IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL

SKRIPSI

Oleh:

PEDRO NADIRIO ADHIREKSAN

71120002

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

2016

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL

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:

PEDRO NADIRIO ADHIREKSAN
71120002

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2016

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL

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, 8 Juni 2016

PEDRO NADIRIO ADHIREKSAN
71120002

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL
Nama Mahasiswa	:	PEDRO NADIRIO ADHIREKSAN
N I M	:	71120002
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2015/2016

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 8 Juni 2016

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Antonius Rachmat C., S.Kom.,M.Cs.

HALAMAN PENGESAHAN

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL

Oleh: PEDRO NADIRIO ADHIREKSAN / 71120002

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 2 Juni 2016

Yogyakarta, 8 Juni 2016
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Antonius Rachmat C., S.Kom.,M.Cs.
3. Budi Susanto, SKom.,M.T.
4. Hendro Setiadi, M.Eng

Dekan

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

Ketua Program Studi

(Gloria Virginia, Ph.D.)

UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan Yesus Kristus atas segala 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 Bapak Antonius Rachmat C, S.Kom., M.Cs. selaku Dosen Pembimbing I dan II yang telah mendukung, membimbing, memberikan ide serta masukan-masukan bagi Penulis dalam pembuatan sistem, pelaksanaan penelitian, hingga penulisan laporan.
3. Teman-teman yang telah membantu menjadi responden dalam penelitian-penelitian yang dilakukan Penulis sehingga tugas akhir ini dapat berjalan dengan lancar.
4. Teman-teman seperjuangan TI UKDW angkatan 2012 (terutama kepada Vivi Citra, Monica Natasha, Henry Susilo, Tiffany Widya, Michael Christian, Ady Purnama, Hendy Yudhitya) yang telah bersama-sama berjuang dalam menyelesaikan studi di prodi Teknik Informatika UKDW dan tugas akhir ini.
5. Pihak-pihak lain yang yang telah membantu jalannya pengerjaan tugas akhir ini baik secara langsung ataupun tidak langsung.

Yogyakarta, 12 Mei 2016

Pedro Nadirio Adhireksan

INTISARI

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL

Keamanan sebuah data yang bersifat rahasia merupakan suatu hal yang penting dan dipertimbangkan pada era digital saat ini. Setiap pemilik data rahasia tentu tidak ingin apabila datanya dapat diakses atau bahkan diubah seenaknya oleh pihak tertentu dengan tujuan yang tidak baik. Setiap data seharusnya hanya dapat diakses oleh pihak-pihak yang memiliki hak akses terhadap data tersebut. Dalam beberapa kasus, terdapat sebuah data rahasia yang hanya dapat diakses apabila terdapat sejumlah pihak yang memiliki hak akses bersedia untuk mengakses rahasia tersebut. Apabila pihak yang akan mengakses sebuah rahasia berjumlah kurang dari nilai yang telah tentukan, maka rahasia tersebut tidak dapat diakses. Proses pengaksesan data secara kelompok tersebut tidak dapat dilakukan oleh sembarang pihak yang tidak memiliki hak akses atau mencoba mengakses data rahasia dengan cara yang tidak semestinya.

Sistem yang akan dibangun adalah sistem pengamanan sebuah data rahasia yang hanya dapat diakses apabila setiap pihak pemilik hak akses bersedia mengakses data rahasia tersebut secara bersamaan. Penelitian akan dilakukan dengan tujuan menguji apakah sistem yang dibangun berhasil mengamankan sebuah data rahasia dalam bentuk digital. Penelitian yang dilakukan juga meliputi pengujian terhadap kemampuan sistem dalam menangani setiap tindakan curang yang dilakukan oleh pihak-pihak tertentu. Dari hasil penelitian yang telah dilakukan, sistem berhasil untuk mengamankan data rahasia dalam bentuk digital serta menangani setiap tindakan curang yang dilakukan serta mendeteksi pihak yang melakukan kecurangan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

IMPLEMENTASI SECURE MULTI-PARTY COMPUTATION MENGGUNAKAN METODE SHAMIR SECRET SHARING PADA PENGAMANAN DOKUMEN RAHASIA DIGITAL

Keamanan sebuah data yang bersifat rahasia merupakan suatu hal yang penting dan dipertimbangkan pada era digital saat ini. Setiap pemilik data rahasia tentu tidak ingin apabila datanya dapat diakses atau bahkan diubah seenaknya oleh pihak tertentu dengan tujuan yang tidak baik. Setiap data seharusnya hanya dapat diakses oleh pihak-pihak yang memiliki hak akses terhadap data tersebut. Dalam beberapa kasus, terdapat sebuah data rahasia yang hanya dapat diakses apabila terdapat sejumlah pihak yang memiliki hak akses bersedia untuk mengakses rahasia tersebut. Apabila pihak yang akan mengakses sebuah rahasia berjumlah kurang dari nilai yang telah tentukan, maka rahasia tersebut tidak dapat diakses. Proses pengaksesan data secara kelompok tersebut tidak dapat dilakukan oleh sembarang pihak yang tidak memiliki hak akses atau mencoba mengakses data rahasia dengan cara yang tidak semestinya.

Sistem yang akan dibangun adalah sistem pengamanan sebuah data rahasia yang hanya dapat diakses apabila setiap pihak pemilik hak akses bersedia mengakses data rahasia tersebut secara bersamaan. Penelitian akan dilakukan dengan tujuan menguji apakah sistem yang dibangun berhasil mengamankan sebuah data rahasia dalam bentuk digital. Penelitian yang dilakukan juga meliputi pengujian terhadap kemampuan sistem dalam menangani setiap tindakan curang yang dilakukan oleh pihak-pihak tertentu. Dari hasil penelitian yang telah dilakukan, sistem berhasil untuk mengamankan data rahasia dalam bentuk digital serta menangani setiap tindakan curang yang dilakukan serta mendeteksi pihak yang melakukan kecurangan.

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Keamanan sebuah data yang bersifat rahasia merupakan suatu hal yang penting dan dipertimbangkan pada era digital saat ini. Setiap pemilik data rahasia tentu tidak ingin apabila datanya dapat diakses atau bahkan diubah seenaknya oleh pihak tertentu dengan tujuan yang tidak baik. Setiap data seharusnya hanya dapat diakses oleh pihak-pihak yang memiliki hak akses terhadap data tersebut. Dalam beberapa kasus, terdapat sebuah data rahasia yang hanya dapat diakses apabila terdapat sejumlah pihak yang memiliki hak akses bersedia untuk mengakses rahasia tersebut. Apabila pihak yang akan mengakses sebuah rahasia berjumlah kurang dari nilai yang telah tentukan, maka rahasia tersebut tidak dapat diakses. Proses pengaksesan data secara kelompok tersebut tidak dapat dilakukan oleh sembarang pihak yang tidak memiliki hak akses atau mencoba mengakses data rahasia dengan cara yang tidak semestinya.

Melihat fakta bahwa pengamanan data menjadi sebuah hal yang penting, muncul sebuah gagasan untuk membuat sebuah sistem pengamanan untuk melindungi data tersebut dari pihak yang tidak bertanggung jawab. Data rahasia dalam bentuk digital akan diamankan dengan metode-metode yang terdapat pada bidang ilmu kriptografi sehingga pada akhirnya data tersebut tidak dapat diakses secara sembarangan. Setiap data rahasia yang akan diamankan dibagi menjadi beberapa bagian yang nantinya setiap bagian diberikan kepada setiap pihak yang memiliki hak akses terhadap rahasia tersebut. Untuk membentuk kembali rahasia yang telah diamankan, diperlukan kontribusi setiap pihak yang memiliki akses dan memiliki bagian dari rahasia yang telah diamankan. Rahasia hanya dapat terbentuk kembali

apabila terdapat bagian rahasia yang valid dalam jumlah tertentu serta setiap bagian terverifikasi dengan tepat.

Untuk menerapkan pengamanan data yang hanya dapat diakses apabila terdapat kontribusi dari beberapa pihak tertentu, maka penulis akan membuat sebuah skema pengamanan yang menggunakan metode-metode dalam ilmu kriptografi. Sebuah data rahasia dalam bentuk digital akan dienkripsi dengan menggunakan algoritma *AES* (*Advanced Encryption Standard*) yang masih tergolong aman dan sulit untuk dipecahkan. Dalam proses enkripsi ini diperlukan sebuah kunci yang nantinya juga akan digunakan untuk proses dekripsi. Kunci ini akan dibagi kepada sejumlah pihak yang memiliki hak akses dan *trusted party* yang bisa berupa *escrow* dengan konsep *Secure Multiparty Computation* menggunakan skema *Shamir' Secret Sharing. Secret Sharing* merupakan sebuah teknik pengamanan dengan cara memecah rahasia dan mendistribusikannya ke sejumlah pihak (Bogdanov, 2007). Sistem yang dibangun dapat mendeteksi apabila terdapat bagian rahasia yang tidak valid atau proses verifikasi bagian rahasia yang tidak tepat. Pada akhirnya, data rahasia yang telah diamankan hanya dapat diakses oleh pihak yang memiliki hak akses, sehingga pihak lain bahkan pihak *server* tidak dapat melakukan akses ke data rahasia tersebut.

1.2. Rumusan Masalah

Rumusan masalah yang menjadi dasar dalam kasus ini adalah bagaimana mengintegrasikan *Secure Multiparty Computation* menggunakan *Shamir's Secret Sharing* dengan kriptografi untuk mengamankan dan mendistribusikan pesan rahasia serta menguji keamanan metode yang digunakan.

1.3. Batasan Masalah

Agar sistem tidak menyimpang dari ruang lingkup pembahasan, diperlukan batasan masalah sebagai berikut:

1. Dokumen Rahasia diamankan menggunakan algoritma *Advanced Encryption Standard* 256-bits dengan menggunakan kunci yang degenerate oleh sistem sebelum dipecah menggunakan *Shamir's Secret Sharing Scheme*.
2. Kunci terenkripsi untuk membuka Dokumen Rahasia akan didistribusikan ke jumlah yang telah ditentukan pemilik Dokumen Rahasia yaitu sejumlah partisipan. Banyaknya jumlah pecahan kunci yang dapat dihasilkan sistem berjumlah antara 1 – 100 pecahan kunci.
3. Dokumen Rahasia dapat dibuka hanya bila setiap partisipan memberikan kunci yang valid tanpa adanya satu kunci pun yang palsu.
4. Dokumen Rahasia yang dapat diamankan dapat berupa *plaintext* atau beberapa format file seperti .txt, .pdf, .mp3, .jpg,. png dengan ukuran tidak lebih dari 1 MB.

1.4. Tujuan Penelitian

Tujuan dari penulisan tulisan ini adalah untuk membangun sistem pengamanan dokumen rahasia dalam bentuk digital dengan menerapkan *Multi-party Computation* menggunakan protokol *Shamir Secret Sharing Scheme* serta menguji skema dan metode yang digunakan dalam sistem.

1.5. Metode Penelitian

1. Metode Studi Literatur
2. Penulis melakukan studi pustaka yang dilakukan dengan cara mempelajari teori-teori dan literature yang berkaitan dengan *multi-party computation* dan protokol *Shamir Secret Sharing* untuk

mendukung pembangunan sistem. Analisa Masalah dan Perancangan Sistem

Melakukan analisis masalah yang dimulai dengan identifikasi masalah, memahami kerja sistem yang akan dibuat, serta membuat rancangan dan *interface* sistem.

3. Implementasi Sistem

   Perancangan sistem diimplementasikan dalam bentuk kode program (*coding*) berbasis web.

4. Pengujian Sistem

   Pengujian dilakukan terhadap program yang telah dibuat. Pengujian ini juga mencakup keamanan, seperti dilakukan uji coba kecurangan-kecurangan yang mungkin terjadi seperti percobaan pemalsuan kunci, percobaan pembukaan dokumen rahasia dengan jumlah kunci yang tidak sesuai, dan sebagainya.

5. Dokumentasi Sistem

   Penyusunan laporan tugas akhir lengkap dengan analisis yang didapatkan.

1.6. Sistematika Penulisan

Pada Bab 1 berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan. Sub-bab pertama dari Bab 1 membahas mengenai latar belakang masalah dari pembuatan sistem keamanan dokumen rahasia digital, kemudian pada Sub-bab kedua akan dirumuskan poin-poin masalah yang akan diselesaikan. Batasan-batasan sistem yang dibuat akan dijelaskan pada Sub-bab ketiga dan dilanjutkan dengan tujuan serta metode yang akan dilakukan dalam penelitian.

Pada Bab 2 berisi tinjauan pustaka dan landasan teori bagi perancangan sistem. Pada Bab ini juga dijelaskan hal yang mendukung pembuatan sistem keamanan dokumen rahasia digital, termasuk

didalamnya terdapat penjelasan tentang algoritma penglahan citra, perhitungan matriks dan algoritma yang berupa diagram flow atau pseudocode.

Pada Bab 3 berisi perancangan sistem, dimulai dari daftar kebutuhan sistem yang akan dibuat, struktur atau cara kerja sistem yang dijelakan dengan diagram flow, kebutuhan sistem akan perangkat hardware atau software, desain interface untuk pengguna dan perancangan pengujian sistem.

Pada Bab 4 berisi capture dari hasil implementasi pada sistem yang telah dibuat. Hasil yang sudah tercapture disertai dengan penjelasan tentang kegunaan, alur dan hasil yang didapatkan dari tiap fungsi dalam sistem. Juga menjelaskan tentang hasil analisa mengenai seberapa optimal metode yang dipilih untuk memecahkan permasalahan yang ada.

Pada Bab 5 berisi kesimpulan dari apa yang telah dibahas pada bab-bab sebelumnya dan sekaligus menjawab apa yang menjadi permasalahan terutama pada Bab 1 Sub-bab yang kedua yaitu tentang perumusan masalah. Selain itu penulis juga menguraikan kesulitan-kesulitan yang dihadapi dalam pembuatan sistem. Jika penulis memiliki ide untuk penulisan lanjutan, maka penulis dapat mencantumkan Sub-bab baru tentang saran, yang berisi tentang rujukan penelitian lanjutan atau pengembangan sistem dari sistem yang telah dibuat ini.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi sistem dan analisis yang telah dilakukan, maka dapat disimpulkan beberapa hal sebagai berikut:

1. Rahasia yang dimasukkan pengguna berhasil diamankan dengan metode *Shamir Secret Sharing Scheme*. Rahasia hanya dapat terbentuk kembali apabila terdapat setiap pecahan kunci yang valid. Terbukti bahwa dengan adanya sebuah kunci saja yang bernilai tidak valid, rahasia tidak dapat terbentuk kembali.
2. Sistem telah berhasil mendeteksi tindak kecurangan pemalsuan pecahan kunci untuk membuka sebuah rahasia. Sistem meggunakan pecahan kunci cadangan untuk melakukan proses deteksi kecurangan tersebut.
3. Pemalsuan pecahan kunci dengan cara mengubah sebagian nilai dari kunci tanpa mengubah ukuran kunci akan tetap menghasilkan sebuah rahasia walau tidak sempurna. Hal ini tidak dapat diatasi oleh algoritma *Shamir Secret Sharing Scheme* karena rahasia tetap dapat terbentuk walau tidak sesuai dengan rahasia awal dan tidak memberi dampak *error*. Untuk mengatasi hal ini, sistem menyimpan *hashed secret* untuk dibandingkan dengan rahasia yang berhasil dibentuk. Terbukti sistem dapat mendeteksi apabila terdapat indikasi pemalsuan kunci.
4. Untuk lebih meningkatkan keamanan sebuah rahasia, maka pada alur proses pengamanan diperlukan sebuah *PassCode*. Dengan adanya pengamanan tambahan dengan *PassCode* ini, maka hanya pihak yang memiliki *PassCode* yang dapat membuka rahasia. Sistem sekalipun tidak dapat mencoba membuka rahasia tanpa adanya *PassCode* yang sesuai.
5. Apabila terdapat pecahan kunci valid yang hilang maka rahasia tidak dapat lagi terbentuk. Hal ini telah dapat diatasi dengan cara menyediakan fitur

Request Key yang digunakan untuk meminta kunci cadangan yang disimpan sistem. Terbukti kunci cadangan yang disimpan, dapat digunakan untuk pembentukan kembali rahasia.

6. Karena terdapat kunci cadangan yang disimpan di dalam server, maka pihak yang memiliki hak menggunakan fitur *Request Key* dapat melakukan tindakan curang untuk membuka rahasia tanpa kontribusi pihak pemilik pecahan kunci. Apabila hal tersebut terjadi, maka sistem tidak dapat mencegah hal tersebut.

5.2 Saran

Untuk pengembangan sistem lebih lanjut, dapat dilakukan dengan cara mengembangkan sistem pengamanan Dokumen Rahasia Digital pada *platform* lain seperti pada *smartphone Android* atau *iOS*. Hal tersebut dapat dilakukan karena sistem pengamanan Dokumen Rahasia Digital cocok diimplementasikan pada *mobile device* karena memberi kemudahan akses yang lebih baik bagi penggunanya. Terdapat hal yang perlu diperhatikan untuk pengembangan sistem pada *mobile device*, yaitu bagaimana cara mengintegrasikan setiap proses yang terdapat pada sistem seperti proses pengumpulan kembali pecahan kunci sehingga nyaman dan mudah digunakan oleh penggunanya.

DAFTAR PUSTAKA

Bogdanov, D. (2007, May 1). Foundations and properties of Shamir's secret sharing scheme Research Seminar in Cryptography.

Boneh, D. (2012). Cryptography 1. Stanford University.

Cramer, R., Damgard, I., & Nielsen, J. B. (2012, December 31). Secure Multiparty Computation and Secret Sharing. *An Information Theretic Approach*, 27-40.

Goubin, L., & Martinelli, A. (2011). *Protecting AES with Shamir's Secret Sharing Scheme*.

Hirt, M. (2001). Multi-Party Computation. *Efficient Protocols, General Adversaries, and Voting*.

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

Katz, J., & Lindell, Y. (2008). *Introduction to Modern Cryptography*. New York: Chapman & Hall/CRC.

Kesiman, M. W., & Munir, R. (2004). *Penerapan Secret Sharing Scheme Pada Joint Ownership Watermarking Untuk Citra Digital*, 2-3.

Mahajan, P., & Abhishek, S. (2013). *A Study of Encryption Algorithms AES, DES and RSA for Security*.

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.

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

Mollin, R. (2007). *An Introduction to Cryptography (2nd edition).* Florida: Chapman & Hall/CRC.

Relan, V. (2009). *Secret Sharing*. Retrieved 2015, from UMBC: http://userpages.umbc.edu/~relan1/Day1%20Secret%20Sharing.pdf

Rivest, Ronald L. (2003). RSA Problem.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd edition).* New Jersey: John Wiley & Sons, Inc.

Yuniati, V., Indiyanta, G., & Rachmat, A. (2009). *Enkripsi dan Dekripsi dengan Algoritma AES 256 Untuk Semua Jenis File*.