IMPLEMENTASI APLIKASI VIDEO CONFERENCE MENGGUNAKAN ALGORITMA BLOWFISH BERBASIS JAVA MEDIA FRAMEWORK

Agung Hardono[1], Maman Abdurohman[2], Fazmah Arif Yulianto[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Komunikasi merupakan aspek penting yang tidak bisa dipisahkan dari kehidupan manusia, mulai dari komunikasi yang biasa berupa percakapan sampai komunikasi yang menggunakan teknologi canggih yang menggunakan mediamedia tertentu seperti video conference. Perkembangan teknologi komunikasi juga sejalan dengan perkembangan teknologi keamanan data. Keamanan data merupakan salah satu aspek penting dalam penyelenggaraan komunikasi, terutama jika data yang dikomunikasikan merupakan data-data yang bersifat rahasia .Oleh karena itu diperlukan metode untuk mengamankan data pada aplikasi video conference agar pihak yang tidak berhak tidak dapat mengakses data yang sifatnya rahasia., salah satu metodenya adalah dengan menggunakan enkripsi.

Pada tugas akhir ini akan dilakukan pembuatan aplikasi video conference dengan menggunakan bahasa pemrograman Java dan Java Media Framework (JMF) dengan menerapkan algoritma Blowfish sebagai metode pengamanan data multimedia yang dipertukarkan dalam aplikasi video conference. Dari hasil penelitian tugas akhir diperoleh bahwa penggunaan algoritma Blowfish tidak memberikan pengaruh yang mengganggu terhadap kualitas audio dan video dari aplikasi video conference atau dengan kata lain penggunaan algoritma Blowfish masih layak digunakan dalam aplikasi video conference dengan menggunakan Java dan Java Media Framework.

Kata Kunci : -

Abstract

Communications represent important aspect that can’t be dissociated from human life, start from ordinary communications in the form of conversation until communications using sophisticated technology using certain medias such as video conference. Technological growth of communications also in line with technological growth of data security. Data security represent one of important aspect in communications management, especially if communicated data represent in secret datas . Therefore we needed the method which used as a peacemaker media in data communications at application of video conference in order to the party which have no business to access data represent in data secret., one of method by using encryption.

At this final project will be done by making of application of video conference by using java programming language and JMF(Java Media Framework) by applying Blowfish algorithm as method of security of data multimedia which exchanged in application of audio of video conference. Result of final project obtained that use of algorithm Blowfish do not give influence bothering to quality of audio and video from application of video conference or equally use of algorithm Blowfish still be competent used in application of video conference by using Java And Java Media Framework.

Keywords : -

1. Pendahuluan

1.1 Latar Belakang

Dewasa ini komunikasi data pada jaringan Internet maupun intranet telah mencapai kemajuan yang sangat pesat, ditandai oleh pemakaiannya yang lebih beragam dan teknologi yang digunakan sudah sangat jauh berbeda. Hingga kini sudah begitu banyak variasi data yang disebarluaskan melalui Internet maupun intranet. Yang dulunya hanya dilewati paket-paket data biasa, kini sesuai dengan kebutuhannya trafik Internet sudah dilewati paket-paket multimedia seperti suara dan video. Aplikasi yang memungkinkan pertukaran data multimedia salah satunya adalah aplikasi *video conference*, di mana komunikasi data berupa video dan audio dapat dilakukan diantara dua orang atau lebih. Komunikasi data yang terjadi pada aplikasi *video conference* dapat bersifat rahasia maupun tidak. Oleh karena itu diperlukan suatu cara atau metode yang digunakan sebagai media pengaman dalam komunikasi data pada aplikasi *video conference* agar pihak yang tidak berhak tidak dapat mengakses data yang sifatnya rahasia.

Metode yang digunakan salah satunya adalah dengan menggunakan proses enkripsi data multimedia yang saling dipertukarkan dalam aplikasi *video conference*. Dengan menggunakan proses enkripsi data maka data yang sifatnya rahasia dapat terlindungi dengan aman dari pihak-pihak yang tidak berhak.

Pada tugas akhir ini akan dilakukan pembuatan aplikasi *video conference* dengan menggunakan bahasa pemrograman *Java* dan *Java Media Framework* (JMF) dengan menerapkan algoritma Blowfish sebagai metode pengamanan data multimedia yang dipertukarkan dalam aplikasi *video conference*.

1.2 Perumusan Masalah

Beberapa permasalahan dalam tugas akhir ini dapat didefinisikan dalam berbagai hal berikut :

1. Bagaimana mengimplementasikan pembuatan aplikasi *video conference* dengan menggunakan *Java* dan *Java Media Framework*
2. Bagaimana mengimplementasikan enkripsi dan dekripsi pada data video dan audio atau *payload* video H.263 dan *payload* audio G.723 dengan algoritma Blowfish
3. Bagaimana menganalisis pengaruh penambahan enkripsi dan dekripsi algoritma Blowfish terhadap kualitas audio dan video dengan melakukan pengujian berdasarkan metode MOS (*Mean Opinion Score*)

1.3 Tujuan

Tujuan yang hendak dicapai dalam tugas akhir ini adalah :

1. Mengimplementasikan pembuatan aplikasi *video conference* dengan menggunakan *Java* dan *Java Media Framework*
2. Mengimplementasikan enkripsi dan dekripsi pada data video dan audio atau *payload* video H.263 dan *payload* audio G.723 dengan algoritma Blowfish

3. Menganalisis pengaruh penambahan enkripsi dan dekripsi algoritma Blowfish terhadap kualitas audio dan video dengan melakukan pengujian berdasarkan metode MOS (*Mean Opinion Score*)

1.4 Batasan Masalah

Dalam implementasi tugas akhir ini akan dibatasi oleh beberapa hal, sebagai berikut :

1. Menggunakan bahasa pemrograman *Java* dan *Java Media Framework*
2. Menggunakan *webcam* sebagai media input video dan *microphone* sebagai media input audio
3. Tidak membahas tentang proses *encoding* dan *decoding*
4. Pembuatan aplikasi *video conference* secara garis besar hanya berbasis pada JMF
5. Hanya menggunakan *codec* video H.263 dan *codec* audio G.723
6. Tidak membahas algoritma RSA yang digunakan dalam proses authentifikasi antara client dan server
7. Aplikasi *video conference* hanya dapat melakukan hubungan antara dua user untuk setiap komunikasi

1.5 Metode Penyelesaian Masalah

Metode penelitian yang digunakan untuk memecahkan permasalahan dalam Tugas Akhir ini terdiri dari 5 tahap, yaitu:

1. Tahap Studi Literatur
   Pada tahap ini akan dilakukan pendalaman pemahaman tentang konsep dan teori dari TCP/IP, UDP, RTP, RTCP, *Java Media Framework*, dan algoritma enkripsi blowfish.
2. Tahap Analisis dan Perancangan Perangkat Lunak
   Melakukan perancangan sistem dan perangkat lunak yang akan diimplementasikan. Perancangan sistem dan perangkat lunak akan dimodelkan dengan *UML(Unified Modelling Language)*
3. Tahap Implementasi
   Melakukan implementasi sistem dan perangkat lunak *video conference* yang dibuat dengan bahasa pemrograman *Java* dan *Java Media Framework* berdasarkan analisis dan perancangan yang telah dibuat
4. Tahap Pengujian dan Analisis Hasil Pengujian
   Dari implemetasi yang dilakukan, akan dilakukan skenario pengujian untuk membuktikan bahwa proses enkripsi dekripsi dengan algoritma Blowfish berhasil dilakukan, mendapatkan besarnya proses yang dibutuhkan untuk melakukan enkripsi dekripsi dengan algoritma Blowfish dan hubungan pengaruh penambahan enkripsi dan dekripsi algoritma Blowfish terhadap kualitas audio dan video dengan melakukan pengujian berdasarkan metode MOS (*Mean Opinion Score*)
5. Tahap Pembuatan Laporan
   Laporan yang akan dihasilkan berupa buku Tugas Akhir. Pembuatan laporan dengan mengikuti kaidah penulisan yang berlaku yang berisi mengenai semua dasar teori dan juga hasil dari penelitian tugas akhir

1.6 Sistematika Penulisan

BAB I Pendahuluan
Bab ini menguraikan tugas akhir ini secara umum, meliputi latar belakang masalah, perumusan masalah, tujuan, batasan masalah, dan metode penyelesaian masalah serta sistematika penulisan

BAB II Landasan Teori
Bab ini membahas uraian teori yang berhubungan dengan video conference, Java Media Framework, algoritma blowfish

BAB III Analisis dan Perancangan Sistem
Bab ini berisi analisis kebutuhan sistem, hasil analisis dituangkan dalam pemodelan berorentiasi objek menggunakan notasi UML. Dari tahap analisis kemudian dilanjutkan pada tahap implementasi

BAB IV Implementasi dan Analisis Hasil percobaan
Bab ini membahas mengenai pengujian hasil implementasi yang telah dilakukan. Pengujian dilakukan untuk menilai apakah sistem yang kita buat sudah sesuai dengan hasil analisis dan perancangan sistem. Setelah tahap pengujian dilanjutkan dengan tahap analisis hasil pengujian

BAB V Kesimpulan dan Saran
Berisi kesimpulan dari penulisan Tugas Akhir ini dan saran-saran yang diperlukan untuk pengembangan lebih lanjut

5. Kesimpulan dan Saran

5.1 Kesimpulan

Kesimpulan yang dapat diambil pada tugas akhir ini antara lain:

1. Proses enkripsi dekripsi berhasil dilakukan dengan pembuktian bahwa data tidak dapat diakses oleh orang yang tidak berhak, untuk data audio dapat terdengar tapi tidak dapat dimengerti sedangkan untuk data video tidak dapat dimainkan.
2. Waktu yang diperlukan untuk proses enkripsi audio berada pada range 9319.1033284 nanoseceond, dekripsi audio 8748.96823 nanosecond, enkripsi video 58044.182112 nanosecond dan dekripsi video 69992.661874 nanosecond dengan spesifikasi perangkat keras seperti pada lampiran. Meskipun terdapat tambahan waktu akibat proses enkripsi dekripsi tetapi tidak memberikan efek/pengaruh yang menganggu terhadap kualitas audio dan video
3. Algoritma Blowfish masih layak digunakan dalam aplikasi real time video conference dengan menggunakan JMF karena meskipun dengan penambahan mekanisme keamanan data tapi tanpa mengorbankan kualitas terlalu besar terbukti dengan penilaian responden yang masih berkisar diantara range cukup baik dan baik.

5.2 Saran

Saran-saran untuk pengembangan tahap selanjutnya antara lain:

1. Mencoba untuk menerapkan aplikasi video conference dengan lebih banyak user (multi user)
2. Mencoba untuk menerapkan aplikasi video conference yang mampu dijalankan pada lingkungan dengan bandwith terbatas, misal pada koneksi dial up 64 kbps
3. Mencoba untuk menerapkan protokol pensinyalan standar seperti SIP atau H.323 agar aplikasi yang berjalan dapat kompatible atau cocok dengan peralatan dan software dari vendor seperti Cisco
4. Mencoba untuk menerapkan video conference dengan berbagai macam format video dan audio yang berbeda.
5. Mencoba untuk menerapkan algoritma block cipher maupun algoritma stream cipher yang lebih baik tingkat keamanannya dan bit rate enkripsinya dibandingkan algoritma Blowfish

Daftar Pustaka

[1] Booch, Grady., Rumbaugh, Jim., and Jacobson, Ivar., 1999, *The Unified Modeling Language User Guide*, Addison-Wesley .

[2] Faisal, Kazi Nasim, What is Ethereal?, URL: http://web2.uwindsor.ca/courses/cs/aggarwal/cs60592/EtherealReport.doc

[3] Fowler, Martin., 2005, *UML Distilled Edisi 3, Panduan Singkat Bahas Pemodelan Objek Standar*, Yogyakarta, Andi

[4] Haneef, Anwar M., 2002, *JMF-Multimedia Networking for The Rest of Us*, URL: http://www.-unix.ecs.umass.edu/~ahaneef

[5] Harold, Elliotte., 2005, *Java Network Programming 3rd Edition*, O'REILLY

[6] Java Media Framework (JMF). URL: http://java.sun.com/products/java-media/jmf/

[7] Java Media Framework API guide 2.0, November 19, 1999

[8] Knudsen, Jonathan., May 1998, *Java Cryptography*, O'REILLY

[9] Kurniawan, Budi., *Program Multimedia With JMF, Part 1*, URL: http://www.javaworld.com/jw-04-2001/jw-0406-jmf1.html, 6 April 2001

[10] Kurniawan, Budi., *Program Multimedia With JMF, Part 2*, URL: http://www.javaworld.com/jw-06-2001/jw-0504-jmf1.html, 4 Mei 2001

[11] Kurniawan, Yusuf., 2004, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika

[12] Prasetyo, Didik., 2004, *Tip dan Trik Pemrograman Java*, Jakarta, Elex Media Komputindo

[13] Schneier, Bruce., *Speed Comparision of Block Cipher on a Pentium*, URL: http://www.schneier.com/blowfish-speed.html

[14] Schulzrinne, H., S. Casner, R. Frederick, and V.Jacobson, 2003, "RTP: a transport protocol for real time application", Request For Comments 3550, Internet Engineering Task Force.

[15] Sidik, Betha., *MySQL Untuk Pengguna, Administrator, dan Pengembang Aplikasi Web*, Bandung, Informatika

[16] Susanto, Budi., 2003, *Pemrograman Client/Server dengan Java 2*, Jakarta, Elex Media Komputindo

[17] Wesley, Addison., *RTP audio and video for the Internet*

[18] Wiley, John., 2004, *Cryptography For Dummies*