Implementasi Kontrol Integritas E-Kiosk untuk Pengamanan Sistem Pemungutan Suara secara Elektronik (*E-Voting*)

Ishom Muhammad Drehem, Supeno Djanali, dan Baskoro Adi Pratomo
Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111 Indonesia
e-mail: supeno@its.ac.id

Abstrak—**Pemungutan suara dalam pemilu di Indonesia masih dilakukan secara manual, yaitu menggunakan media kertas. Dalam sistem tersebut, terjadi risiko kesalahan yang tinggi dalam penghitungan suara mengingat surat suara yang diproses terbilang banyak. Selain itu, rawan terjadi kecurangan terhadap jumlah suara demi memenangkan kelompok atau golongan tertentu. Akibatnya, pelaksanaan pemilu menjadi tidak sesuai dengan asas yang berlaku dan hasilnya tidak akurat. Untuk mengatasinya, dirancanglah sistem pemungutan suara yang lebih modern, yang disebut dengan sistem pemungutan suara secara elektronik (e-voting). Sistem e-voting menggunakan e-kiosk yang memudahkan pemilih dalam memberikan suaranya karena tidak perlu mencoblos dan memasukkan kertas ke dalam kotak kertas suara. Selain itu, faktor integritas data dan keamanan data pemilih lebih aman karena menggunakan metode enkripsi dan transmisi data yang aman. Pada tugas akhir ini, penulis menggunakan dua skenario, yaitu uji fungsionalitas dan uji keamanan data. Dari sisi fungsionalitas, sistem aplikasi yang dibuat sesuai dengan kebutuhan pengguna yaitu dari sisi admin. Terdapat enam fungsionalitas, yaitu cek koneksi untuk servis pengirman SMS, generate token untuk mendapatkan token melalu servis pengiriman SMS,, muat kunci untuk metode pengiriman data menggunakan XML, rekap data pemilih untuk memantau hasil pemilihan partai dan anggota legistlatif pada hari itu juga, tanda tangan saksi dan KPPS, serta kirim data suara dari server lokal menuju server pusat. Sedangkan dari sisi keamanan data, sistem aplikasi mengamanakan data menggunakan metode hash dan enkripsi data untuk dikirimkan menuju server pusat. Yang diamankan adalah data suara basis data. Kemungkinan besar basis data tersebut dapat digunakan oleh admin untuk mengubah data. Skenario yang dirancang tersebut terbukti dapat mengamankan sistem e-voting. Diharapkan skenario tersebut dapat diterapkan pada penggunaan sistem e-voting yang sebenarnya di masa mendatang.**

***Kata Kunci*— Pemilu, Elektronik Voting (E-Voting), E-Kiosk, Metode Enkripsi, Pengamanan Aplikasi.**

I. PENDAHULUAN

INDONESIA adalah negara yang menganut demokrasi dan menjunjung tinggi kedaulatan rakyatnya. Sarana pelaksanaannya adalah pemilihan umum/pemilu. Tujuan adanya pemilu adalah memilih para wakil rakyat untuk duduk di parlemen dan para pemimpin di tingkat nasional, di daerah, maupun di desa. Berdasarkan Pasal 22E ayat (1) UUD 1945, asas pemilu yang berlaku adalah langsung, umum, bebas, rahasia, jujur, dan adil (Luber Jurdil) [1] [2].

Pelaksanaan pemilu saat ini masih bersifat manual. Proses pemungutan dan penghitungan suara yang dilakukan masih bersifat manual dengan menggunakan kertas surat suara. Pelaksanaan semacam ini memiliki kelemahan-kelemahan, antara lain (1) tingginya risiko kesalahan penghitungan suara mengingat banyaknya jumlah surat suara yang harus dihitung dan (2) rawan terjadi kecurangan terhadap jumlah suara untuk kepentingan partai atau golongan tertentu. Akibatnya, kualitas pelaksanaan pemilu dan kepercayaan rakyat terhadap hasil pemilu menurun.

Salah satu solusi untuk mengatasi kelemahan-kelemahan tersebut adalah dengan melaksanakan sistem pemilu yang lebih modern, yang dikenal dengan *e-voting* [3]. Dalam perancangannya, faktor keamanan dengan beberapa aspek seperti *authenticity* (sistem hanya dapat diakses oleh rakyat yang terdaftar sebagai pemilih), *confidentiality* (kerahasiaan), dan *integrity* (jaminan terhadap keaslian suara pemilih) harus diperhatikan untuk mendukung pelaksanaan yang berdasarkan asas pemilu yang berlaku. Untuk beralih menggunakan sistem *e-voting*, diperlukan kesiapan yang matang dari berbagai faktor pendukungnya, mulai dari rancangan sistem, infrastruktur, dan sumber daya manusia yang mumpuni. Dalam masa peralihan tersebut, dapat dilaksanakan pemilu yang menggunakan kombinasi sistem manual dan modern. Pemilu semacam itu disebut dengan *e-voting*.

Penulis mengimplementasikan aspek *integrity* dan *confidentiality* pada pemilu dengan menggunakan *e-kiosk* menjadi alternatif utama untuk pemilihan dengan mengenkripsi beberapa data pemilih dan terbukti berhasil meningkatkan kemanan pada sistem tersebut. Penulis juga akan menerapkan sesuai dengan kondisi pemilu yang berada di Indonesia. Harapannya sistem *e-voting* dapat meningkat animo memilih masyarkat dan peningkatan kepercayaan masyarakat terhadap hasil pemilu dan mengurangi kecurangan yang terjadi selama pelaksanaan pemilu.

II. TINJAUAN PUSTAKA

A. *E-Voting*

Electronic voting (*e-voting*) adalah pemilu yang memanfaatkan sarana teknologi informasi atau perangkat

elektronik, di mana sebagian atau seluruh proses pelaksanaannya, mulai dari pendaftaran pemilih, pemungutan suara, hingga penghitungan suara, dilakukan secara digital. Kelebihan yang dimiliki *e-voting* antara lain adalah menghemat biaya pelaksanaan pemilu, mempercepat proses pemungutan dan penghitungan suara, serta risiko kesalahan teknis yang kecil. Tujuan penggunaan *e-voting* tidak hanya sekadar mempercepat proses pemungutan dan penghitungan suara saja, tetapi yang lebih penting adalah untuk menjaga keaslian suara pemilih, kerahasiaan pemilih, dan juga menjaga akurasi penghitungan suara [7].

B. Sistem Kriptografi RSA

Sistem kriptografi kunci publik atau sering juga disebut dengan kriptografi kunci asimetrik pertama kali diusulkan oleh Diffie dan Hellman pada tahun 1976. Konsep mengenai sistem ini mirip dengan cara kerja kunci gembok. Misalkan ada sebuah peti berisi pesan rahasia, lalu peti itu dikunci dengan gembok yang dimiliki pemilik gembok. Peti terkunci ini dikirim ke penerima yang memiliki kunci untuk membuka gembok. Penerima dapat membuka gembok jika kunci yang dimilikinya merupakan pasangan gembok yang cocok.

Salah satu jenis sistem kriptografi kunci publik adalah sistem kriptografi RSA. RSA dirumuskan oleh tiga orang mahasiswa dari Massachusetts Institute of Technology (MIT): Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1977 RSA menggunakan algoritma enkripsi dan dekripsi yang bersandar pada fungsi satu arah (*one-way function*). Fungsi tersebut dibangun oleh fungsi eksponensial modular. RSA banyak dimanfaatkan untuk proses autentikasi pengguna ke dalam sistem dan *digital signature*.

Algoritma sistem kriptografi RSA diawali dengan tahapan penerima pesan menghasilkan kunci publik dan kunci privat miliknya. Setelah pasangan kunci penerima pesan dihasilkan, maka pengirim pesan dapat menggunakan kunci publik penerima untuk mengirim pesan teks sandi kepada penerima. Akhirnya, setelah pesan teks sandi sampai pada penerima, penerima dapat menggunakan kunci privatnya untuk mengembalikan pesan teks sandi menjadi pesan teks asli.

C. Fungsi Hash SHA-256

Fungsi *hash* adalah fungsi yang masukannya berupa *string* atau pesan dengan panjang sembarang dan keluarannya berupa nilai *hash* (*hash value*) atau pesan sidik dengan panjang tetap yang disebut *digest*/*message digest*. Salah satu cara untuk menghasilkan *digest* adalah dengan memanfaatkan penggunaan fungsi kompresi secara berulang terhadap suatu pesan yang telah dibagi sebelumnya menjadi sejumlah blok pesan. Fungsi *hash* dapat digunakan untuk mewujudkan layanan keamanan jaringan berupa keutuhan data (*data integrity*) dan berguna sebagai parameter yang mengecek ada tidaknya perubahan terhadap data sebelum dan sesudah data itu dikirim atau disebar ke tempat lain dalam satu komputer ataupun melalui jaringan.

Salah satu fungsi *hash* yang menggunakan cara tersebut adalah SHA (*Secure Hash Algorithm*). SHA adalah fungsi *hash* satu arah yang dibuat oleh National Institute of Standards and Technology (NIST). Sampai saat ini SHA memiliki 4 versi, mulai dari SHA-0, SHA-1, SHA-2, dan SHA-3. SHA-2 memiliki beberapa varian, salah satunya adalah SHA-256. SHA-256 adalah fungsi *hash* SHA yang menghasilkan nilai *hash* dengan panjang 256 bit dengan menggunakan iterasi terhadap sejumlah blok pesan yang masing-masing panjangnya 512 bit [8].

D. Basis Data MySQL

Basis data merupakan sekumpulan data-data yang sangat kompleks yang memiliki hubungan satu dengan yang lainnya. Di dalam sebuah *database* data diatur dengan menggunakan sebuah pengelompokan dengan *table*. Pada tabel sendiri juga masih dikelompokkan menjadi beberapa bagian yang berupa *field-field.*

My Structure Query language (MySQL) adalah sebuah sistem manajemen database relasi *(relational database management system)* yang bersifat *open source*, artinya MySQL boleh di download oleh siapa saja,baik versi kode program aslinya *(source code program)* maupun versi binernya *(executable program)* dan bisa digunakan secara (relatif) gratis baik untuk dimodifikasi sesuai dengan kebutuhan seseorang maupun sebagai suatu program aplikasi komputer. Sistem basis data adalah sistem terkomputerisasi yang tujuan utamanya adalah memelihara data yang sudah diolah atau informasi dan membuat informasi tersedia saat dibutuhkan. Pada intinya basis data adalah media untuk menyimpan data agar dapat diakses dengan mudah dan cepat. DBMS adalah satu set program untuk mengakses data yang biasanya menggunakan *QueryStructured Query Language* (SQL). Untuk setiap DBMS yang memiliki konektor sebagai *driver*agar dapat diakses oleh bahasa pemrograman dapat digunakan sebagai tempat penyimpanan data yang persisten

E. GSM.Com.Lib

GSMComm adalah metode pengiriman SMS melalui pengembang perpustakaan atau *library* yang disediakan oleh Visual Studio, bisa menjadi perpustakaan komunikasi yang terdapat didalam GSM. Fungsi dari GSMCom hanya untuk mengirimkan SMS.

III. DESAIN DAN IMPLEMENTASI

A. Perancangan Alur Sistem secara Umum

Gambar 1 menunjukkan alur sistem secara umum. Alur sistem dibagi menjadi bagian (a) proses pemungutan suara dan bagian (b) proses penghitungan suara. Tahapan-tahapan yang terjadi selama proses pemungutan suara adalah:

1) Pemilih datang di Tempat Pemungutan Suara (TPS) sambil membawa tanda pengenalnya berupa Kartu Tanda Penduduk (KTP) dan menuju *admin* untuk mengecek data pada KTP-nya tersebut dengan bantuan perangkat komputer.
2) (a) Jika data pemilih terdapat dalam basis data dan belum pernah memilih sebelumnya, maka pemilih diizinkan masuk TPS. (b) Jika data pemilih tidak terdapat dalam

basis data atau pemilih sudah pernah memilih sebelumnya, maka pemilih tidak diizinkan masuk TPS.

3) Pemilih yang diizinkan masuk TPS menunggu gilirannya dipanggil panitia Kelompok Penyelenggara Pemungutan Suara (KPPS). Setelah pemilih dipanggil, KPPS memberikan surat suara kepada pemilih. Setelah itu pemilih akan mendapatkan nomer token melalui sms yang di kirimkan oleh panitia.
4) Pemilih menuju bilik suara untuk memilih secara online menggunakan e-kiosk.
5) Pemilih meninggalkan TPS.

(a)

Admin dengan *laptop*/PC yang terhubung dengan basis data lokal.

(b)

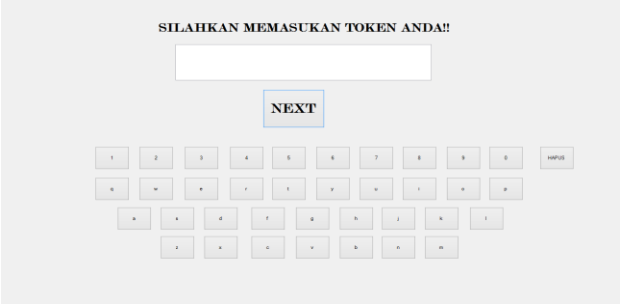
Gambar 1. Alur sistem secara umum: (a) tahap pemungutan suara (b) tahap penghitungan suara

Berikutnya, tahapan-tahapan yang terjadi selama proses pemilihan menggunakan e-kiosk suara adalah:

1) Pemilih setelah mendapatkan sms token, maka pemilih langsung masuk ke bilik yang telah disediakan untuk proses otentikasi sms token di halaman bilik.
2) Setelah masuk ke halaman bilik maka proses selanjutnya adalah pemilih memasukkan sms token ke halaman bilik, ketika sms token valid maka pemilih berhak untuk memilih partai dan memilih anggota legislatif yang didukungnya.
3) Setelah melakukan proses tersebut, pemilih memilih partai, terdapat delapan partai yang sudah disedikan,
4) Setelah memilih partai yang didukung , setelah itu pemilih melakukan pemilihan anggota legislatif yang diusung.
5) Proses pemilihan menggunakan e-kiosk selesai.
6) Data sudah masuk ke server lokal, dan setelah panitia selesai merekap semua data, maka proses selanjutnya adalah tanda tangan panitia baik itu saksi dari masing-masing partai dan KPPS.
7) Setelah proses semua dilakukan semua data keseluruhan yang berada di server lokal dikirim menuju server pusat.
8) Proses pemilihan menggunakan e-voting selesai.

B. *Perancangan E-Kiosk*

E-Kiosk berfungsi sebagai sarana memudahkan pemilih untunk memilih dengan menggunakan *touch screen* pada layar komputer yang disediakan. Berikut Gambar 2 menunjukkan rancangan e-kiosk yang digunakan.



(a)

(b)

(c)

Gambar 2. Rancangan e-kiosk untuk aplikasi sistem *e-voting* yang dibuat (a) bagian masukkan token (b) bagian pilih partai (c) bagian pilih anggota legislatif.

C. *Implementasi*

Berdasarkan alur sistem yang dibuat, dibangun aplikasi sistem *e-voting* yang mengimplementasikan kontrol integritas e-kiosk. Secara garis besar, aplikasi ini terdapat 2 sistem, yaitu halaman admin dan bilik pemilih. Halaman admin berisi enam *tab* seperti yang terlihat pada Gambar 3.

Gambar 3. Implementasi tampilan aplikasi sistem *e-voting*. Aplikasi ini terdiri dari login admin (a) dan halaman utama terdiri dari enam *tab*: Cek koneksi (b), Generate token (c), Muat kunci TPS (d), Rekap Suara (e), Tanda Tangan Panitia (f), serta Kirim ke Server Pusat (g).

Penjelasan singkat masing-masing *tab* tersebut adalah sebagai berikut.

1) *Tab* pertama : Cek koneksi, berfungsi untuk mengatifkan servis sms pada aplikasi yang dibuat.
2) *Tab* kedua : Generate token, berfungsi untuk mengecek data pemilih (NIK, nama, dan statusnya) dalam basis data. Dan mengirimkan sms token pada pemilih, agar pemilih dapat memilih.
3) *Tab* kedua: Muat Kunci Privat, berfungsi untuk memuat kunci privat yang berwujud berkas XML.
4) *Tab* keempat: Rekap Suara, berfungsi untuk memuat rekapitulasi hasil suara sah partai, suara sah calon, dan suara tidak sah.
5) *Tab* kelima: Tanda Tangan Panitia, berfungsi untuk membuat dan menyimpan tanda tangan panitia ke dalam basis data. Tanda tangan dibuat berdasarkan data panitia (ID, nama, dan statusnya) dan status persetujuan disertai alasannya.
6) *Tab* keenam: Kirim ke Server Pusat, berfungsi untuk menampilkan data suara dari basis data untuk kemudian dikirim ke *server* pusat.

IV. UJI COBA DAN EVALUASI

Uji coba dilakukan terhadap aplikasi yang dibuat dan data suara yang sudah tersimpan di basis data dalam keadaan terenkripsi.

A. Skenario 1

Pada skenario ini, dilakukan uji coba mengolah kemanan database pada *field* nomor handphone. Untuk menghindari admin yang ingin mengubah nomor handphone.

JENIS_KELAMIN	ALAMAT_LENGKAP	AGAMA	HP
F	9 Quincy Circle	Buddha	+6281259362430

(a)

JENIS_KELAMIN	ALAMAT_LENGKAP	AGAMA	HP
F	9 Quincy Circle	Buddha	+6281259362431

(b)

Gambar 4. Tampilan pada basis data: (a) sebelum admin belum mengganti nomor handphone dan (b) setelah data suara diganti.

Data nomor handphone setelah diganti oleh admin maka terdapat pesan error karena nomor handphone tidak tervalidasi, karena *hash* value berbeda dengan yang diinginkan oleh hashrow. Berikut Gambar 5 menunjukkan pesan berisi nomor handphone tidak valid.

Gambar 5. Pesan berisi nomor handphone tidak valid.

B. Skenario 2

Pada skenario ini, dilakukan uji coba menemukan adanya perubahan atau pemalsuan terhadap basis data atau database pada tabel pemilih di *field* token. Misalkan pada Gambar 6 terdapat dua data token di basis data *server* lokal: (a) adalah data asli, kemudian dilakukan perubahan terhadap data token baris pertama sehingga tampilan menjadi seperti pada (b).

AGAMA	HP	WAKTU_MEMILIH	TOKEN
Buddha	+6281259362431	NULL	b789ad3222oiasw22a78272812321sddsasd1212esadsd1

(a)

AGAMA	HP	WAKTU_MEMILIH	TOKEN
Buddha	+6281259362431	NULL	1234

(b)

Gambar 6. Perubahan terhadap data token: (a) data token sebelum diubah (b) data token setelah diubah

Cara paling mudah untuk menemukan perubahan tersebut adalah ketika admin merubah data token tersebut maka asumsi admin dapat memasukkan token tersebut di bilik pemilih dan admin dapat memilih partai dan anggota legislatif sesuai dengan yang admin inginkan.

Sistem aplikasi e-voting ini mempunyai keamanan data dari sisi database yaitu mengamankan agar supaya database tersebut tidak bisa diganti oleh admin. Yang kita amankan adalah menampilkan di *field* token hasil *hash* kedua dari token aslinya. Karena *hash* value nya berbeda dengan total *hashrow* maka akan muncul pesan menolak, seperti Gambar 7.

Gambar 7. Pesan yang ditampilkan saat memasukkan data token yang diubah atau dipalsukan.

Pesan pada Gambar 7 menunjukkan bahwa *hash* value data token yang dikirim tersebut berbeda dengan yang sebenarnya. Saat menghasilkan token, aplikasi terlebih dahulu akan menghasilkan nilai *hash* dari gabungan data nama calon dan NIK yang dienkripsi. Jika hasil nilai *hash*-nya berbeda, maka data *hash* value token juga berbeda sehingga data suara yang diubah tersebut tidak bisa masuk ke *server* lokal.

V. KESIMPULAN DAN SARAN

Kesimpulan yang diperoleh antara lain:

1. Dengan melihat hasil uji coba fungsionalitas, semua kontrol aplikasi yang dibuat dapat berjalan dengan baik.
2. Rancangan keamanan data didalam database dapat berjalan dengan baik dari sisi admin melakukan kecurangan mengganti kolom token dan nomer handphone.
3. Data suara yang diubah atau dipalsukan tidak bisa dikirim ke *server* pusat karena nilai *hash* atau *signature* yang dihasilkan antara data yang asli dan data yang diubah adalah berbeda.
4. Data suara yang sebelumnya telah dikirim ke *server* pusat tidak bisa dikirim lagai karena nomor id data suara yang dikirim sebelumnya dengan yang dikirim lagi adalah sama.

Beberapa saran yang dapat disampaikan adalah:

1. Perlu adanya peralatan peralatan khusus dalam pemilihan umum di Indonesia, seperti laptop dan Wifi. Agar data tersebut dapat dikirim menuju *server* lokal maupun pusat.
2. Untuk proses autentikasi aplikasi *E-Voting* menggunakan nama dan nomor KTP, ke depannya untuk proses otentikasi untuk pemilihan umum yang berada di Indonesia dengan perkembangan teknologi yang semakin maju maka penulis memberi saran kepada KPU (Komisi Pemilihan Umum) agar proses autentikasi menggunakan pemindaian barcode *e-KTP* atau dengan menggunakan fingerprint.

DAFTAR PUSTAKA

[1] A. Rokhman, "Prospek Penerapan E-Voting di Indonesia," Universitas Jendral Soedirman, 2011. [Online]. Available: http://map.unsoed.ac.id/2011/11/29/prospek-penerapan-e-voting-diindonesia.

[2] "BPPT Sukses Uji Coba Evoting Berbasis E-KTP di Jembrana, Bali," Sekretariat Kabinet Republik Indonesia, 18 Desember 2013. [Online].

[3] C. Utama, *CodeIgniter Framework. Bandung: Universitas Pasundan.*, 2011.

[4] I. Sommerville, *Software Engineering, 9th edition, AddisonWesley*, 2011.

[5] "PHP adalah - Hypertext Preprocessor," 10 Desember 2013. [Online]. Available: http://agiptek.com/index.php/php/101-php.html. [Diakses 23 12 2014].

[6] P. Mansyurin, "Debian Web *Server* with OpenSSL (HTTPS)," 9 Desember 2013. [Online]. Available: http://lebaksono.wordpress.com/2010/12/20/debian-web-*server*-withopenssl-https. [Diakses 23 12 1014].

[7] M. Mogollon, "Cryptography and Security Sevices: Mechanisms and Applications," 2007.

[8] U. P. Nasional, 8 Desember 2013. [Online]. Available: http://www.library.upnvj.ac.id/pdf/2s1teknikinformasi/205511014/bab2.pdf. [Diakses 23 12 2014].

.