ISSN. 1412-0100 VOL 16, NO 1, APRIL 2015

Pengembangan Web E-Voting Menggunakan *Secure Election Protocol*

Irpan Adiputra Pardosi[1], Ronsen Purba[2]
STMIK Mikroskil, Jl. Thamrin No. 112, 124, 140, Telp. (061) 4573767, Fax. (061) 4567789
[1,2]Jurusan Teknik Informatika, STMIK Mikroskil, Medan
[1]irpan@mikroskil.ac.id, [2]ronsen@mikoskil.ac.id

Abstrak

Sistem e-voting akan memberikan kemudahan kepada pemilih dan panitia pelaksana dari segi waktu maupun biaya. Sistem voting melalui internet (e-voting) akan menemui permasalahan terkait keamanan komunikasi dan data sehingga diperlukan sebuah protokol kriptografi yang disebut Secure Election Protocol. Prosedur kerja dari Secure Election Protocol dengan dua panitia sentral menggunakan CTF dan CLA menjadi panitia. Protokol ini menggunakan algoritma AES-128 untuk mengamankan data yang dikirimkan, dan algoritma RSA untuk mengamankan kunci AES-128 serta menggunakan kombinasi algoritma DSA dan SHA-1 untuk membentuk tanda tangan digital dari pesan yang dikirimkan. Perangkat lunak e-voting menggunakan Secure Election Protocol dengan dua panitia sentral ini mampu mengamankan proses pemilihan online (e-voting) untuk pemilihan Ketua BITSMIKRO dengan baik dan benar. Kebutuhan teknologi e-voting yang aman di masa mendatang akan semakin besar. Penerapan kriptografi pada penelitian ini telah membuktikan perannya dalam mengamankan pemilihan online (e-voting).

Kata kunci— e-voting, secure election protocol, pemilihan online, web e-voting

Abstract

E-voting system will provide convenience to voters and the executive committee in terms of time and cost. Voting system via the internet (e-voting) will a need of security-related issues and data communications requiring a cryptographic protocol called Secure Election Protocol. The working procedures of the Election Protocol Secure with two central committee using CTF and CLA into committee. This protocol uses AES-128 algorithm for securing the transmitted data and to secure key RSA algorithm AES-128 algorithm and uses a combination of DSA and SHA-1 to form a digital signature of a message sent. E-voting software using Secure Election Protocol with two central committee was able to secure the electoral process online (e-voting) for the election of the Chairman BITSMIKRO properly. E-voting technology needs safe in the future will be even greater. The application of cryptography in this study has proven its role in securing online voting (e-voting).

Keywords— *e-voting, secure election protocol, online voting, web e-voting*

1. PENDAHULUAN

Pemilihan dengan e-voting bertujuan mengatasi permasalahan yang timbul pada pemilihan konvensional baik dari segi biaya dan waktu [1]. Disamping keuntungan yang ditawarkan terdapat berbagai masalah pada penerapan e-voting, termasuk menjamin bebas dari penyadapan, menghindari pelaku yang curang, ataupun panitia yang bersekongkol sehingga proses pemilihan tetap jujur dan adil [2]. Untuk mengatasi masalah ini, penulis menggunakan protokol kriptografi yaitu Secure Election Protocol. Protokol ini mampu mencegah panitia untuk mengetahui nomor validasi yang diambil oleh

setiap pemilih sehingga panitia tidak dapat mengetahui suara yang diberikan oleh setiap pemilih, hanya pemilih sah yang dapat memilih, setiap pemilih hanya dapat memilih satu kali, tidak ada yang bisa menduplikasi atau mengubah pilihan seseorang dan setiap pemilih yakin kalau suaranya sudah masuk dalam penghitungan suara [3]. Protokol ini menggunakan satu panitia pengawas dan pelaksana, algoritma RSA (Rivest, Shamir & Adleman) digunakan untuk mengamankan kunci, algoritma AES-128 mengamankan data dan SHA-1 digabung dengan DSA sebagai tanda tangan digital, untuk menghindari penyangkalan. Penulis membuat perangkat lunak pemilihan online atau e-voting menggunakan prosedur kerja dari Secure Election Protocol, dengan menerapkan konsep keamanan untuk memenuhi pemilihan secara jujur dan adil.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian berupa analisis masalah dan proses yang akan dijabarkan di bawah ini.

2.1 Analisis Masalah

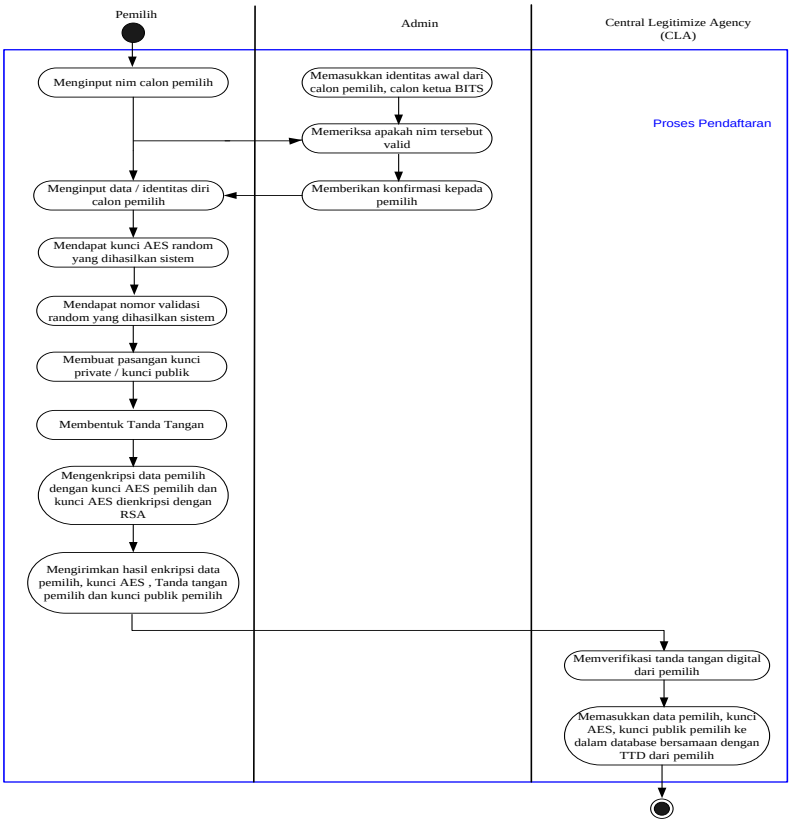
Pemilihan online (e-voting) akan menimbulkan beberapa permasalahan dan salah satu solusi yang dapat digunakan untuk menyelesaikan deretan masalah dalam e-voting dengan menerapkan protokol pemilihan dengan dua panitia sentral yang diperkenalkan oleh A. Salomaa pada sekitar tahun 1990 yang diberi nama Secure Election Protocol dengan dua panitia sentral. Pemilihan online (e-voting) dengan dua panitia sentral yang akan dibuat ini terdiri dari 5 entitas di dalamnya yaitu: Pemilih dan Calon yang akan dipilih (ketua BITSMIKRO). Panitia yang bertugas dalam pemilihan diantaranya **admin** sebanyak 1 orang, bertugas untuk menginput data-data pemilih dan calon, menginput data awal website serta bertugas menonaktifkan pemilih sesuai permintaaan CLA. **CLA** (*Central Legitimization Agency*) sebanyak 2 orang bertugas untuk memberikan nomor kepada pemilih, membuat informasi mengenai voting dan mengkonfirmasi admin untuk menonaktifkan pemilih. CTF (*Central Tabulating Facility*) sebanyak 2 orang bertugas untuk menyimpan data pemilihan, mengawasi kinerja CLA dalam memberikan nomor pemilihan melalui laporan yang diterima CTF.

2.2 Analisis Proses

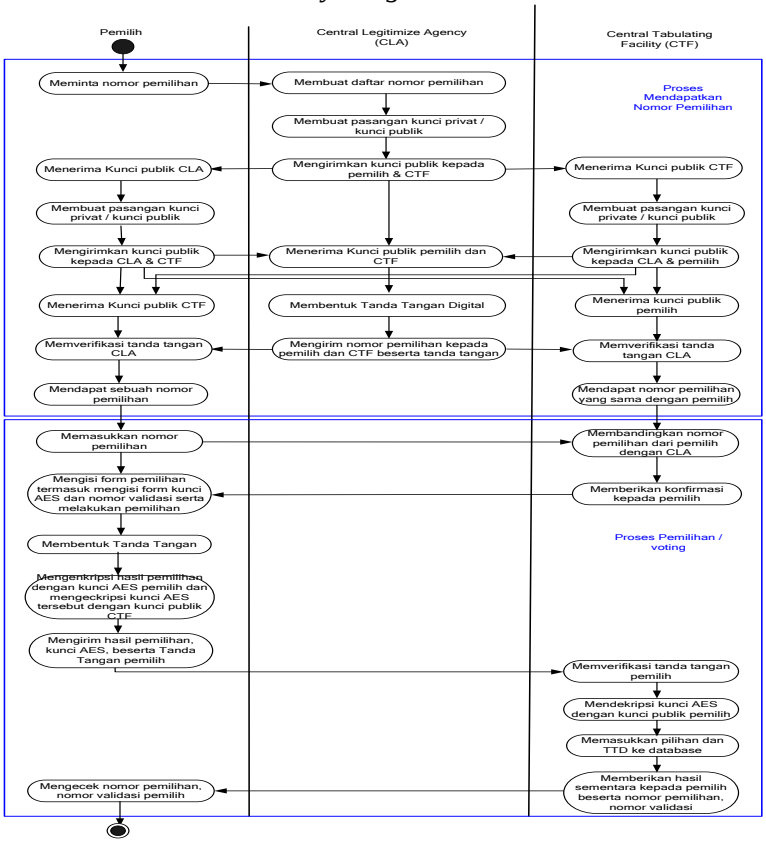
Secure Election Protocol dengan dua panitia sentral dapat diterapkan untuk melakukan proses pemilihan (*voting*) di *internet*. Protokol ini memerlukan beberapa algoritma pendukung dalam melakukan prosedur kerjanya, seperti:

a. Algoritma kriptografi kunci *simetri* AES-128 digunakan untuk mengenkripsi dan mendekripsi data yang dikirim.
b. Algoritma kriptografi kunci publik RSA, digunakan untuk mengenkripsi dan mendekripsi kunci yang digunakan pada saat mengenkripsi data.
c. Algoritma DSA dan SHA-1, digunakan untuk membuat tanda tangan digital.
d. Fungsi *Fast Exponentiation*, yang digunakan untuk menghitung nilai dari operasi perpangkatan modulo bilangan besar. Fungsi ini digunakan dalam proses enkripsi dan dekripsi pada algoritma RSA.
e. Algoritma *Extended Euclidean*, yang digunakan untuk menghitung nilai invers modulo. Algoritma ini digunakan pada proses pembentukan kunci dari algoritma RSA yaitu untuk menghitung nilai kunci enkripsi.

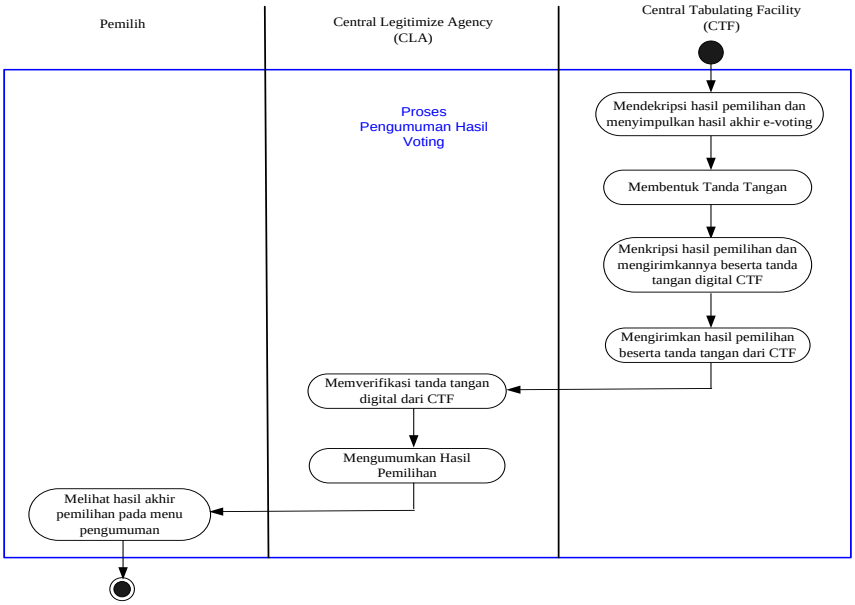
Proses kerja dari sistem e-voting akan dijabarkan dengan *activity diagram* seperti pada gambar 1, gambar 2 dan gambar 3 di bawah ini



Gambar 1. *Activity Diagram* Pendaftaran

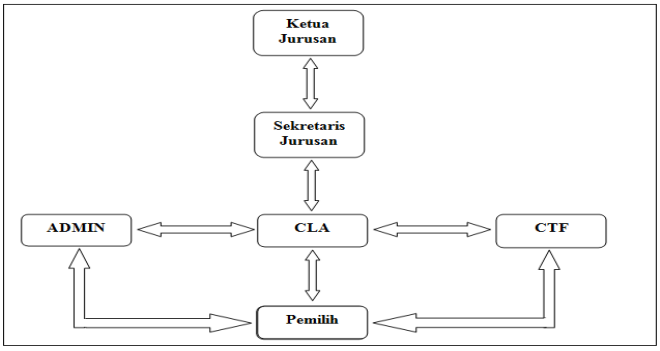


Gambar 2. *Activity Diagram* Proses Pemilihan *e-voting*



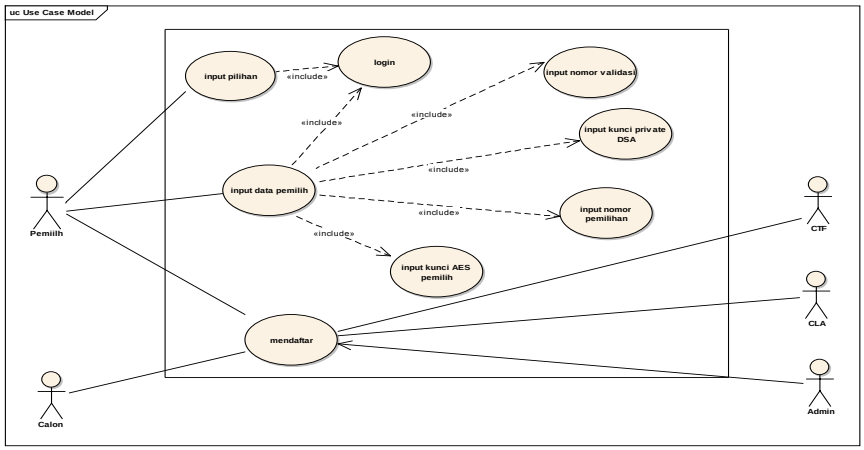
Gambar 3. *Activity Diagram* Pengumuman Hasil *e-voting*

Untuk menjelaskan struktur hirarki otoritas pengguna dari pengguna pada sistem e-voting ini dijelaskan pada gambar 4 dibawah ini:



Gambar 4. Hirarki Sistem e-*Voting*

Pemodelan sistem dari e-voting digambarkan dengan use case untuk memudahkan memahami kinerja dari sistem secara keseluruhan. Gambar 5 di bawah ini menjabarkan sistem secara keseluruhan.



Gambar 5. *Use Case* Sistem

2.3 Kriptografi

Kriptografi dewasa ini bukan lagi hanya sekedar enkripsi dan dekripsi. *Authentication* (otentikasi) adalah bagian dari hidup yang fundamental sebagai kerahasiaan. *Digital signatures* (tanda tangan digital) memaketkan sebuah dokumen ke dalam prosesor kunci khusus, sedangkan digital *timestamps* (stempel waktu digital) memaket sebuah dokumen ke dalam penciptaannya pada waktu tertentu. Kriptografi modern berkembang dengan pesat dan berbagai variasi, namun kriptografi secara fundamental didasarkan pada masalah-masalah yang sulit untuk dipecahkan. [4]

2.3.1 Algoritma Kriptografi Kunci Publik RSA (Rivest, Shamir dan Adleman)

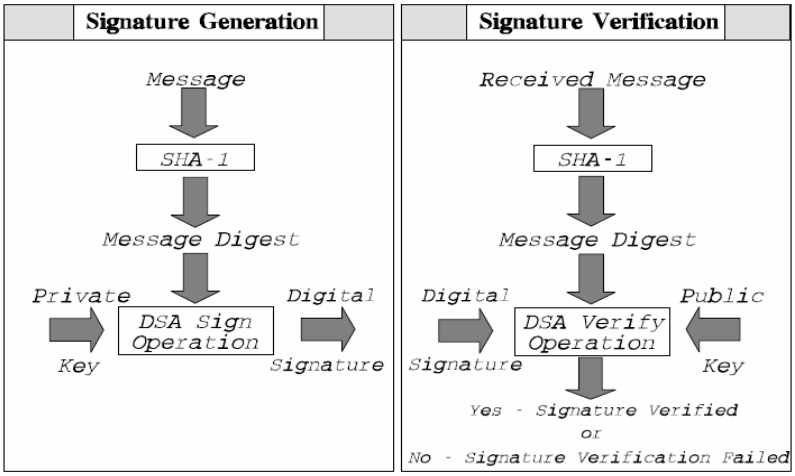
Menurut Rinaldi Munir, dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, algoritma kriptografi kunci publik yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu Ron (R)ivest, Adi (S)hamir dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima[4]. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang bagus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Algoritma RSA memiliki besaran-besaran sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. n = p . q (tidak rahasia)
3. $\phi(n) = (p - 1)(q - 1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

2.3.2 *Digital Signature Algorithm (DSA)*

Tanda tangan digital DSA berbentuk sepasang besar angka yang ditampilkan komputer sebagai string dari digit biner. Tanda tangan digital dihitung dengan menggunakan sejumlah aturan dan sejumlah parameter sehingga identitas pemilik dan integritas data dapat diverifikasi. Pembuat tanda tangan menggunakan kunci privat untuk membuat tanda tangan; sedangkan kunci publik, yang berkorespondensi dengan kunci privat namun tidak sama, digunakan untuk memverifikasi tanda tangan. [2]

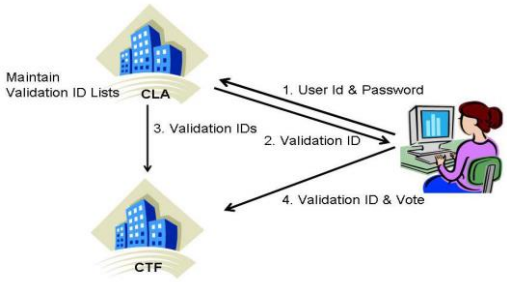


Gambar 6. Enkripsi dan dekripsi DSA[2].

2.3.3 *Secure Election Protocol Voting* dengan Dua Panitia Sentral

Salah satu alternatif solusi yang dapat diterapkan untuk melakukan voting di internet adalah dengan menggunakan dua buah panitia sentral, yaitu *Central Legitimization Agency* (CLA) dan *Central Tabulating Facility* (CTF)[3]. CLA berfungsi untuk melakukan pendaftaran pemilih yang sah dan CTF untuk menghitung jumlah suara. Kedua panitia tidak boleh saling bertukar data satu sama lain. Protokol ini dipublikasikan oleh A. Salomaa pada tahun 1990. Proses kerja dari protokol yang menggunakan dua buah panitia sentral untuk melakukan proses voting ini adalah sebagai berikut[3]:

a. Setiap pemilih mengirimkan sebuah pesan kepada CLA untuk meminta sebuah nomor validasi.
b. CLA mengirimkan sebuah nilai validasi acak yang unik kepada pemilih. CLA memegang sebuah daftar nomor validasi. CLA juga memiliki sebuah daftar penerima nomor validasi, untuk mencegah seorang pemilih meminta dua buah nomor validasi.
c. CLA mengirimkan daftar nomor validasi kepada CTF.
d. Setiap pemilih memilih sebuah nomor identifikasi acak dan membuat sebuah pesan yang berisi nomor identifikasi acak tersebut, nomor validasi yang diterimanya dari CLA dan suara (pilihannya). Pemilih mengirimkan pesan tersebut kepada CTF.



Gambar 7. Ilustrasi Arus Pesan pada Protokol *Voting* dengan Dua Panitia[5]

3. HASIL DAN PEMBAHASAN

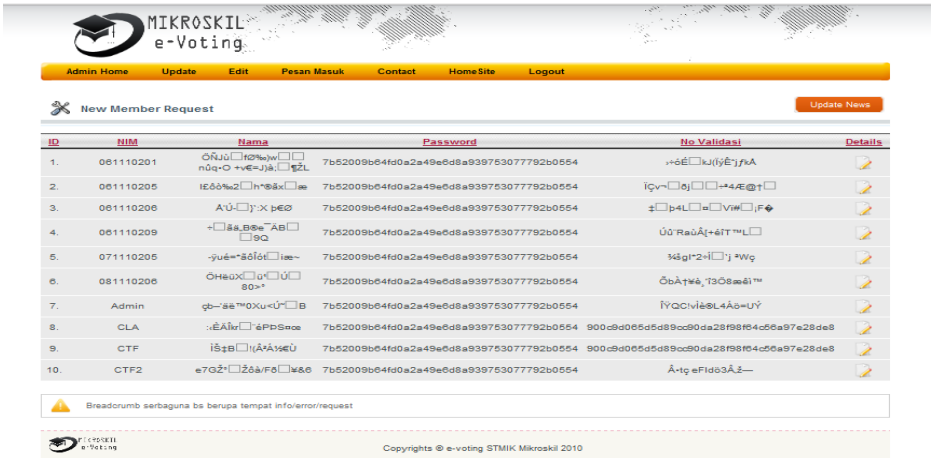
Hasil dari penelitian ini akan dijabarkan berupa tampilan hasil yang akan terlihat bagi masing-masing pengguna sistem e-voting, termasuk proses pengamanan yang dilakukan sistem, kemudian dari hasil akan dilakukan pembahasan mengenai kriteria keamanan sesuai dengan yang telah didaftarkan di awal.

3.1 Hasil

Pada gambar 8 di bawah, merupakan tampilan awal dari sistem e-voting ini, yang dapat diakses oleh semua pengguna sistem.

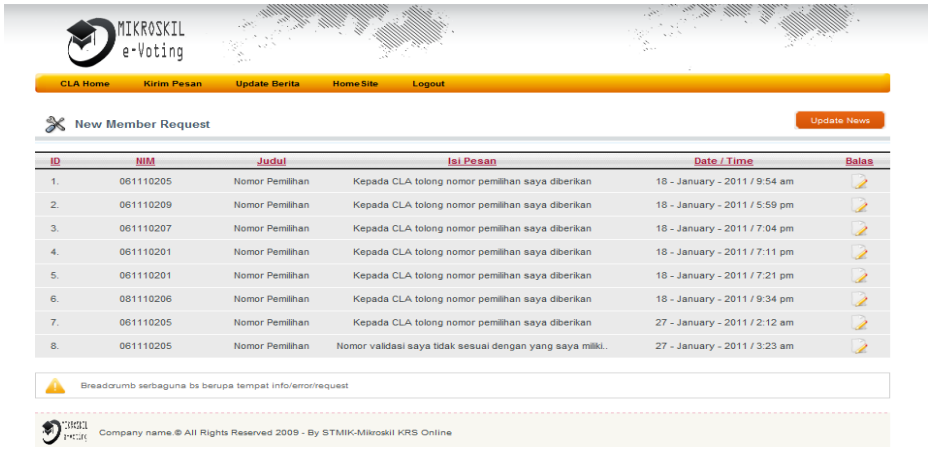
Gambar 8. Menu *Front end Visitor*

Pada gambar 9 memperlihatkan tampilan dari halaman Admin. Data-datanya sudah diamankan dengan dienkripsi.



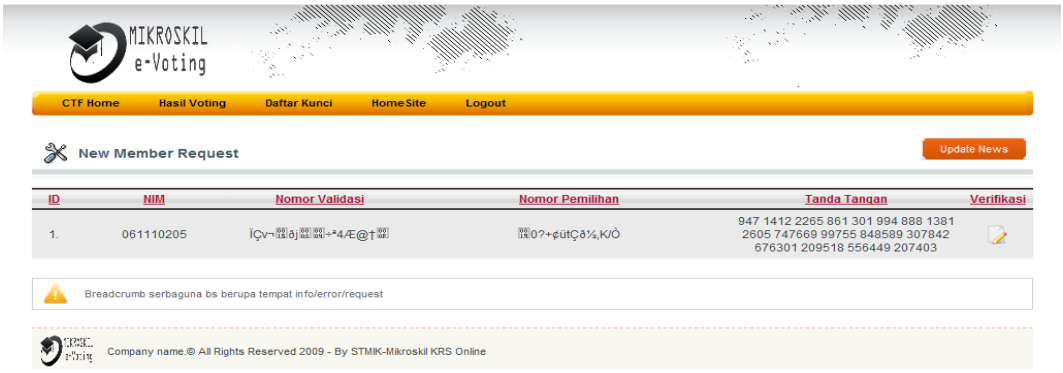
Gambar 9. Menu *Back end Admin*

Pada gambar 10 merupakan halaman dari CLA, data-datanya juga sudah diamankan dengan dienkripsi.



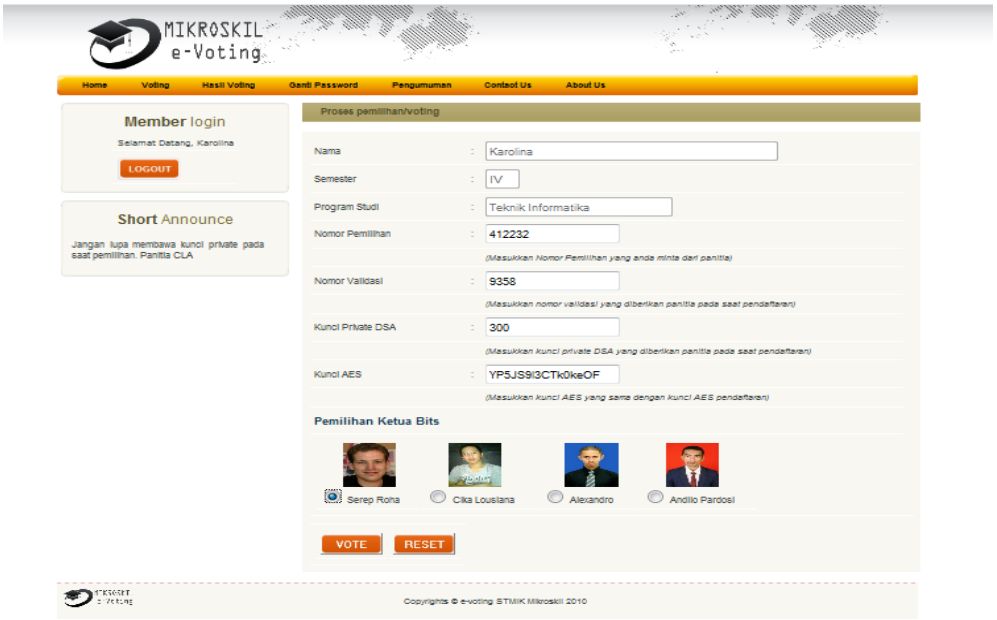
Gambar 10. Menu *Back end CLA*

Pada gambar 11 merupakan halaman dari CTF, data-datanya juga sudah diamankan dengan dienkripsi.



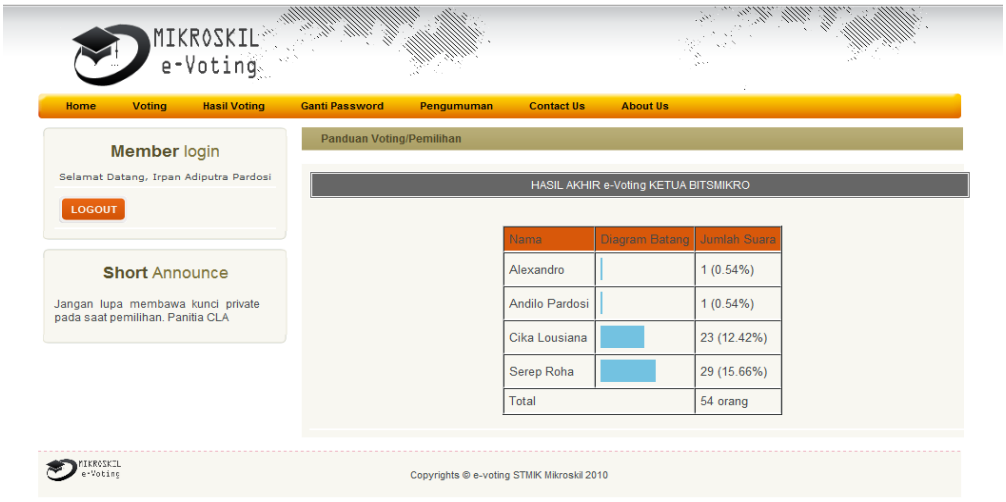
Gambar 11. Menu Back end CTF

Pada gambar 12 merupakan halaman *vote* yang akan telihat saat hari pemilihan. Proses pemilihan hanya dapat dilakukan jika pemilih memiliki nomor pemilihan, nomor validasi, kunci DSA dan AES. Data tersebut didapatkan saat melakukan pendaftaran dan di *request* dari admin CLA.



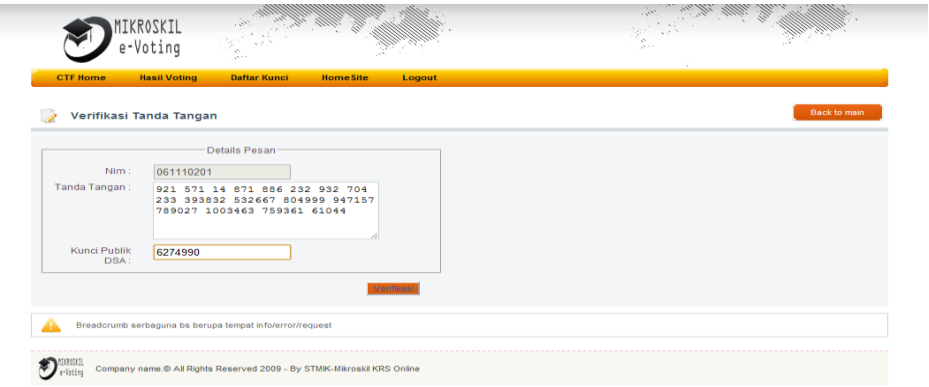
Gambar 12. Halaman *Vote* (Pemilihan)

Pada gambar 13 terlihat hasil sementara dari proses pemilihan, dan hasil ini hanya akan muncul jika semua kunci yang di halaman *vote* sudah benar.



Gambar 13. Halaman Hasil Voting Setelah Hari-H

Pada gambar 14 terlihat halaman verifikasi tanda tangan digital saat panitia CLA mengirimkan hasil pemilihan kepada panitia CTF, untuk memastikan keaslian data.



Gambar 14. Halaman Verifikasi Tanda Tangan

3.2 Pembahasan

Berdasarkan pengujian yang telah dilakukan terhadap perangkat lunak ini maka dapat disimpulkan bahwa perangkat lunak ini telah memenuhi kriteria keamanan yakni:

a. Kerahasiaan.
Dari hasil pengujian perangkat lunak ini, kriteria keamanan yang pertama telah terpenuhi dimana setiap pesan / data yang akan dikirimkan ke server terlebih dahulu akan dienkripsi menggunakan algoritma AES-128 sehingga pihak yang tidak berhak terhadap pesan tersebut tidak akan mengetahui isinya. Kriptografi simetris memiliki kelemahan dimana keamanannya hanya terletak pada kerahasiaan kuncinya saja jadi untuk mengamankan kunci AES ketika dikirimkan ke server maka kunci tersebut di enkripsi juga menggunakan algoritma RSA, sehingga kerahasiaan data terjamin sampai di server proses ini dapat dilihat pada gambar 12.

b. Integritas
Dalam pengirim pesan / data dari *client* ke *server* maka harus dipastikan kalau data yang disimpan atau yang diterima tidak rusak, ataupun tidak diubah oleh pihak yang tidak berhak. Hal ini bisa diatasi dengan adanya sidik jari digital yang dibentuk menggunakan algoritma SHA-1 yang hasilnya selalu unik dimana dalam sistem ini dikombinasikan dengan algoritma DSA, sehingga jika pesan mengalami perubahan dalam pengiriman maka sidik jari digitalnya pasti tidak valid dan secara otomatis tanda tangannya juga pasti tidak akan valid, dengan cara ini dipastikan integritas dari data terjamin sampai di server. Hasil pengujian dapat dilihat pada gambar 14.

c. Otentikasi
Mekanisme untuk memastikan keaslian data atau identitas pasangan komunikasi, telah terpenuhi hal ini dapat dibuktikan dengan adanya tanda tangan digital yang dibuat menggunakan algoritma SHA-1 dan algoritma DSA dimana setiap pesan yang dikirim akan dibuat tanda tangan digitalnya sehingga kita dapat memastikan keaslian data dan indentitas pasangan komunikasi karena sistem akan memverifikasi tanda tangan digital dari pasangan komunikasi kita dan jika tanda tangan tersebut tidak valid maka proses tidak akan dilanjutkan tapi diminta diulang kembali. Hasil pengujian dapat dilihat pada gambar 12 dan gambar 14.

d. Anti-Penyangkalan
Untuk menghindari penyangkalan dari pemilih di kemudian hari ketika melakukan pemilihan maupun ketika meminta nomor pemilihan dari CLA maka pesan yang dikirimkan akan disertakan dengan tanda tangan digitalnya, hal yang sama juga dilakukan untuk menghindari adanya panitia CLA palsu ketika memberikan nomor pemilihan kepada pemilih dengan cara ini maka tindakan penyangkalan dapat diatasi dengan baik. Hasil pengujian dapat dilihat pada gambar 14.

4. KESIMPULAN

Hasil pengujian yang dilakukan menunjukkan *Secure Election Protocol* dengan dua panitia sentral telah memenuhi kriteria keamanan yaitu kerahasiaan, integritas, otentikasi, dan anti-penyangkalan. Dengan menggunakan algoritma kriptografi AES dalam proses pengiriman data, algoritma RSA untuk mengenkripsi kunci AES dan algoritma SHA-1 serta algoritma DSA untuk menandatangani pesan yang dikirim, Kemudian perangkat lunak dapat digunakan sebagai prototipe pemilihan online yang aman dalam sistem yang nyata.

5. SARAN

Penulis ingin memberikan beberapa saran yang mungkin berguna untuk pengembangan perangkat lunak lebih lanjut seperti mengganti algoritma yang digunakan sehingga waktu proses lebih cepat dengan tingkat keamanan yang sama atau lebih baik, menambahkan hirarki panitia berjenjang yang memiliki fungsi yang berbeda-beda, menambahkan mekanisme yang dapat mengidentifikasi kecurangan - kecurangan yang terjadi antara pemilih dengan panitia, maupun antar panitia.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu dan yang telah memberi dukungan selama proses penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1] A. Rokhman, 2011, "Prospek dan Tantangan Penerapan E-Voting di Indonesia," *Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia*.

[2] K. M. Hutagalung, 2012, "Perancangan Perangkat E-Voting Berbasis e-KTP," *Saintikom*.

[3] J. Sireesha and S.-I. Chakchai, 2005, "Secure Virtual Election Booth with Two Central Facilites," *Department of Computer Science Washington University*, p. 13, USA.

[4] R. Munir, 2006, Pengantar Kriptografi, Informatika, Bandung.

[5] H. Lipmaa, 2010, "Secure Electronic Voting Protocols,".

[6] A. Kadir, 1991, Pengenalan Perangkat Keras dan Perangkat Lunak, Andi, Bandung.

[7] P. Kasiman, 2006, Aplikasi Web Dengan PHP dan Mysql, Andi, Yogyakarta.

[8] A. Kadir, 2008, Dasar Pemrograman Web Dinamis Menggunakan PHP, Andi, Yogyakarta.

[9] N. Bunafit, 2004, Database Relasional Dengan Mysql, Andi, Yogyakarta.

[10] A. Muslim, 2010, "Gunadarma, UML dan Use Case," 17 August 2006. [Online]. Available: http://amuslim.staff.gunadarma.ac.id/Downloads/folder/0.0. diakses tanggal 22 Februari 20010.

[11] M. Nikita, P. Chetan, C. Suruchi and P. R. S, 2008, "Secure Online Voting System Proposed By Biometrics And Steganography," *Exploring Research And Innovations*, vol. 3, no. 5.

[12] S. Bruce, 1996, Applied Criptography, Second Edition, Wiley & Sons.Inc, Canada.

[13] S. Christopher, 2006, CSS Cookbook, O'Reily Media. Inc, USA.