IMPLEMENTASI PEMILIHAN ONLINE PRESIDEN MAHASISWA DENGAN KEAMANAN SISTEM MENGGUNAKAN METODE BLIND SIGNATURES DAN AES

Skripsi

oleh
R. FIRMAN PUTRA ARDIANTO
22104950

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

IMPLEMENTASI PEMILIHAN ONLINE PRESIDEN MAHASISWA DENGAN KEAMANAN SISTEM MENGGUNAKAN METODE BLIND SIGNATURES DAN AES

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

R. FIRMAN PUTRA ARDIANTO
22104950

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI PEMILIHAN ONLINE PRESIDEN MAHASISWA DENGAN KEAMANAN SISTEM MENGGUNAKAN METODE BLIND SIGNATURES DAN AES

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 24 Juni 2015

R. FIRMAN PUTRA ARDIANTO
22104950

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI PEMILIHAN ONLINE PRESIDEN MAHASISWA DENGAN KEAMANAN SISTEM MENGGUNAKAN METODE BLIND SIGNATURES DAN AES
Nama Mahasiswa	:	R. FIRMAN PUTRA ARDIANTO
N I M	:	22104950
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2014/2015

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 24 Juni 2015

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Theresia Herlina R., S.Kom.,M.T.

HALAMAN PENGESAHAN

IMPLEMENTASI PEMILIHAN ONLINE PRESIDEN MAHASISWA DENGAN KEAMANAN SISTEM MENGGUNAKAN METODE BLIND SIGNATURES DAN AES

Oleh: R. FIRMAN PUTRA ARDIANTO / 22104950

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 15 Juni 2015

Yogyakarta, 24 Juni 2015
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Theresia Herlina R., S.Kom.,M.T.
3. R. Gunawan Santosa, Drs. M.Si.
4. Kristian Adi Nugraha, S.Kom., M.T.

Dekan

(Budi Susanto, S.Kom., M.T.)

Ketua Program Studi

(Gloria Virginia, Ph.D.)

DAFTAR ISI

ABSTRAK

Pemilihan Presiden Mahasiswa dilaksanakan setahun sekali di Universitas, khususnya Universitas Kristen Duta Wacana. Para Mahasiswa sangatlah tertarik dengan orasi dan debat antar kandidat, karena pentingnya pemilihan Presiden Mahasiswa yaitu untuk mewakili seluruh mahasiswa di Universitas dan menjalankan semua kebutuhan mahasiswa di seluruh Universitas. Namun, pemilihan Presiden Mahasiswa di Universitas Kristen Duta Wacana masih menggunakan cara yang manual, yaitu Mahasiswa harus datang ke tempat pemungutan suara dan mengumpulkannya ke kotak suara. Cara manual masih digunakan karena cara ini masih yang paling aman dan *Real-time* dan kejujuran masih dapat di buktikan secara kasat mata dengan melihat orang yang memilih. Namun sekarang Internet sudah meluas dan semua mahasiswa sudah dapat menggunakannya untuk kebutuhan sehari-hari. Internet bukan hal yang asing lagi bagi dunia dan bahkan sekarang internet merupakan suatu kebutuhan yang harus terpenuhi. Salah satunya adalah digunakan untuk Pemilihan Presiden Mahasiswa. Pemilihan secara online ini menghemat waktu para Mahasiswa dan dapat memilih dimanapun tempatnya. Ada di suatu kondisi dimana Mahasiswa malas untuk datang ke tempat pemungutan suara, dan lebih untuk memilih golput dan membuang hak pilihnya begitu saja. Penelitian ini akan membuat system yang online, dimana system online ini dapat mencangkup semua mahasiswa dimanapun tempatnya. Penelitian ini juga membuat system keamanan untuk Pemilihan Presiden Mahasiswa karena Pemilihan Presiden Mahasiswa sangatlah rahasia dan sangat fatal jika dimanipulasi. System ini online dan juga terdapat manfaatnya yaitu menghemat biaya, waktu dan tempat. Namun dengan system online ini masih terdapat banyak factor yang harus terjamin keamanannya dan kegunaannya. Inilah kelemahan system online, semua harus dapat terfikirkan segala kemungkinan yang akan terjadi pada system terutama dari hackers dan penyerang lainnya. Hal inilah yang membuat menarik menjadi penelitian bagaimana metode yang baik dan system keamanan yang baik untuk system online ini.

ABSTRAK

Pemilihan Presiden Mahasiswa dilaksanakan setahun sekali di Universitas, khususnya Universitas Kristen Duta Wacana. Para Mahasiswa sangatlah tertarik dengan orasi dan debat antar kandidat, karena pentingnya pemilihan Presiden Mahasiswa yaitu untuk mewakili seluruh mahasiswa di Universitas dan menjalankan semua kebutuhan mahasiswa di seluruh Universitas. Namun, pemilihan Presiden Mahasiswa di Universitas Kristen Duta Wacana masih menggunakan cara yang manual, yaitu Mahasiswa harus datang ke tempat pemungutan suara dan mengumpulkannya ke kotak suara. Cara manual masih digunakan karena cara ini masih yang paling aman dan *Real-time* dan kejujuran masih dapat di buktikan secara kasat mata dengan melihat orang yang memilih. Namun sekarang Internet sudah meluas dan semua mahasiswa sudah dapat menggunakannya untuk kebutuhan sehari-hari. Internet bukan hal yang asing lagi bagi dunia dan bahkan sekarang internet merupakan suatu kebutuhan yang harus terpenuhi. Salah satunya adalah digunakan untuk Pemilihan Presiden Mahasiswa. Pemilihan secara online ini menghemat waktu para Mahasiswa dan dapat memilih dimanapun tempatnya. Ada di suatu kondisi dimana Mahasiswa malas untuk datang ke tempat pemungutan suara, dan lebih untuk memilih golput dan membuang hak pilihnya begitu saja. Penelitian ini akan membuat system yang online, dimana system online ini dapat mencangkup semua mahasiswa dimanapun tempatnya. Penelitian ini juga membuat system keamanan untuk Pemilihan Presiden Mahasiswa karena Pemilihan Presiden Mahasiswa sangatlah rahasia dan sangat fatal jika dimanipulasi. System ini online dan juga terdapat manfaatnya yaitu menghemat biaya, waktu dan tempat. Namun dengan system online ini masih terdapat banyak factor yang harus terjamin keamanannya dan kegunaannya. Inilah kelemahan system online, semua harus dapat terfikirkan segala kemungkinan yang akan terjadi pada system terutama dari hackers dan penyerang lainnya. Hal inilah yang membuat menarik menjadi penelitian bagaimana metode yang baik dan system keamanan yang baik untuk system online ini.

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pemilihan presiden mahasiswa yang diadakan setahun sekali di universitas khususnya Universitas Kristen Duta Wacana memiliki peminat mahasiswa dan rasa semangat untuk mendengarkan orasi, debat antar kandidat terutama pada saat pemilihan kandidat. Pemilihan presiden mahasiswa ini penting mengingat harus ada wakil mahasiswa untuk mendengarkan dan menyampaikan semua kebutuhan mahasiswa terhadap universitas. Pemilihan presiden mahasiswa ini masih menggunakan cara yang manual yaitu Mahasiswa harus datang ke tempat pemungutan suara, lalu memilih dengan cara mencoblos surat suara dan mengumpulkannya ke tempat pengumpulan suara. Cara manual masih digunakan karena cara ini yang masih aman dan terbukti jujur karena langsung dapat dilihat pemilihan suara di bilik – bilik tempat suara, dan melihat secara langsung orang yang bertugas menghitung suara. Namun di jaman sekarang ini mahasiswa telah banyak menggunakan internet. Hampir semua mahasiswa familiar dengan internet dan bahkan internet menjadi sebuah kebutuhan yang harus terpenuhi. Internet juga sudah digunakan secara global dan keamanannya pun sudah terjamin di berbagai bidang. Salah satunya diaplikasikan ke pemilihan presiden mahasiswa. Pemilihan secara online berbasis web ini mendukung dan menghemat waktu mahasiswa untuk memilih kapanpun dan dimanapun berada.

Pemilihan presiden mahasiswa saat ini terdapat banyak kekurangan dan kelebihannya, kelebihannya adalah rasa kepercayaan terhadap pemungutan jumlah suara dan secara real terbukti bahwa suara itu sah. Namun dilain sisi, masih banyak mahasiswa yang tidak dapat meluangkan waktunya untuk memilih calon kandidat yang diyakini karena harus datang ke Tempat Pemungutan Suara (TPS) untuk memilih. Terkadang juga ada yang malas untuk antri dan memilih di TPS, hal

lainnya, mahasiswa terkadang mencoblos sembarangan dan akhirnya mendapatkan suara tidak sah. Mahasiswa tidak tahu cara berorasi masing-masing kandidat kalau mahasiswa tersebut tidak mengenal kandidatnya. Sehingga pada saat pemilihan, mahasiswa hanya asal memilih saja tanpa memikirkan performa orasi kandidat.

Penelitian kali ini akan membuat sebuah sistem beserta keamanan sistemnya untuk pemilihan presiden mahasiswa. Sistem ini memiliki kelebihan yaitu online. Sistem online dapat merangkul semua mahasiswa baik yang sibuk atau tidak, dapat menggunakan hak pilihnya di mana saja. Kelebihan ini sangatlah mendukung perkembangan sistem pemilihan mahasiswa mulai dari waktu, biaya, dan tempat. Namun dengan sistem online ini banyak faktor keamanan yang harus dijamin tingkat keamanan dan prosedur keamanan sistemnya sendiri. Hal inilah yang menimbulkan masalah dari sistem online ini, mulai dari *hackers* dan *spy*. Hal ini yang menarik untuk menjadi penelitian, bagaimana metode dan sistem keamanan yang baik untuk sistem pemilihan online ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka peneliti akan melakukan penelitian sistem aplikasi pemilihan presiden mahasiswa online. Secara garis besar, penelitian ini memiliki perumusan masalah sebagai berikut :

1. Bagaimana mengimplementasikan metode blind signature dan AES untuk sistem keamanan pemilihan online presiden mahasiswa.
2. Efisiensi pemrosesan data oleh system dengan menggunakan double enkripsi, single enkripsi atau tidak sama sekali, perbedaan dilihat dari satuan ukuran waktu pada saat mengirimkan data

1.3 Batasan Sistem

Dalam penelitian ini, peneliti memberikan batasan sistem yang akan dibuat antara lain :

1. Aplikasi hanya untuk sistem pemilihan presiden mahasiswa Universitas Kristen Duta Wacana.
2. Voters mengikuti aturan waktu dan tanggal untuk melakukan voting dengan mengikuti jam Gmail indonesia untuk mengatasi adanya penggantian jam dan tanggal pada device user.
3. Diasumsikan bahwa semua email students mahasiswa Universitas Kristen Duta Wacana yang terdaftar adalah email aktif.

1.4 Tujuan Penelitian

Tujuan penelitian sebagai berikut :

1. Membuat sistem pemilihan online presiden mahasiswa menggunakan blind signature dan AES.
2. Mambandingkan system lebih baik menggunakan system keamanan menggunakan double enkripsi, single enkripsi atau tidak sama sekali.

1.5 Metode Penelitian

Metode yang digunakan untuk penulisan Tugas Akhir adalah sebagai berikut :

1. **Studi Pustaka**

   Mempelajari dasar teori dari berbagai sumber literature, jurnal, dan internet mengenai metode *blind signatures, zero knowledge proof, two factor authentication,* dan AES.

2. **Perancangan Sistem**

   Sistem dirancang berbasis online web agar semua mahasiswa dapat menggunakan di semua tempat serta waktu yang telah ditentukan secara leluasa. Sistem pemilihan ini menggunakan batasan waktu (tanggal dan jam) yang telah ditentukan oleh sistem untuk pemilihan presiden mahasiswa. Sistem pemilihan presiden mahasiswa memiliki fitur untuk menampilkan video orasi kandidat. Voters dapat login ke sistem dengan ID dan password

yang telah di dapat di email masing-masing. Setelah login, voters harus submit dan akan mendapatkan 8 digit PIN untuk konfirmasi.

3. **Implementasi Sistem**
    a. Mengimplementasikan *blind signature* untuk keamanan sistem pada pemilihan presiden mahasiswa.
    b. Mengimplementasikan enkripsi dan dekripsi menggunakan AES untuk mengamankan data serta pengirimannya.
4. **Pengujian Sistem**

    Pengujian sistem dilakukan dengan cara menerobos sistem keamanan pemilu online. Pengujian dilakukan dengan melakukan berbagai kemungkinan yang terjadi pada saat login, verifikasi, voting dan logout pada sistem. Mencoba melakukan kegiatan tidak sesuai prosedur sistem yang telah ditentukan.
5. **Pengambilan data**
    a. Pengumpulan data-data berupa yang berupa jurnal ilmiah, artikel, dan data-data lain yang mendukung penelitian Tugas Akhir ini.
    b. Pengambilan data dengan cara melakukan pengambilan data di Universitas Kristen Duta Wacana.

1.6 Sistematika Penulisan

Sistematika penulisan akan tebagi menjadi lima bab dengan urutan penulisan sbagai berikut :

BAB I PENDAHULUAN bab ini berisi latar belakang masalah, Rumusan Masalah, Batasan Sistem, Tujuan Penelitian, Metode Penelitian dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA bab ini berisi Tinjauan pustaka dan Landasan Teori

BAB III ANALISIS DAN PERANCANGAN SISTEM pada bab ini mencangkup analisis teori-teori serta fitur-fitur sistem yang akan digunakan serta bagaimana menterjemahkannya kedalam sistem yang akan dibuat.

BAB IV IMPLEMENTASI DAN ANALISIS SISTEM bab ini memuat hasil implementasi dan pembahasan implementasi.

BAB V KESIMPULAN DAN SARAN bab ini berisi kesimpulan tentang hasil-hasil penelitian sistem dan saran untuk pengembangan sistem.

Selain berisi bab-bab utama tersebut, Tugas Akhir ini juga dilengkapi dengan intisari, kata pengantar, daftar isi, daftar tabel, daftar gambar, daftar pustaka dan lampiran.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan percobaan terhadap system menggunakan Enkripsi AES dan RSA Blind Signature dapat ditarik kesimpulan sebagai berikut :.

- Percobaan dilakukan dengan double enkripsi, mulai dari AES dan hasil AES di enkripsi kembali oleh RSA Blind Signature, pengujian berhasil dan hasil perhitungan waktu prosesing data masih sangat cepat.
- Lebih baik system menggunakan metode enkripsi daripada hanya satu atau tidak sama sekali karena hasil eksekusi waktu hanya berbeda 0.10308408737183 detik
- Pengujian dilakukan oleh voters dengan melakukan double login menggunakan browser yang berbeda. System dapat mencegah terjadinya double login karena pada saat login pertama kali IP address voters langsung terdaftar pada database.
- Pengujian dilakukan oleh voters dengan double login menggunakan device yang berbeda, system dapat menagani hal tersebut dengan handal karena IP voters langsung terdaftar pertama kali login
- Pengujian dilakukan oleh voter dengan mengganti jadwal pada jam device yang digunakan disesuaikan dengan jadwal yang terdaftar, dan pada saat voters ingin memilih kandidat, user kembali lagi mengganti jadwal di device, dengan merefresh halaman, user tetap login namun pilihan kandidat tidak lagi tampil, dan system berhasil menangani hal tersebut.
- Pengujian system dilakukan oleh voters, setelah memilih kandidat, user mencoba kembali untuk memilih kandidat yang lain yang berada di daftar. Namun system berhasil mencegah dengan adanya status pemilih pada voters.

- Pengujian system oleh voters, mencoba melakukan lompatan web address dengan mengetik secara manual address yang ingin dituju. System dapat memblokir hal tersebut karena terdapat session yang seharusnya dirandom pada saat login pertama kali.

5.2 Saran

Adapun saran untuk mengembangkan sistem yang ada dalam penelitian ini. Sistem dalam penelitian dapat dikembangkan sehingga mampu menangani berbagai kemungkinan user melakukan percobaan kesalahan dan berbagai interupsi dan pengamanan data saat pemilihan terjadi dan untuk meregristrasi user dan kandidat dapat menggunakan metode yang lebih cepat daripada mendaftarkan user atau kandidat satu persatu karena memakan waktu yang sangat lama jika data yang diinputkan banyak.

Daftar Pustaka

Al-Hazaimeh A.M.O. (2013). *A New Approach For Complex Encrypting and Decrypting Data* .diakses tanggal 27 mei 2015 dari http://airccse.org/journal/cnc/5213cnc08.pdf.

Al-Shamaa, Khaled. (2007). *Encrypt And Decrypt with RSA Public Keys* .diakses tanggal 27 mei 2015 dari http://www.phpclasses.org/package/4121-PHP-Encrypt-and-decrypt-data-with-RSA-public-keys.html

Bellovin, Rebecca. (2014). *Cryptography: Authentication, Blind Signatures, and Digital Cash*. diaksestanggal 28 mei 2015 dari https://math.berkeley.edu/~rmb/writings/chaum.pdf.

Cid, Carlos, **Murphy**, Sean, **Robshaw**, Matthew. (2006). *Algebraic Aspects of the Advanced Encryption Standard*.USA :Springer.

Chaum, David (1983). *Blind signatures for untraceable payments*.Diakses tanggal 29 mei 2015 dari http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.

DI-Management. (2013). *RSA Algorithm* .diakses tanggal 28 mei 2015 dari http://www.di-mgt.com.au/rsa_alg.html

Federal Information Processing Standards Publication 197.(2001). Advanced Encryption Standard(AES). Diakses tanggal 26 mei 2015 dari http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Juels, Ari.,Luby, Michael. (2010). *Security of Blind Digital Signatures*.Diakses tanggal 20 mei 2010 darihttp://www.cs.ucla.edu/~rafail/PUBLIC/30.pdf.

Rivest, R., A. Shamir; L. Adleman .(1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* .diaksestanggal 27 mei 2015 dari http://people.csail.mit.edu/rivest/Rsapaper.pdf.

Ryan, Dermont. M. (2007).*Blind Signature and Implementation in RSA*. diaksestanggal 29 mei 2015 dari https://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/blind_sigs.html