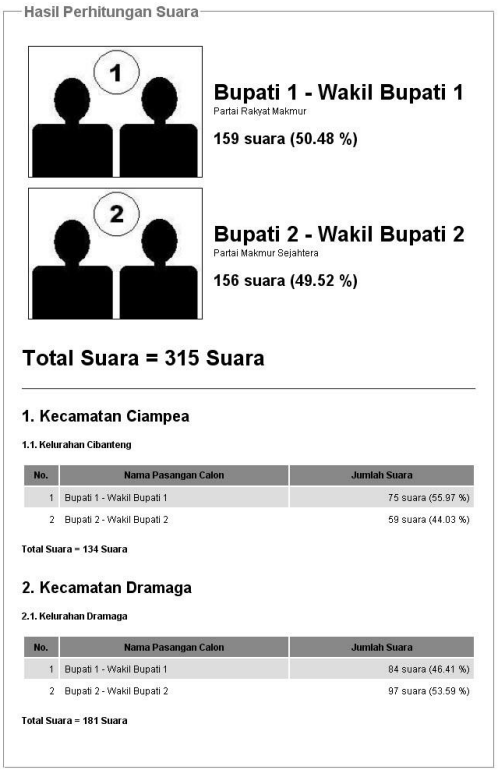
Gambar 17. File enkripsi hasil perhitungan di TPS

Setelah perhitungan suara di kelurahan selesai, selanjutnya adalah perhitungan suara total dimana sistem di kelurahan akan mengirimkan hasil perhitungannya ke pusat. Gambar 19 menunjukkan halaman untuk pengiriman hasil perhitungan ke pusat setelah panitia menekan tombol “Kirim Hasil Pemilihan”. Setelah perhitungan selesai, sistem akan manampilkan hasil perhitungan total beserta hasil perhitungan pada masing-masing kelurahan yang dapat dilihat pada Gambar 20.



Gambar 18. Dekripsi hasil perhitungan suara dari TPS

Gambar 19. Halaman hasil perhitungan di kelurahan



Gambar 20. Halaman hasil perhitungan suara total

Analisa Keamanan Sistem

Fitur Keamanan sistem yang diterapkan pada sistem *e-voting* ini meliputi:

1. Penerapan *Captcha*

Penerapan *captcha* digunakan untuk mencegah pengisian *form* seperti pendaftaran secara otomatis yang dilakukan mesin atau program karena tidak ada program komputer yang bisa membaca susunan teks seperti manusia. Penerapan *captcha* ini juga digunakan untuk mencegah pembobolan pada halaman *login* yang dapat dilakukan oleh program komputer seperti metode *brute force* yang mencoba menebak *id* dan *password* secara acak dengan segala kemungkinan kombinasi karakter, tetapi metode tersebut tidak bisa membaca

captcha. Pada halaman pemilihan juga diterapkan *captcha* yang bertujuan mencegah pemilihan otomatis oleh program komputer, jadi setiap pemilih yang hendak memilih harus memasukkan *captcha* pada pilihannya.

2. Penggunaan *Session*

Session digunakan pada setiap halaman untuk mengecek apakah setiap pengunjung yang mengakses halaman itu mempunyai hak atau tidak, jika pengunjung tidak berhak maka sistem tidak akan mengizinkan pengunjung untuk mengakses halaman tersebut. Untuk halaman pemilih hanya dapat dilihat oleh pemilih yang sudah *login* ke sistem begitu juga untuk halaman *administrator*. Setiap *session* yang dibuat akan selalu dicocokkan dengan basis data, sehingga jika ada pengunjung yang menggunakan *session* palsu maka tetap tidak akan bisa mengakses halaman *e-voting*.

Fungsi untuk pengecekan *session* untuk mengecek *login* pemilih dan *administrator* dapat dilihat pada Gambar 21. Fungsi *isLogin()* dan *isAdmin()* akan digunakan pada setiap halaman yang membutuhkan autentikasi pengunjung.

3. Penerapan Algoritme Kunci Publik, Kunci Simetri, dan Fungsi *Hash*

Penerapan algoritme dan fungsi hash ini digunakan untuk mengenkripsi dan dekripsi data yang digunakan pada data *login* pemilih, pilihan pemilih, dan pengiriman hasil perhitungan untuk menjaga kerahasiaan dan keamanan data. Penerapan algoritme kunci publik menggunakan algoritme RSA, untuk algoritme kunci simetri menggunakan algoritme *twofish*, dan fungsi *hash* menggunakan SHA-512.

Algoritme RSA dapat membuat kunci publik, kunci privat, dan modulo secara otomatis ketika pemilih melakukan pendaftaran yang selanjutnya kunci privat akan dienkripsi oleh algoritme *twofish* menggunakan kunci dari password pemilih sehingga pemilih mudah untuk mengingatnya. Algoritme RSA ini digunakan untuk melakukan enkripsi pada saat pemilih melakukan pemilihan, yaitu calon yang dipilih akan dienkripsi oleh kunci publik pemilih dan disimpan dalam basis data sehingga hanya pemilih saja yang tahu pilihannya dengan cara memasukkan *password* yang akan mendekripsi kunci privat dengan algoritme *twofish* kemudian pilihan pemilih akan didekripsi menggunakan kunci privatnya. Fungsi *hash* digunakan pada saat pendaftaran untuk mendapatkan nilai hash dari *password* yang dimasukkan pemilih yang akan disimpan dalam basis data.

4. Pengecekan Karakter pada Saat *Login*

Pengecekan karakter pada saat *login* digunakan untuk menahan serangan dari SQL *Injection*. Jadi ketika *login* terdapat masukan karakter aneh seperti karakter tanda kutip satu, kutip dua atau karakter persen, maka sistem akan memberikan peringatan kesalahan.

```
function isLogin()
{
    session_start();
    if(session_is_registered("id_pemilih") and
session_is_registered("no_ktp") and
session_is_registered("nama") and
session_is_registered("password")) {
        if(!empty($_SESSION['id_pemilih']) and
!empty($_SESSION['no_ktp']) and
!empty($_SESSION['nama']) and
!empty($_SESSION['password'])) {
            $pemilih = mysql_num_rows(query("select id from
pemilih where id='$_SESSION[id_pemilih]' and
no_ktp='$_SESSION[no_ktp]' and
nama='$_SESSION[nama]'"));
            $login = mysql_num_rows(query("select
id_pemilih from login where
id_pemilih='$_SESSION[id_pemilih]' and
password='$_SESSION[password]'"));
            if($pemilih and $login)
            return true;
            else
            return false;
        }
        else
        return false;
    }
    else
    return false;
}
```

Gambar 2. Fungsi pengecekan *login* pemilih menggunakan *session*.

SIMPULAN

Pemilihan kepala daerah di Indoensia saat ini menggunakan kertas suara yang membutuhkan banyak sumber daya, tenaga, dan waktu terutama dalam proses perhitungan suara. Dengan menggunakan pemilihan secara digital atau *electronic voting* (*e-voting*) dapat menghemat waktu dan tenaga yang digunakan terutama dalam proses perhitungan suara. Penelitian ini berhasil menerapkan sistem *e-voting*yang terdiri dari sistem pendaftaran, validasi dan pengaktifan pemilih, *login*/masuk ke sistem, sistem pemilihan, dan sistem perhitungan suara. Penerapan tersebut dalam bentuk simulasi komputer yang dibangun menggunakan bahasa pemrograman PHP dan dijalankan melalui *web browser.*

DAFTAR PUSTAKA

Ahn L. von, Blum M, Langford J. 2004*. Telling Humans And Computers Apart Automatically*. Communications Of The ACM.

Azhari R. 2005. *E-voting*. Depok: UI.

Boneh D. 1999.*Twenty Years of attacks on the RSA Cryptosystem*. Notices of the American Mathematical Society (AMS).

Canard S, Sibert H. 2001. *How to fit cryptographic e-voting into smart cards*. Perancis: IOS Press.

Guritman S. 2003. *Pengantar Kriptografi.* Bogor: IPB

McLeod R. 2004. *Management Information System*. New Jersey: Pearson Education Inc.

Schneier B *et al*. 1998. *Twofish: A 128-Bit Block Cipher.* USA