IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION DENGAN PROTOKOL SHAMIR'S THRESHOLD SECRET SHARING PADA ELECTRONIC VOTING

Skripsi

©UKDW

oleh
MICHAEL CHRISTIAN
71120113

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI UNIVERSITAS KRISTEN DUTA WACANA

2016

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION DENGAN PROTOKOL SHAMIR'S THRESHOLD SECRET SHARING PADA ELECTRONIC VOTING

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

MICHAEL CHRISTIAN
71120113

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA

2016

©UKDW

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION DENGAN PROTOKOL SHAMIR'S THRESHOLD SECRET SHARING PADA ELECTRONIC VOTING

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, 10 Juni 2016

MICHAEL CHRISTIAN
71120113

©UKDW

HALAMAN PENGESAHAN

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION DENGAN PROTOKOL SHAMIR'S THRESHOLD SECRET SHARING PADA ELECTRONIC VOTING

Oleh: MICHAEL CHRISTIAN / 71120113

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 24 Mei 2016

Yogyakarta, 10 Juni 2016
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Ignatia Dhian E. K. R, S.Kom, M.Eng
3. Budi Susanto, SKom., M.T.
4. Restyandito, S.Kom.,MSIS, Ph.D

Dekan

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

Ketua Program Studi

(Gloria Virginia, Ph.D.)

v

©UKDW

UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan Yesus Kristus atassegala berkat, penyertaan, dan anugerah-Nya yang sudah diberikan kepada Penulis selama mengerjakan tugas akhir ini. Penulis juga ingin mengucapkan terima kasih kepada pihak-pihak yang telah memberikan banyak dukungan kepada Penulis, antara lain:

1. Keluarga yang senantiasa memberi dukungan dalam bentuk doa dan motivasi yang tidak henti-hentinya selama Penulis mengerjakan tugas akhir ini.
2. Bapak Willy Sudiarto Raharjo, S.Kom.,M.Cs. dan Ibu Ignatia Dhian E K R, S.Kom., M.Eng. selaku Dosen Pembimbing I dan II yang telah mendukung, membimbing, memberikan ide serta masukan-masukan bagi Penulis dalam pembuatan aplikasi, pelaksanaan penelitian, hingga penulisan laporan.
3. Teman-temanseperjuangan TI UKDW angkatan 2012 (terutama kepada Vivi Citra, Monica Natasha, Tiffany Widya, Pedro Nadirio, Michael Christian, Ady Purnama, Hendy Yudhitya) yang telah bersama-sama berjuang dalam menyelesaikan studi di prodi Teknik Informatika UKDW dan tugas akhir ini.
4. Pihak-pihak lain yang yang telah membantu jalannya pengerjaan tugas akhir ini baik secara langsung ataupun tidak langsung.

Yogyakarta, 12 Mei 2016

Michael Christian

©UKDW

INTISARI

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION DENGAN PROTOKOL SHAMIR'S THRESHOLD SECRET SHARING PADA ELECTRONIC VOTING

Voting adalah salah satu metode bagi rakyat untuk mengungkapkan pendapatnya tentang suatu topik tertentu, dengan kata lain suara adalah kunci demokrasi. Pada sistem *voting* yang sekarang digunakan, ada pengawasan ketat dari pemerintah untuk meyakinkan apakah voting sudah dijalankan secara benar atau tidak, selain itu juga untuk memastikan hanya orang – orang yang sudah memenuhi syarat tertentu yang dapat mengikuti *voting*. Saat ini masalah yang banyak terjadi pada saat *voting* adalah pembelian suara, di mana hak suara rakyat dapat dibeli untuk mendukung partai tertentu, selain itu proses *voting* yang sekarang diterapkan membutuhkan banyak dana dan upaya untuk mencapai keamanan yang diharapkan.

Bahasa yang digunakan dalam penelitian ini adalah PHP dan Javascript menggunakan software Sublime Text 2. Pemilihan Bahasa pemrograman PHP dan Javascript didasari atas pertimbangan bahwa bahasa pemrograman ini mendukung *library-library* yang menerapkan kriptografi, selain itu supaya aplikasi ini dapat diakses oleh banyak *device*.

Tujuan dari penelitian ini adalah membuat applikasi *e-voting* berbasis *web* menggunakan metode *Secure Multi-Party Computation* dengan protokol *Shamir's Threshold Secret Sharing* yang dapat mencegah dan mengetahui bila ada data *vote* yang tidak *valid.*

©UKDW

DAFTAR ISI

©UKDW

©UKDW

©UKDW

DAFTAR GAMBAR

©UKDW

©UKDW

INTISARI

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION DENGAN PROTOKOL SHAMIR'S THRESHOLD SECRET SHARING PADA ELECTRONIC VOTING

Voting adalah salah satu metode bagi rakyat untuk mengungkapkan pendapatnya tentang suatu topik tertentu, dengan kata lain suara adalah kunci demokrasi. Pada sistem *voting* yang sekarang digunakan, ada pengawasan ketat dari pemerintah untuk meyakinkan apakah voting sudah dijalankan secara benar atau tidak, selain itu juga untuk memastikan hanya orang – orang yang sudah memenuhi syarat tertentu yang dapat mengikuti *voting*. Saat ini masalah yang banyak terjadi pada saat *voting* adalah pembelian suara, di mana hak suara rakyat dapat dibeli untuk mendukung partai tertentu, selain itu proses *voting* yang sekarang diterapkan membutuhkan banyak dana dan upaya untuk mencapai keamanan yang diharapkan.

Bahasa yang digunakan dalam penelitian ini adalah PHP dan Javascript menggunakan software Sublime Text 2. Pemilihan Bahasa pemrograman PHP dan Javascript didasari atas pertimbangan bahwa bahasa pemrograman ini mendukung *library-library* yang menerapkan kriptografi, selain itu supaya aplikasi ini dapat diakses oleh banyak *device*.

Tujuan dari penelitian ini adalah membuat applikasi *e-voting* berbasis *web* menggunakan metode *Secure Multi-Party Computation* dengan protokol *Shamir's Threshold Secret Sharing* yang dapat mencegah dan mengetahui bila ada data *vote* yang tidak *valid.*

©UKDW

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Voting adalah salah satu metode bagi rakyat untuk mengungkapkan pendapatnya tentang suatu topik tertentu, dengan kata lain suara adalah kunci demokrasi. Pada sistem *voting* yang sekarang digunakan, ada pengawasan ketat dari pemerintah untuk meyakinkan apakah voting sudah dijalankan secara benar atau tidak, selain itu juga untuk memastikan hanya orang – orang yang sudah memenuhi syarat tertentu yang dapat mengikuti *voting*. Salah satu masalah yang terjadi saat ini adalah ketidakpercayaan kandidat pada penyelenggara *voting* dengan cara menuduh penyelenggara *voting* melakukan kecurangan atau manipulasi pada hasil *voting*, selain itu proses *voting* yang sekarang diterapkan membutuhkan banyak dana dan upaya untuk mencapai keamanan yang diharapkan.

Electronic voting dapat menjadi solusi untuk kelemahan sistem *voting* yang sebelumnya. *electronic voting* dapat menjaga privasi dari *voter*, di mana hanya dia sendiri yang tahu apa yang dia *vote*. Selain itu *electronic voting* dapat memberikan kepercayaan lebih pada kandidat dan masyarakat, karena data *vote* tidak disimpan terpusat melainkan satu data *vote* dapat disimpan terpisah, sehingga sulit untuk melakukan manipulasi. *Secure multi-party computation* adalah protokol, di mana sejumlah orang dalam satu grup dapat memperoleh dan menghitung secara bersama-sama suatu fungsi dari beberapa variabel yang diberikan oleh anggota grup dengan suatu cara tertentu. Hasil dari fungsi tersebut pada akhirnya akan diketahui oleh seluruh anggota grup, tetapi tidak satupun dari mereka yang mengetahui input yang dimasukkan oleh anggota yang lain dalam fungsi tersebut.

©UKDW

Penulis akan membuat sistem *electronic voting* berbasis *web* dengan mengimplementasikan *secure multi-party computation* menggunakan protokol *Shamir's threshold secret sharing*.

1.2. Rumusan Masalah

Dalam rangka membangun sistem elektronik voting dengan mengimplementasikan *secure multi-party computation*, hal yang perlu dipertimbangkan adalah bagaimana memverifikasi bila ada data *vote* yang tidak *valid*?

1.3. Batasan Masalah

Penelitian yang dilakukan memiliki beberapa batasan sebagai berikut :

1. Sistem berfokus pada keamanan data pada proses perhitungan suara.
2. Menggunakan *randomize algorithm*, sehingga meskipun dengan *input* yang sama, tetapi akan selalu menghasilkan *output* yang berbeda-beda, karena kemungkinan muncul *input* yang sama adalah besar (kandidat biasanya hanya sekitar 2 sampai 3 partai).
3. Menggunakan protokol *Shamir's Threshold Secret Sharing*, di mana *ciphertext* dibagi menjadi beberapa bagian dan diberikan pada masing-masing *collection centre*.
4. Menggunakan *RSA 128 bit* untuk enkripsi awal pada data *vote*.
5. Diasumsikan *server admin* aman.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah membuat applikasi *e-voting* berbasis *web* menggunakan metode *Secure Multi-Party Computation* dengan protokol *Shamir's Threshold Secret Sharing* yang dapat mencegah dan mengetahui bila ada data *vote* yang tidak *valid.*

©UKDW

1.5. Metode Penelitian

Tahapan yang dilakukan dalam penelitian ini adalah :

1. Metode pengumpulan data-data referensi

   Mengumpulkan dan mempelajari bahan-bahan referensi yang berhubungan dengan kriptografi *Secure Multi-Party Protocol, Shamir Threshold Secret Sharing, RSA.*

2. Metode Pembuatan Sistem

   Mengimplementasikan hasil studi yang sudah dipelajari kedalam bentuk aplikasi *web-based.*

3. Metode Pengujian Sistem

   Melakukan pengujian terhadap sistem yang telah dibuat dengan menjalankan sistem sesuai role untuk mengetahui keberhasilan sistem, dan mencoba melakukan manipulasi data pada sistem untuk mengetahui seberapa aman algoritma yang digunakan.

4. Dokumentasi Sistem

   Penyusunan laporan tugas akhir sesuai dengan analisis yang didapatkan.

©UKDW

1.6. Sistematika Penulisan

Sistematika penulisan terdiri dari lima bab, di mana secara garis besar masing-masing bab membahas hal-hal sebagai berikut.

Bab 1 Pendahuluan, berisi penjelasan umum tentang penelitian yang akan dilakukan. Bab ini terdiri dari tujuh bagian, yaitu latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab 2 Landasan Teori, bab ini terbagi menjadi dua bagian, yaitu tinjauan pustaka dan landasan teori. Tinjauan pustaka digunakan sebagai acuan untuk menguraikan teori-teori dari berbagai sumber pustaka untuk mendukung proses pemecahan masalah pada penelitian. Landasan teori berisi teori-teori yang relevan dan dapat digunakan untuk menjelaskan variable-variabel penelitian.

Bab 3 Analisis dan Perancangan sistem, berisi indentifikasi masalah, peluang dan tujuan dengan berpedoman pada teori-teori yang ada dan bagaimana menerjemahkannya ke dalam suatu sistem yang hendak dibuat. Pada dasarnya bab ini memuat perancangan sistem secara keseluruhan.

Bab 4 Implementasi dan Analisis Sistem, berisi penjelasan bagaimana rancangan pada bab 3 diimplementasikan dan diuji, beserta hasil dari sistem yang dijalankan dan analisa dari sistem yang dibuat.

Bab 5 Kesimpulan dan Saran, berisi kesimpulan apa saja yang diperoleh dari hasil penelitian yang telah selesai dilakukan dan saran untuk memberikan hasil yang lebih baik dalam penelitian yang sejenis.

©UKDW

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil implementasi dan analisis yang telah dibuat dan dibahas pada bab sebelumnya, maka dapat disimpulkan :

1. Data *vote* pada proses transmisi telah dienkripsi sehingga apabila data berhasil disadap, *attacker* tidak dapat mengetahui isi data *vote*.
2. Sistem dapat mendeteksi pihak yang memiliki kunci *invalid,* dengan cara mencocokan masing – masing kunci yang didapat dari *collection centre* dengan kunci cadangan pada *server admin,* melalui hal ini akan didapat *collection centre* yang memiliki data *invalid*.
3. Bila semua kunci pada *collection centre invalid* pada suatu data *vote*, maka data tersebut tidak dapat di rekonstruksi ulang.

5.2. Saran

Untuk meingkatkan kinerja dari sistem ini dapat dilakukan dengan meningkatkan keamanan pada saat melakukan *vote,* terkhusus ketika salah satu proses *insert* di *server* kandidat gagal atau salah satu proses *collect* di *server* kandidat gagal, maka proses *insert* atau *collect* yang lain juga harus dibatalkan.

©UKDW

Daftar Pustaka

Meijering, E. (2002, 08 07). A chronology of interpolation: from ancient astronomy to modern signal and image processing. *Proceedings of the IEEE* , pp. 319-342.

Horner, W. G. (1819). A new method of solving numerical equations of all orders, by continuous approximation. Royal Society of London.

Method for Polynomial Evaluation. (n.d.). Retrieved from GeeksforGeeks: http://www.geeksforgeeks.org/horners-method-polynomial-evaluation/

D. L. (2010). Component Based Electronic Voting Systems. In D. L., D. C., Markus Jackobsson, R. L. Rivest, P. Y. Ryan, J. B., M. K., & B. A. (Eds.), *Towards Trustworthy Elections* (Vol. 6000, pp. 260-273). Springer Berlin Heidelberg.

Syahroni, Z. G., Adi, H. D., & A. M. (2011). *Secret Sharing Schemes.* Universitas Jember.

Mollin, R. A. (2008). *An Introduction to Cryptography, Second Edition* (Vol. 50).

Lestariningati, S. I. (2009, 05). Desain Sistem On-Site Voting Untuk Mengatasi Fraud. *Seminar Nasional Informatika*, 81-86.

Kaliski, B. (2006, 04). The Mathematics of the RSA Public-Key Cryptosystem. *Mathematics Awareness Month*.

Nair, D. G., Kumar, S., & Binu, V. P. (2015, 02). An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation.

Based, M. A., Reistad, T. I., & Mjolsnes, S. F. (2009). Internet Voting using Multiparty Computations. *The Norwegian Information Security Conference*, 136-147.

Kurahara, J., Kiyomoto, S., Fukushima, K., & Tanaka, T. (2008). A New (k, n)-Threshold Secret Sharing Scheme and Its Extension⋆. In T.-C. Wu, C.-L. Lei, V. Rijmen, & D.-T. Lee (Eds.), *Information Security* (pp. 455-470). Springer Berlin Heidelberg.

©UKDW

Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography.*

Fadil, L. E. (n.d.). An Electronic Voting Based On Multi-Party Computation.

©UKDW