IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET

Skripsi

oleh
EKO SULARSONO
22084479

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

IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET

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

EKO SULARSONO
22084479

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

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET

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, 1 Oktober 2014

EKO SULARSONO
22084479

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET
Nama Mahasiswa	:	EKO SULARSONO
N I M	:	22084479
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2014/2015

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 11 September 2014

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, SKom.,M.Cs	Yuan Lukito, S.Kom., M.Cs.

HALAMAN PENGESAHAN

IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET

Oleh: EKO SULARSONO / 22084479

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 26 September 2014

Yogyakarta, 1 Oktober 2014
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Yuan Lukito, S.Kom., M.Cs.
3. Budi Susanto, SKom.,M.T.
4. Erick Purwanto, S.Kom, M.Com.

Dekan	Ketua Program Studi
(Drs. Wimmie Handiwidjojo, MIT.)	(Nugroho Agus Haryono, M.Si)

UCAPAN TERIMAKASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan kasih-Nya sehingga penulis dapat menyelesaikan laporan Tugas Akhir dengan judul "Implementasi Algoritma Rijndael 128 Pada Aplikasi Chatting Berbasis HTML5 Websocket" dengan baik pada waktu yang tepat. Penulisan laporan ini merupakan kelengkapan dan pemenuhan bagi penulis sebagai syarat dalam memperoleh gelar Sarjana Komputer. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan melatih mahasiswa khususnya penulis agar dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan penelitian dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, masukan dan dukungan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Willy Sudiarto Raharjo, S.Kom., M.Cs. selaku dosen pembimbing I yang selalu sabar dalam membimbing, memberi masukan dan memberi arahan hingga Tugas Akhir ini terselesaikan.
2. Bapak Yuan Lukito, S.Kom., M.Cs. selaku dosen pembimbing II yang selalu sabar dalam membimbing, memberi masukan dan memberi arahan hingga Tugas Akhir ini terselesaikan.
3. Keluarga Petrus Sumarsono – Emiliana Suliyanti yang selalu memberikan dukungan, semangat dan doa.
4. Para sahabat, teman dan pihak lain yang tidak dapat penulis sebutkan satu per satu atas dukungan dan semangat yang diberikan.
5. Semesta yang telah memberi kesempatan sehingga Tugas Akhir ini dapat terselesaikan dengan baik pada waktu yang tepat.

Penulis menyadari bahwa penelitian dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian, sehingga suatu saat nanti penulis dapat memberikan karya yang lebih baik lagi. Akhir kata, dengan menyadari kekurangan dan keterbatasan yang dimiliki, penulis menyampaikan permohonan maaf yang sebesar-besarnya apabila ada kesalahan dalam penyusunan laporan Tugas Akhir ini. Semoga penelitian dan laporan Tugas Akhir ini dapat berguna bagi kita semua.

Yogyakarta, September 2014

Penulis

INTISARI

IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET

Telah banyak inovasi dan terobosan untuk menciptakan layanan komunikasi yang bisa diandalkan. Salah satu inovasi yang saat ini digemari banyak orang adalah layanan *chatting* berbasis web. Sebagai media komunikasi jarak jauh yang dapat diandalkan, layanan *chatting* berbasis web dituntut untuk mampu mengirim dan menerima pesan dalam waktu yang singkat. Selain itu, distribusi pesan instan pada layanan tersebut juga harus dipertimbangkan aspek keamanannya, sehingga keaslian dan kerahasiaan pesan instan yang dikirim atau diterima tetap terjaga.

Sebagai pemenuhan kebutuhan komunikasi *realtime* jarak jauh, pada penelitian ini dibangun aplikasi *chatting* berbasis HTML5 WebSocket menggunakan library Socket.IO. Teknik kriptografi Rijndael 128 selanjutnya diterapkan untuk mengamankan distribusi pesan instan pada aplikasi *chatting* yang dibuat. Selelah teknologi kriptografi Rijndael terimplementasikan, dilakukan pengujian untuk menguji seberapa aman distribusi pesan instan dalam perjalanan dan keamanan data pengguna yang tersimpan pada server.

Algoritma Rijndael dapat diimplementasikan pada aplikasi *chatting* berbasis HTML5 WebSocket yang dibangun. Pengujian yang telah dilakukan pada aplikasi tersebut menunjukkan bahwa implementasi algoritma Rijndael dapat mengamankan data pengguna yang tersimpan pada server. Penerapan teknologi kriptografi Rijndael pada sistem distribusi pesan instan juga memberi keamanan pada paket data pesan dalam perjalanan.

Kata Kunci: kriptografi, Rijndael, enkripsi, dekripsi, WebSocket, chatting

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Komunikasi berlaku mutlak dalam kehidupan manusia karena merupakan sarana antar manusia agar tetap terhubung satu dengan yang lain. Salah satu media komunikasi yang sangat digemari saat ini adalah aplikasi *chatting* berbasis web. Kerahasiaan pesan instan pada aplikasi chatting berbasis web menjadi hal yang vital dan krusial sehingga membutuhkan sistem keamanan. Pesan instan yang dikirim atau diterima dapat bersifat rahasia dan eksklusif, sehingga pengguna tidak menginginkan pesan tersebut diketahui oleh pihak yang tidak memiliki hak.

Distribusi pesan instan yang memiliki informasi berharga pada aplikasi *chatting* dapat diamankan dengan menggunakan suatu teknik penyandian yang biasa disebut dengan kriptografi. Rijndael 128 pada Mei 2002 dijadikan standar algoritma kriptografi oleh pemerintah federal Amerika Serikat. Pada tahun 2000 Henri Gilbert dan Marine Minier melakukan kriptoanalisis terhadap algoritma Rijndael 128. Kriptoanalisis yang dilakukan hanya dapat menembus 7 dari 10 ronde yang ada pada algoritma Rijndael 128. Mereka menyimpulkan bahwa bahwa algoritma Rijndael 128 cukup aman dan handal karena memiliki kompleksitas yang sangat tinggi.

Aplikasi *chatting* berbasis web tentu akan sangat sulit diciptakan jika pengembang halaman web hanya mengandalkan kemampuan yang ada pada HTML tradisional. Teknologi terbaru pada HTML5 yaitu WebSocket memungkinkan pengembang halaman web menciptakan aplikasi *real time* yang lebih canggih dibandingkan menggunakan metode-metode terdahulu seperti polling, long polling dan HTTP streaming. Evaluasi kinerja arsitektur web modern yang dilakukan oleh Johan Andre Lundar, Tor-Morten Grønli dan Gheorghita

Ghinea pada tahun 2013 menyimpulkan bahwa penggunaan protokol WebSocket dapat meningkatkan fleksibilitas dan keandalan suatu website. WebSocket menjadi salah satu pilihan terbaik saat ini untuk menunjang kebutuhan komunikasi *real time* yang dibutuhkan oleh aplikasi *chatting* berbasis web.

Pada penelitian ini akan dibuat aplikasi *chatting* berbasis HTML5 WebSocket untuk meningkatkan fleksibilitas, keandalan serta memenuhi kebutuhan komunikasi *real time* jarak jauh. Teknik kriptografi Rijndael 128 akan diterapkan untuk mengamankan distribusi pesan instan pada aplikasi *chatting* berbasis HTML5 WebSocket yang akan dibuat.

1.2. Rumusan Masalah

Rumusan masalah yang ada dalam penelitian ini adalah bagaimana membuat aplikasi *chatting* yang aman berbasis HTML5 WebSocket dengan menggunakan teknologi enkripsi dan dekripsi Rijndael 128.

1.3. Batasan Masalah

Batasan-batasan pada penelitian ini adalah:

a Algoritma yang digunakan adalah algoritma Rijndael 128 bit.

b Algoritma Rijndael 128 hanya digunakan untuk enkripsi dan dekripsi pesan instan yang bertipe *plain text* (ASCII).

c Aplikasi *chatting* yang dibuat tidak menyediakan fitur *attachment.*

1.4. Hipotesis

Algoritma Rijndael 128 dapat diimplementasikan pada aplikasi *chatting* berbasis HTML5 WebSocket sehingga distribusi pesan instan pada aplikasi tersebut dapat terjaga keaslian, keamanan dan kerahasiaannya.

1.5. Tujuan Penelitian

Tujuan dari penelitian pada penulisan Tugas Akhir ini adalah :

a. Membuat aplikasi *chatting* berbasis HTML5 WebSocket dengan menggunakan algoritma Rijndael 128 untuk enkripsi dan dekripsi pesan instan yang dikirim atau diterima melalui aplikasi tersebut.
b. Menguji seberapa aman aplikasi *chatting* berbasis HTML5 WebSocket yang menggunakan algoritma Rijndael 128 untuk enkripsi dan dekripsi pesan instan yang dikirim atau diterima melalui aplikasi tersebut.

1.6. Metode Penelitian

Metode yang digunakan dalam penulisan tugas akhir ini adalah :

a Melakukan studi pustaka/literatur untuk mempelajari materi atau teori-teori terkait penelitian yang akan dilaksanakan. Semua informasi dan data yang dibutuhkan dalam penelitian ini dikumpulkan dari buku dan Internet.
b Merancang dan membangun aplikasi *chatting* berbasis HTML5 WebSocket.
c Merancang dan menguji program enkripsi dan dekripsi *plain text* (ASCII) untuk pesan instan dengan menggunakan algoritma Rijndael 128.
d Mengimplementasikan program algoritma Rijndael 128 untuk enkripsi dan dekripsi pesan instan dengan aplikasi *chatting* berbasis HTML5 WebSocket.
e Menguji aplikasi *chatting* berbasis HTML5 WebSocket yang telah terimplementasi dengan program enkripsi dan dekripsi pesan instan menggunakan algoritma Rijndael 128.
f Membuat laporan dan kesimpulan dari hasil pengujian dan analisis yang diperoleh.

1.7. Sistematika Penulisan

Sistematika penulisan tugas akhir ini dijabarkan menjadi 5 bagian utama. Bab 1 merupakan pendahuluan, yang memberi gambaran tentang penelitian yang akan dilakukan. Pendahuluan berisi latar belakang masalah, rumusan masalah, batasan masalah, hipotesis, tujuan penelitian, metode penelitian dan sistematika penulisan. Bab 2 merupakan tinjauan pustaka, yang terdiri dari dua bagian utama yaitu tinjauan pustaka dan landasan teori. Tinjauan pustaka dan landasan teori akan menguraikan berbagai teori yang mendukung dan menjadi dasar untuk memecahkan masalah dalam penelitian yang dilakukan. Bab 3 merupakan analisis dan perancangan sistem, berisi tentang perancangan sistem secara keseluruhan. Analisis dan perancangan sistem mencakup kebutuhan sistem, blok diagram sistem, *flowchart*, desain input-output dan rancangan pengujian.

Bab 4 merupakan implementasi dan analisis sistem, yang memuat hasil implementasi program dan analisis/pembahasan dari hasil yang diperoleh secara detail. Bab 5 merupakan kesimpulan dan saran, yang merupakan bagian akhir dari laporan. Kesimpulan merupakan jawaban dari pertanyaan yang ada pada rumusan masalah penelitian, sedangkan saran mencakup metode/ pengembangan yang belum dilakukan pada penelitian ini. Saran tersebut diharapkan dapat memperbaiki kinerja sistem jika diterapkan pada penelitian selanjutnya.

BAB 5
KESIMPULAN

5.1. Kesimpulan

Setelah dilakukan pengujian dan analisis terhadap aplikasi yang telah dibuat, dapat disimpulkan bahwa:

1. Penggunaan *platform* Node.js memberi kemudahan dalam membangun aplikasi *chatting* dengan performa baik dan cepat. Hal ini disebabkan karena Node.js memiliki fitur *non-blocking I/O* yang sangat dibutuhkan pada aplikasi *realtime.*
2. Socket.IO menyediakan fitur transport dengan protokol WebSocket dan dapat digunakan berdampingan dengan Node.js. Hal ini membuat komunikasi *realtime* antara client dan server pada aplikasi *chatting* yang dibuat dapat diakomidir dengan baik.
3. Penggunaan fitur socket.join(room) pada Socket.IO memastikan pesan yang dikiirim dan diterima pada aplikasi *chatting* hanya dapat dilihat oleh pengguna aplikasi di room yang sama.
4. Algoritma Rijndael dapat diimplementasikan pada aplikasi *chatting* berbasis HTML5 WebSocket yang telah dibangun. Semua proses enkripsi dan dekripsi dengan algoritma Rijndael dilakukan di sisi client. Hal ini membuat distribusi data pengguna dan pesan instan pada aplikasi tersebut lebih terjaga keamanannya.
5. Data *nickname* dan nama *room* yang disimpan pada server sebelumnya telah mengalami proses enkripsi dengan algoritma Rijndael. Data *password room* yang tersimpan pada server sebelumnya telah mengalami proses hashing menggunakan algoritma SHA-3. Hal ini membuat keamanan data yang tersimpan di dalam server lebih terjaga keamanannya.

6. Dari analisis yang telah dilakukan, meskipun paket data yang keluar ataupun masuk tanpa menggunakan protokol SSL tetap tersamarkan dan sulit dimengerti, penggunaan protokol keamanan SSL (Secure Socket Layer) akan memberi keamanan berlapis pada aplikasi yang telah dibangun.

5.2. Saran

Aplikasi *chatting* saat ini merupakan salah satu media komunikasi antar manusia agar tetap terhubung satu dengan yang lain. Sebagai saran untuk pengembangan sistem selanjutnya dan penelitian lain yang berkaitan dengan topik ini, penulis menyarankan agar:

1. Melakukan penambahan fitur *attachment* pada aplikasi *chatting* untuk memperluas kegunaan dan fungsionalitas sistem.
2. Menerapkan teknologi kriptografi Rijndael pada tipe data yang berbeda. Tipe data yang dimaksud dapat berupa audio, video ataupun citra. Implementasi teknologi kriptografi Rijndael pada tipe data yang berbeda selanjutnya juga dapat diaplikasikan pada fitur *attachment*.
3. Melakukan pengembangan lebih lanjut pada bagian penyebaran kunci. Pengembangan dalam penyebaran kunci dapat dilakukan dengan menggunakan algoritma pertukaran kunci seperti algoritma Diffie-Hellman.
4. Melakukan pengembangan lebih lanjut dengan menambah fitur *personal chat* pada aplikasi *chatting.* Pengembangan terhadap fitur ini diharapkan dapat memungkinkan pengguna mengirimkan pesan (berkomunikasi) secara personal kepada pengguna lain dalam *room* yang sama.
5. Melakukan perbaikan dan pengembangan antarmuka aplikasi *chatting* dengan mempertimbangkan prinsip-prinsip utama desain antarmuka.

DAFTAR PUSTAKA

Arius, D. (2008). Pengantar Ilmu KRIPTOGRAFI, Teori, Analisis dan Implementasi. Andi Offset, Yogyakarta.

Bibeault, B., & Katz, Y. (2010). jQuery in Action (2nd ed.). Manning Publications Co. Diakses pada tanggal 16 Mei 2014 dari http://www.csgnet.org/extra/livros/jQuery.%5BBear_Bibeault,_Yehuda_Katz%5D_jQuery_in_Action,_Sec(BookFi.org).pdf

Daemen, J., & Rijmen, V. (2003). AES proposal: Rijndael. Diakses pada tanggal 26 Juli 2013 dari http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

Gelens, J., Bourget, A., & Anderson, J. (2014). gevent-socketio Documentation. (Release 0.3.1). Diakses pada tanggal 16 Mei 2014 dari https://media.readthedocs.org/pdf/gevent-socketio/latest/gevent-socketio.pdf

Gilbert, H., & Minier, M. (2000). A collisions attack on the 7-rounds Rijndael. France : Centre National d'Etudes des Télécommunications. Diakses pada tanggal 24 Februari 2014 dari http://perso.citi.insa-lyon.fr/mminier/papers/GilbertMinier_AES00.pdf

Kalemi, E., & Tola, K. (2013). Updating web content in real time using Node. js. Diakses pada tanggal 19 Februari 2014 dari http://dspace.epoka.edu.al/mobile/bitstream/handle/1/844/paper_12.pdf?sequence=1

Kumar, M. V. (2013). CRYPTOGRAPHY--A SOLUTION FOR INFORMATION SECURITY THREATS. *Golden Research Thoughts*, 3(1). Diakses pada tanggal 12 Desember 2013 dari http://www.aygrt.isrj.net/UploadedData/2592.pdf

Lundar, J., Grønli, T. M., & Ghinea, G. (2013). Performance Evaluation of a Modern Web Architecture. *International Journal of Information Technology and Web Engineering (IJITWE)*, *8*(1), 36-50.

Mardanov, Azat. (2014). Express.js Guide - The Comprehensive Book on Express.js. Diakses pada tanggal 16 Mei 2014 dari http://samples.leanpub.com/express-sample.pdf

Sanders, B. (2010). Smashing Html5. John Wiley & Sons. Diakses pada tanggal 16 Desember 2013 dari blog.sijinhe.com/wp-content/uploads/2011/10/di-0483.pdf

Scheneier, B. (1996). Applied Cryptography Second Edition: protocols, algorithms, and source code in C. John Wiley and Sons. Diakses pada tanggal 26 Februari 2014 dari http://www.cse.iitk.ac.in/users/anuag/crypto.pdf

Simpson, K. (2012). JavaScript and HTML5 Now. O'Reilly Media, Inc.. Diakses pada tanggal 23 Juli 2013 dari http://dev.bowdenweb.com/a/lib/javascript-and-html5-now/javascript-and-html5-now.pdf

Sudrajat, J., Siallagan, M. P., & Irawan, B. (2005). Implementasi Kriptografi Untuk Keamanan Data Dengan Menggunakan Metode Advanced Encryption Standard (AES) 128. Bandung : JBPTUNIKOMPP. Diakses pada tanggal 11 Desember 2013 dari http://elib.unikom.ac.id/files/disk1/39/jbptunikompp-gdl-s1-2005-jajasudraj-1922-jurnal-i-l.doc

Wang, V., Salim, F., & Moskovits, P. (2013). The Definitive Guide to HTML5 WebSocket. Apress. Diakses pada tanggal 24 Juli 2014 dari http://it-ebooks.info/go.php?id=2026-1395905654-f114ccf36d0bdde0cbe89d7c0bf4e440