APLIKASI *SECURE e-ELECTION* DENGAN MEMANFAATKAN FUNGSI KRIPTOGRAFI DAN TEKNOLOGI *FINGERPRINT* UNTUK MENDUKUNG *e-DEMOCRACY*

Panji Yudha Prakasa[1)], Ikhsan Budiarso[2)], Esti Rahmawati Agustina[3)]
[1,2,3)]Lembaga Sandi Negara RI, Jl. Haryono RM No 70, Ragunan, Pasar Minggu, Jaksel
Email : panji.prakasa@yahoo.co.id[1)] san_crypto3@yahoo.co.id[2)] rahma_cryptn@yahoo.co.id[3)]

Abstrak
Proses Pemilihan Umum (Pemilu) seperti Pemilihan Kepala Daerah (Pilkada), Pemilihan Legislatif (Pileg), dan Pemilihan Presiden (Pilpres) di Indonesia dewasa ini masih rawan kecurangan untuk kepentingan salah satu golongan, seperti yang terindikasi kuat terjadi pada beberapa Pilkada yang telah dilaksanakan. Hal ini terjadi karena terdapat beberapa titik dalam tahapan Pemilu yang berpotensi besar bisa dilakukan berbagai macam kecurangan. Kecurangan ini bisa berupa manipulasi data pada saat proses pengiriman hasil penghitungan suara di Tempat Pemungutan Suara (TPS) untuk direkapitulasi di tingkat Panitia Pemilihan Kecamatan (PPK). Hal lain yang dapat dimanfaatkan adalah adanya sisa kertas suara yang juga berpotensi menimbulkan praktik curang. Secara sistem juga belum dapat dibuktikan seorang pemilih benar-benar melakukan pemilihan di sebuah TPS. Sistem yang berlaku sekarang, petugas KPPS-lah yang mencatat kehadiran seorang pemilih.
Dengan berbagai potensi kecurangan tersebut, sudah saatnya kita berupaya untuk mengatasi dan mencegah hal-hal tersebut terjadi pada pemilihan yang akan datang. Pemerintah telah membentuk Panitia Pengawas Pemilu (Panwaslu) untuk meminimalisir terjadinya berbagai kecurangan dalam Pemilu. Namun demikian, tetap harus ada perbaikan terkait dengan sistem pemilihan yang selama ini digunakan dan masih dilakukan secara manual (by paper). Dengan memanfaatkan kemajuan teknologi, sistem Pemilu di Indonesia dapat dilakukan secara elektronik. Penerapan sistem Pemilu secara elektronik dapat memberikan berbagai kemudahan dan keuntungan dibandingkan dengan pemilihan secara manual. Namun, dibalik kemudahan dan keuntungan yang diberikan belum tentu sistem pemilihan secara elektronik itu aman. Dengan demikian harus ada suatu jaminan keamanan terhadap sistem tersebut. Salah satu cara untuk memberikan jaminan keamanan sistem adalah dengan menerapkan fungsi kriptografi pada sistem pemilihan elektronik tersebut sehingga mampu mengatasi kerawanan kecurangan yang mungkin terjadi.
Aplikasi Secure e-election merupakan konsep Pemilu secara elektronik yang menerapkan fungsi kriptografi dan mendukung azas Pemilu yaitu Langsung, Umum, Bebas, Rahasia, Jujur, dan Adil (LUBER JURDIL). Aplikasi ini terdiri dari aplikasi pendaftaran pemilih, aplikasi pemungutan suara, aplikasi pengecekan pilihan serta aplikasi web untuk mengakses daftar pemilih dan hasil pemilu. Fitur yang terdapat dalam aplikasi ini adalah database online yang memuat daftar pemilih se-Indonesia dan hasil pemilihan serta otentikasi pemilih dilakukan dengan menggunakan fingerprint sehingga memungkinkan pemilih melakukan pemilihan di TPS manapun.

Kata kunci: Pemilu, kriptografi, *secure e-Election, fingerprint, e-Democracy*

1. PENDAHULUAN

Pada awalnya pemilihan umum dilaksanakan untuk pemilihan anggota DPR, DPD, dan DPRD. Pada tahun 2004 dilaksanakan Pemilihan Umum Presiden dan wakil presiden untuk pertama kalinya, kemudian pada tahun 2005 dilaksanakan pemilihan kepala daerah untuk pertama kalinya juga.

Proses Pemilihan Umum (Pemilu) seperti Pemilihan Kepala Daerah (Pilkada), Pemilihan Legislatif (Pileg), dan Pemilihan Presiden (Pilpres) di Indonesia dewasa ini masih rawan kecurangan untuk kepentingan salah satu golongan, seperti yang terindikasi kuat terjadi pada beberapa Pilkada yang telah dilaksanakan. Hal ini terjadi karena terdapat beberapa titik dalam tahapan Pemilu yang berpotensi besar bisa dilakukan berbagai macam kecurangan. Kecurangan ini bisa berupa manipulasi data pada saat proses pengiriman hasil penghitungan suara di Tempat Pemungutan Suara (TPS) untuk direkapitulasi di tingkat Panitia Pemilihan Kecamatan (PPK). Hal lain yang dapat dimanfaatkan adalah adanya sisa kertas suara yang juga berpotensi menimbulkan praktik curang. Secara sistem juga belum dapat dibuktikan seorang pemilih benar-benar melakukan pemilihan di sebuah TPS. Sistem yang berlaku sekarang, petugas KPPS-lah yang mencatat kehadiran seorang pemilih.

Dengan berbagai potensi kecurangan yang disebutkan di atas, sudah saatnya kita berupaya untuk mengatasi dan mencegah hal-hal tersebut terjadi pada pemilihan yang akan datang. Pemerintah telah membentuk Panitia Pengawas Pemilu (Panwaslu) untuk meminimalisir terjadinya berbagai kecurangan dalam Pemilu. Namun demikian, tetap harus ada perbaikan terkait dengan sistem pemilihan yang selama ini digunakan dan masih dilakukan secara *manual* (*by paper*).

Dengan memanfaatkan kemajuan teknologi, sistem pemilu di Indonesia dapat dilakukan secara elektronik. Pemilihan secara elektronik ini kita kenal dengan nama *e-election.* Beberapa negara maju dan berkembang seperti Finlandia, Lithuania, Brasil, dan India telah menerapkan pemilihan secara elektronik dalam bentuk *e-voting*. Dalam beberapa tahun kedepan, melalui program USO (*Universal Service Obligation*) pemerintah akan menyediakan fasilitas akses komunikasi suara dan data hingga menjangkau seluruh desa di tanah air sehingga *e-election* semakin berpeluang untuk diterapkan. [7]

Pemanfaatan teknologi di berbagai ranah kehidupan manusia layaknya pisau bermata dua. Dalam penerapan teknologi sistem Pemilu secara elektronik dapat memberikan berbagai kemudahan dan keuntungan dibandingkan dengan pemilihan secara manual. Namun, dibalik kemudahan dan keuntungan yang diberikan belum tentu sistem pemilihan secara elektronik itu aman. Dengan demikian harus ada suatu jaminan keamanan terhadap sistem tersebut. Salah satu cara untuk memberikan jaminan keamanan sistem adalah dengan menerapkan fungsi kriptografi pada sistem pemilihan elektronik tersebut sehingga mampu mengatasi kerawanan kecurangan yang mungkin terjadi.

Dengan latar belakang yang telah dikemukakan maka permasalahan yang diangkat dalam paper ini adalah bagaimana membangun aplikasi *secure e-election* dengan memanfaatkan fungsi kriptografi dan teknologi *fingerprint* untuk mendukung e-*democracy*.

2. TINJAUAN PUSTAKA

a. e-election

Merupakan kependekan dari *electronic election*, *e-electio*n merupakan proses pemilihan umum yang melibatkan kecanggihan teknologi informasi.[6]

b. Kriptografi

1) Pengertian

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu *cryptos* artinya rahasia (*secret*) dan *graphein* artinya tulisan (*writing*) [3]. Jadi kriptografi berarti tulisan rahasia (*secret writing*). Kriptografi merupakan studi tehnik matematika yang berkaitan dengan aspek kemanan informasi.[1]

2) Layanan Kriptografi [3]

Layanan yang diberikan kriptografi dalam mendukung keamanan informasi adalah:

a) Kerahasiaan (*Confidentialit*y)

Merupakan aspek pencegahan penyingkapan informasi kepada pihak yang tidak memiliki hak terhadap infomasi tersebut. Aspek ini dapat disediakan dengan kriptografi yaitu dengan menyandi (*encrypt*) informasi tersebut.

b) Integritas (*Integrity*)

Merupakan aspek pencegahan perubahan informasi oleh pihak yang tidak memiliki otoritas untuk merubah informasi tersebut. Untuk memenuhi kebutuhan ini haruslah dapat untuk mendeteksi perubahan informasi, yaitu penyisipan, penghapusan, dan penggantian. Salah satu cara untuk menyediakan aspek ini dengan kriptografi adalah menggunakan fungsi hash.

c) Otentikasi (*Authentication*)

Merupakan aspek menjamin informasi tersebut adalah asli. Juga untuk menjamin keabsahan orang-orang yang terlibat dalam pertukaran informasi. Aspek ini dapat disediakan dengan kriptografi menggunakan algoritma kunci simetrik maupun algoritma kunci asimetrik.

d) Nir penyangkalan (*Non-repudiation*)

Merupakan aspek menjamin agar pihak-pihak yang terlibat tidak dapat menyangkal dikemudian hari. Untuk menyediakan aspek ini dengan kriptografi dapat menggunakan algoritma tanda tangan digital (*digital signature algorithm*).

3) Algoritma Kriptografi

Algoritma kriptogafi adalah langkah-langkah atau tahapan dalam melakukan proses pengubahan teks terang menjadi teks sandi. Secara umum, algoritma kriptografi dibagi menjadi 2 (dua), yaitu algoritma enkripsi/penyandian dan algoritma *has*h.

4) Protokol Kriptografi

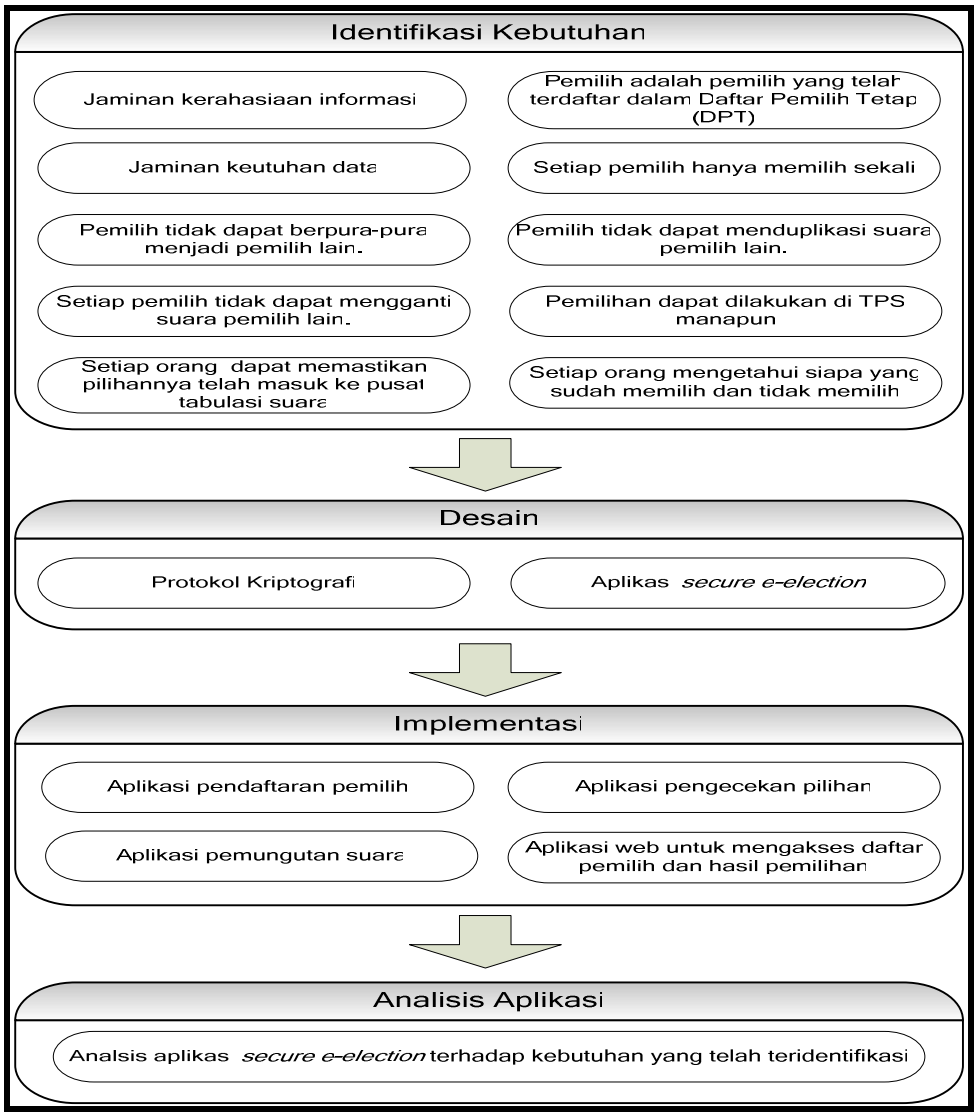
Protokol merupakan serangkaian langkah, melibatkan dua pihak atau lebih, didesain untuk menyelesaikan sebuah pekerjaan. Protokol kriptografi adalah potokol yang menggunakan kriptografi. Agar dapat menggunakan kriptografi dalam menyelesaikan persoalan keamanan informasi, haruslah diperhatikan protokol kriptografi yang berhubungan dengan aspek kemanan informasi yang ingin disediakan [3]. Contoh protokol kriptografi untuk penyandian, protokol kriptografi untuk otentikasi, protokol untuk pertukaran kunci, protokol *secure e-election* dan sebagainya.

c. Fingerprint [1]

Dalam bahasa Indonesia, *fingerprint* diartikan sebagai sidik jari. Setiap orang, termasuk mereka yang terlahir kembar identik, memiliki pola sidik jari yang khas untuk diri mereka masing-masing, dan berbeda satu sama lain. Dengan kata lain, tanda pengenal manusia tertera pada ujung jari mereka. Sistem pengkodean ini dapat disamakan dengan sistem kode garis (*barcode*) sebagaimana yang digunakan saat ini. Kegunaan *fingerprint* ini adalah untuk autentikasi dalam berbagai aplikasi.

3. METODE PENELITIAN

Metode penelitian yang digunakan yaitu model proses, yang dijelaskan pada gambar 1:

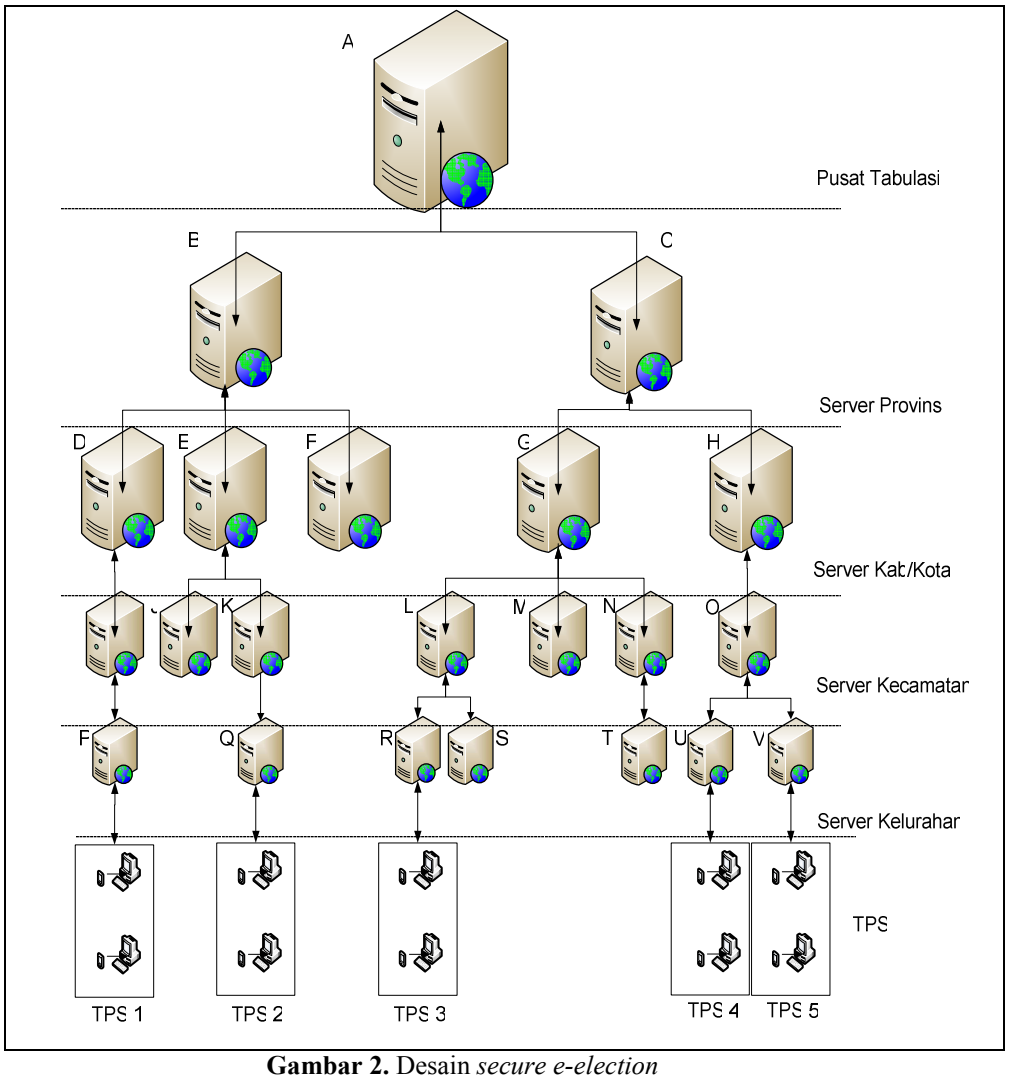


Gambar 1. Metode Penelitian

4. PEMBAHASAN

a. Mekanisme *secure e-election*

Sebagaimana yang telah dijelaskan dalam bagian pendahulan, bahwa dengan menggunakan aplikasi *secure e-election*, pemilih tidak lagi harus memilih pada TPS di mana ia terdaftar. Namun, pemilih dapat langsung memilih pada TPS manapun di Indonesia.



Gambar 2. Desain *secure e-election*

Gambar 2 menjelaskan ilustrasi dari mekanisme dan tahapan aliran data (*data flow*) pada aplikasi *secure e-election*.

Berikut beberapa contoh kasus yang dapat menjelaskan mekanisme *secure e-election* :

1) Pemilih terdaftar dan memilih pada TPS dimana pemilih tersebut terdaftar.
   Misalkan pemilih terdaftar pada TPS 1 dan memilih pada TPS1 juga, maka aliran datanya (*data flow*) adalah sebagai berikut:
   - Alur Verifikasi Pemilih.
     TPS 1 - *Server* Kelurahan P - TPS 1.
   - Alur Penyampaian Hasil Pemilihan
     TPS 1 - *Server* Kelurahan P - *Server* Kecamatan I - *Server* Kab/Kota D - *Server* Provinsi B - Pusat Tabulasi A.
   - Alur peng-*update*-an *database.*
     Pusat Tabulasi A - *Server* Provinsi B - *Server* Kab/Kota D - *Server* Kecamatan I - *Server* Kelurahan P.
2) Pemilih terdaftar di suatu TPS tetapi memilih pada TPS lain yang masih berada pada Kecamatan yang sama.
   Misalkan pemilih terdaftar pada TPS 4, tetapi memilih pada TPS 5. Maka aliran datanya (*data flow*) adalah sebagai berikut:
   - Alur Verifikasi Pemilih
     TPS 5 - *Server* Kelurahan V - *Server* Kecamatan O - *Server* Kelurahan V -TPS 5.
   - Alur Penyampaian Hasil Pemilihan
     TPS 5 - *Server* Kelurahan V - *Server* Kecamatan O - *Server* Kab/Kota H - *Server* Provinsi C - Pusat Tabulasi A.

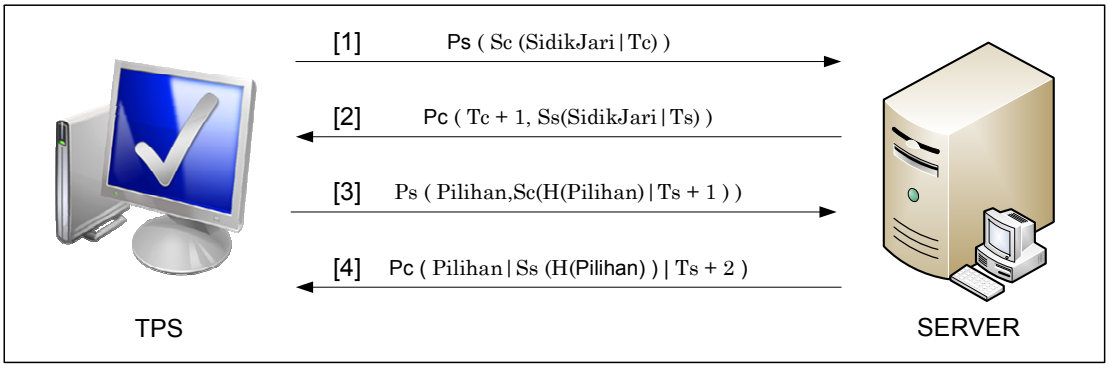
- Alur peng-*update*-an database.
  Pusat Tabulasi A - *Server* Provinsi C - *Server* Kab/Kota H - *Server* Kecamatan O - *Server* Kelurahan U.

3) Pemilih terdaftar di suatu TPS tetapi memilih pada TPS lain yang berbeda Propinsi.
   Misalkan pemilih terdaftar pada TPS 2, tetapi memilih pada TPS 3. Maka aliran datanya (*data flow*) adalah sebagai berikut:
   - Alur Verifikasi Pemilih
     TPS 3 - *Server* Kelurahan R - *Server* Kecamatan L - *Server* Kab/Kota G - *Server* Provinsi C - Pusat Tabulasi A - *Server* Provinsi C - *Server* Kab/Kota G - *Server* Kecamatan L - *Server* Kelurahan R – TPS 3.
   - Alur Penyampaian Hasil Pemilihan
     TPS 3 - *Server* Kelurahan R - *Server* Kecamatan L - *Server* Kab/Kota G - *Server* Provinsi C - Pusat Tabulasi A.
   - Alur peng-*update*-an database.
     Pusat Tabulasi A - *Server* Provinsi B - *Server* Kab/Kota E - *Server* Kecamatan K - *Server* Kelurahan Q.

Adapun tahapan pelaksanaan pemilihan dengan menggunakan aplikasi *secure e-election* adalah sebagai berikut:

- Setiap warga negara Indonesia yang telah memenuhi persyaratan berdasarkan UU Nomer 10 Tahun 2008 akan diregistrasi oleh petugas KPUD sebagai Pemilih dan dicantumkan dalam Daftar Pemilih Tetap (DPT). Proses registrasi ini meliputi pendataan dan pengambilan *fingerprint* pemilih.
- Data pemilih dan *fingerprint*-nya akan disimpan pada setiap *server* (*server* Kelurahan, *server* Kecamatan, *server* Kab/Kota, *server* Provinsi, *server* Pusat Tabulasi).
- Pada pelaksanaan pemilihan, dengan menggunakan aplikasi *secure e-election*, pemilih yang telah terdaftar pada DPT dapat langsung menyalurkan aspirasinya dengan mendatangi salah satu TPS dimanapun.
- Setelah melakukan proses pemilihan, pemilih langsung dapat memverifikasi suaranya telah masuk ke dalam Pusat Tabulasi Suara.

b. Protokol *secure e-election*



Gambar 3. Desain Protokol *secure e-election*

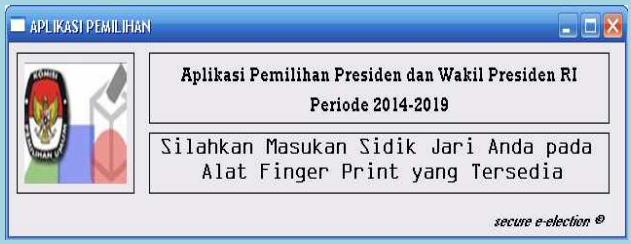
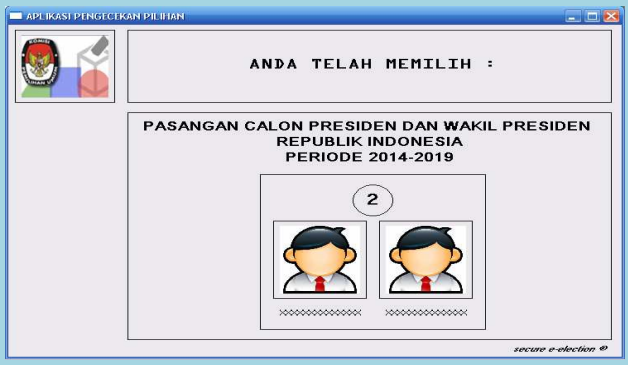
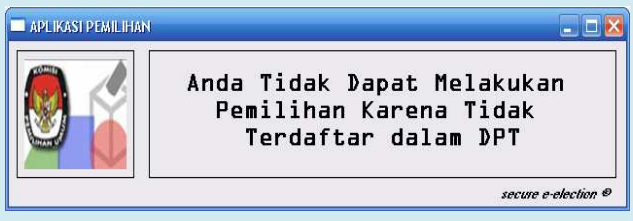
Penjelasan gambar 3 yaitu sebagai berikut :

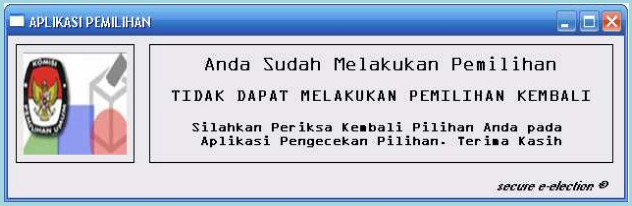
1) Pemilih melakukan *login* aplikasi di TPS dengan memasukkan sidik jari pada *fingerprint reader*. Kemudian aplikasi akan melakukan enkripsi terhadap *timestamp Tc* dan sidik jari dengan menggunakan kunci privat TPS. Setelah itu mengirimkan *Sc (SidikJari, Tc)* kepada *server* secara terenkripsi dengan menggunakan kunci public *server*.
2) *Server* akan memverifikasi sidik jari dengan *database server*. Kemudian *server* akan melakukan enkripsi terhadap *timestamp Ts* dan sidik jari dengan menggunakan kunci privat *server*. Setelah itu mengirimkan *Ss (SidikJari | Ts)* bersamaan dengan *timestamp Tc + 1* yang dikirim oleh TPS secara terenkripsi dengan menggunakan kunci publik TPS.
3) TPS akan memverifikasi *timestamp Tc* yang dikirimkan dengan *timestamp Tc + 1* yang diterima dari *server*. Jika *timestamp* sesuai, maka pilihan akan dikirimkan kepada *server* secara terenkripsi bersamaaan dengan hasil enkripsi terhadap *hash* dari pilihan dan *timestamp* Ts +1.

ISSN: 1979-2328

4) *Server* merespon hasil pilihan dengan membuat *digital signature* terhadap pilihan *Ss(H(Pilihan))* tersebut dan mengirimkannya secara terenkripsi bersamaan dengan *Pilihan* dan *timestamp Ts + 2*. Kemudian TPS akan memverifikasi hasil dekripsi *digital signature H(Pilihan)* dengan hasil *hash Pilihan* dan *timestamp* yang dikirim dengan *Ts + 2* yang diterima.

c. Analisis Aplikasi

Identifikasi Kebutuhan	Pembuktian
Jaminan kerahasiaan informasi	Aplikasi *secure e-election* mengimplementasikan algoritma enkripsi RSA 1024 bit.
Jaminan keutuhan data	Aplikasi *secure e-election* mengimplementasikan algoritma *hash* SHA-1.
Pemilih tidak dapat berpura-pura menjadi pemilih lain.	Aplikasi *secure e-election* memanfaatkan *fingerprint* untuk melakukan pemilihan. 
Setiap pemilih tidak dapat mengganti suara pemilih lain.	Aplikasi *secure e-election* memanfaatkan *fingerprint* untuk melakukan pemilihan.
Setiap orang dapat memastikan pilihannya telah masuk ke Pusat Tabulasi Suara	Aplikasi *secure e-election* akan menampilkan hasil pilihan yang telah masuk dalam Pusat Tabulasi Suara. 
Pemilih adalah pemilih yang telah terdaftar dalam Daftar Pemilih Tetap (DPT)	Aplikasi *secure e-election* akan menampilkan peringatan seperti gambar berikut jika pemilih tidak terdaftar dalam DPT. 

Setiap pemilih hanya memilih sekali	Aplikasi *secure e-election* akan menampilkan peringatan seperti gambar berikut jika pemilih melakukan pemilihan untuk yang kedua kalinya. 
Pemilih tidak dapat menduplikasi suara pemilih lain.	Aplikasi *secure e-election* telah mengimplementasikan protokol kriptografi yang memnfaatkan *timestamp* untuk mencegah adanya duplikasi pilihan.
Pemilihan dapat dilakukan di TPS manapun	Aplikasi *secure e-election* memanfaatkan *fingerprint* untuk otentikasi pemilih secara *online* dan *database server* dapat diakses oleh TPS manapun sehingga pemilih dapat melakukan pemilihan di TPS manapun.
Setiap orang mengetahui siapa yang sudah memilih dan tidak memilih	Hasil pemilihan dapat diakses melalui situs KPU, seperti gambar berikut: 

Kelebihan aplikasi *secure e-election* bila dibandingkan dengan sistem pemilu saat ini adalah sebagai berikut :

1) Pemilihan dapat dilakukan di TPS manapun secara *online*.
2) Otentikasi pemilih menggunakan *fingerprint* sehingga dapat meminimalisir kecurangan, yaitu duplikasi suara dan melakukan pemilihan ganda serta secara sistem dapat membukitan bahwa seorang pemilih telah benar-benar melakukan pemilihan.
3) Memanfaatkan teknik kriptografi untuk mendukung keamanan informasi yaitu *confidentiality* (kerahasiaan), *integrity* (keutuhan data), *authentication* (otentikasi), dan *non-repudiation* (tidak ada penyangkalan).
4) Hasil pemilihan dapat diketahui lebih cepat.
5) Pemilih dapat memastikan bahwa pilihannya telah masuk dalam pusat tabulasi suara.

5. KESIMPULAN

Aplikasi *secure e-election* merupakan sistem pemilihan umum elektonik yang didesain untuk dapat melakukan pemilihan di TPS manapun secara *online*. Aplikasi ini menggunakan *fingerprint* untuk otentikasi pemilih sehingga dapat meminimalisir kecurangan, yaitu duplikasi suara dan melakukan pemilihan ganda serta secara sistem dapat membukitan bahwa seorang pemilih telah benar-benar melakukan pemilihan. Selain itu aplikasi ini memanfaatkan teknik kriptografi untuk mendukung keamanan informasi yaitu *confidentiality* (kerahasiaan), *integrity* (keutuhan data), *authentication* (otentikasi), dan *non-repudiation* (tidak ada penyangkalan)

6. PENELITIAN SELANJUTNYA

Pada paper ini masih terdapat keterbatasan sehingga perlu dilakukan penelitian selanjutnya yaitu analisis matematis terhadap protokol *secure e-election* yang digunakan dan pengamanan data pada *server*.

7. DAFTAR PUSTAKA

[1] Agustina, Esti Rahmawati dan Kurniati, Agus. 2007. *DNA Fingerprint sebagai Solusi Kelemahan Biometrik Fingerprint*
[2] Menezes, Alfred J., Van Ooschot, Paul C., Vanstone, Scott A. 1997. *Handbook of Applied Cryptography*. Boca Raton: CRC press LLC
[3] Munir, Rinaldi. 2006. *Kriptografi.* Informatika : Bandung
[4] Schneier, Bruce. 1996. *Applied Cryptography : Protocols, Algorithms, and Source Code in C Second Edition*. John Wiley & Sons, Inc. New York.
[5] Stallings, William. 2005. *Cryptography and Network Security Principles and Practices, Fourth Edition*. Upper Saddle River, NJ : Prentice Hall.
[6] http://sipemilu.org/ti-kpu/10-riset-e-voting/ (akses terakhir 9 Mei 2009)
[7] http://www.syamsulbahrum.web.id/politik/?p=792 (akses terakhir 7 Mei 2009)