PENGAMANAN DATA VIDEO SURVEILLANCE SECARA REAL-TIME MENGGUNAKAN ENKRIPSI SELEKTIF DENGAN ALGORITMA SERPENT

Irvan Yogatama, Surya Michrandi Nasution,ST.,M.T.[2],Anton Siswo Raharjo Ansori,S.T.,M.T.[3]

[1,2,3]Sistem Komputer, Fakultas Teknik Elektro – Univesitas Telkom Jln. Telekomunikasi No.1 Terusan Buah Batu Bandung 40257 Indonesia yogatamavan@gmail.com[1], michrandi@telkomuniversity.ac.id[2], raharjo@telkomuniversity.ac.id[3]

ABSTRAK

Berkembangnya layanan video *surveillance* membuat aspek keamanan datanya menjadi penting. Data yang penting tersebut hanya bisa diakses oleh orang-orang tertentu. Kriptografi merupakan sebuah metode pengamanan data yang awalnya dipusatkan pada data berbentuk tulisan. Algoritma yang dipakai juga mempengaruhi tingkat kualitas dan keamanan data tersebut. Oleh karena itu perlu adanya metode enkripsi untuk menyembunyikan informasi data tersebut dari pihak ketiga. Pada penelitian Tugas Akhir ini dibangun suatu sistem dengan enkripsi selektif menggunakan algoritma serpent. Dasar dari enkripsi selektif adalah untuk mengurangi volume komputasi selama proses enkripsi/dekripsi. Enkripsi selektif membutuhkan kunci yang kuat oleh karenanya, algoritma serpent di implementasikan sebagai faktor keamanan dari sistem ini.Pada penelitian Tugas Akhir ini dibangun sistem pengamanan data video *surveillance* yang merupakan sebuah solusi untuk mengamankan data video dan memberikan hak akses secara aman kepada orang yang benar-benar memiliki hak tersebut. Pada perancangan ini akan dibangun sebuah sistem yang dapat mengamankan data video dari kamera webcam secara real-time dengan cara enkripsi data videonya, serta memberi hak akses kepada orang yang benar-benar mempunyai hak streaming terhadap video tersebut yang bisa melakukan dekripsi data tersebut ke dalam file aslinya.Dalam sistem ini di peroleh pengujian yang menunjukan bahwa enkripsi selektif menggunakan algoritma serpent dengan *generate key* tertentu dapat mengenkripsi dan mendekripsi video surveillance streaming secara real-time karena menghasilkan delay kurang dari satu second.

Kata Kunci: kriptografi, enkripsi selektif, serpent, video streaming, video surveillance, real-time

ABSTRACT

In development of video surveillance service makes data safety aspect important. The important data only can be accessed by certain people. Criptograph is a safety data method which is concentrated on written data. The algorithm which is used also influences quality and the data safety. That's why it needs an encription method to hide the data information from the third person.

In this final project will be made a system which using selective encryption with serpent algorithm. The basis of selective encryption is to reduce the volume of computation for encryption / decryption process. A strong key is required by the selective encryption, therefore the serpent algorithm implemented as a security factor of this system.

In this final project will be made also a video surveillance data safety which is a solution to secure video data and give access safely to people who have rights. In this design will be made a system which can secure video data from camera in rieal time by encripting the video data, also give access to people who have rights to the streaming video who can decrypt the data to the original file.

The result of this system shows that selective encryption with serpent algorithm with particular generated key could encrypt and decrypt surveillance video streaming with real-time because the delay lesser than one second

Keyword: *criptography*, *selective encryption* , *serpent*, *video streaming*, video *surveillance*, *real-time*

I. PENDAHULUAN

1.1. Latar Belakang

Era globaisasi saat ini membuat penggunaan layanan video *surveillance* di beberapa ruangan semakin dibutuhkan guna meningkatkan keamanan dan privasi bagi penggunanya. Adanya video *real-time streaming* berfungsi untuk merekam suatu kegiatan, tentu penting bagi beberapa instansi seperti perbankan, perkantoran, pertahanan negara, dan lain-lain. Namun pertukaran informasi tersebut tentu saja dapat menimbulkan resiko jika informasi yang dipertukarkan dapat diakses oleh pihak-pihak yang tidak bertanggung jawab. Maka dari itu kerahasiaan data pun semakin ditingkatkan, salah satunya dengan menerapkan metode kriptografi

Kriptografi merupakan metode pangamanan dengan mengubah data asli menjadi acak atau tidak dapat dibaca oleh pembaca jika tidak memiliki kuncinya.[1], adapun berbagai macam teknik kriptografi salah satunya dalah dengan enkripsi selektif

Algoritma enkripsi selektif atau sering disebut soft encryption adalah sebuah teknik enkripsi dengan cara mengenkripsi hanya sebagian porsinya saja, sedangkan sisa nya dibiarkan saja sebagaimana semestinya. Video akan di enkripsi dengan cara memproses sebagian nilai byte nya saja [3].. Namun, algoritma yang kuat akan lebih membantu dalam optimalisasi keamanan pada enkripsi selektif tersebut, salah satu algoritma yang memiliki kekuatan di keamanan nya salah satunya adalah algoritma serpent.

Dalam tugas akhir ini algoritma serpent dipilih untuk mengisi peran pertahanan keamanan dari enkripsi selektif. Algoritma serpent merupakan sebuah block cipher dengan kekuatan keamanan yang tinggi, terbukti bahwa serpent menjadi finalis dalam kontes Advanced Encryption Standard (AES). Serpent bekerja dengan substitution-permutation network (SP-network), yang dalam pengoperasiannya menggunakan 4 word yang berukuran 32 bit. Algoritma serpent memiliki ukuran blok sebesar 128 bit [4]. Dengan mengkombinasikan enkripsi selektif dengan algoritma serpent, maka sistem dapat di optimasi dengan kecepatan dari enkripsi selektif dan keamanan yang kuat dari algoritma serpent.

1.2. Rumusan Masalah

Bagaimana cara menerapkan proses enkripsi dan dekripsi selektif untuk real-time video surveillance streaming menggunakan algoritma kriptografi serpent?

1. Memodifikasi algoritma serpent dengan metode enkripsi selektif.
2. Menerapkan proses enkripsi dan dekripsi selektif untuk real-time video surveillance streaming.
3. Menganalisis hasil pengujian yang telah dilakukan dengan pengukuran parameter waktu proses, avalanche effect, delay, jitter, data rate, frame rate, dan bandwidth.

1.3. **Tujuan**

Penelitian Tugas Akhir mengenai enkripsi dan dekripsi pada real-time video streaming ini memiliki beberapa tujuan, diantaranya:

1. Menerapkan dan memodifikasi algoritma serpent dengan metode enkripsi selektif.
2. Menerapkan proses enkripsi dan dekripsi untuk real-time surveillance video streaming menggunakan algoritma kriptografi selektif dengan serpent.
3. Menganalisis hasil pengujian yang telah dilakukan dengan pengukuran parameter waktu proses, avalanche effect, delay, jitter, bitrate, frame rate, dan bandwidth.

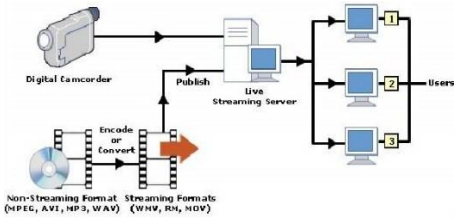
1.4. Batasan Masalah

1. Surveillance video direkam menggunakan webcam.
2. Menggunakan kunci simetris.
3. Client tidak terlibat dalam pendistribusian kunci
4. Software yang digunakan berbasis java.
5. Tidak membahas pembobolan jaringan
6. Sistem tidak menyimpan file dalam bentuk ber ekstensi
7. Admin tidak memerlukan proses autentikasi

II. TEORI DASAR

2.1 Video Streaming

Streaming adalah sebuah proses untuk memainkan audio atau video secara.langsung atau dengan pre-recorder dari sebuah server. Streaming audio atau video akan langsung dijalankan ketika adanya request dari seorang user. Dengan cara demikian, maka proses running aplikasi yang di unduh berupa waktu yang lama dapat dihindarkan tanpa harus melakukan proses penyimpanan file terlebih dahulu. Ketika saebuah file di stream, akan terjadi pembentukan sebuah buffer pada computer client, dan file video atau audio tersebut akan mulai di unduh ke dalam bufferyang telah terbentuk pada client.



Gambar 2.1 Arsitektur Video Streaming

2.2 Enkripsi Selektif

Enkripsi selektif adalah metode untuk mengenkripsi hanya sebagian dari video, dan beberapa bagian lain nya diabaikan. Tujuan dari enkripsi selektif adalah untuk mempercepat proses enkripsi dan mengurangi delay. Enkripsi selektif bisa dilakukan dengan mengenkripsi video hanya pada frame tertentu, atau sebagian dari nilai bit, sementara beberapa bagian lain hanya diabaikan.

2.3 Algoritma Serpent

Serpent adalah algoritma block cipher yang menggunakan SP-network dengan 4 word yang berukuran 32 bit dalam operasinya. Sehingga dengan demikian serpent memiliki ukuran panjang 128 bit. Persamaan dibawah ini menjelaskan bagaimana operasi cipher:

$$\square = IP(P)$$
$$\square_{+1} = \square\square)$$
$$C = FP(\square_{32}) \quad \ldots[2]$$

Fungsi R dapat digambarkan secara lebih detail sebagai berikut :

$$\square X) = L(\square(X \otimes \square)), \quad i = 0 \ldots 30 \quad \ldots[2]$$

Berikut adalah pseudo-code untuk algoritma serpent:

Table 2.4 Pseudo-code Serpent [4]

```
B := IP(P)

For i:=0 to 30 do

   B := L(□(B ^ □) )

B := □(B ^ □) ^ □32

C := FP(B)
```

Ada dua macam mode dalam algoritma serpent, yaitu mode standar dan mode bitslice. Mode standar serpent adalah mode yang implementasinya berdasarkan pseudo-code di atas, sedangkan mode bitslice implementasi setiap fase nya tidak dipisahkan ke dalam fungsi-fungsi tersendiri, namun digabungkan dalam satu fungsi.

2.4.1 Enkripsi Mode Standar

Berikut adalah proses dari enkripsi mode standar dari algoritma serpent:

1. **Permutasi Awal**

   Dalam permutasi awal, bit input akan diacak sesuai dengan nilai matriks dari algoritma serpent:

.32 round SP-network

- Operasi Key Mixing

  Pada operasi ini, block input di-XOR-kan dengan kunci round.

  $\square := \square \otimes \square$

- S-Box

Serpent memiliki 8 buah S-Box yang setiap S-Box ini memiliki 16 entri yang tiap entrinya mempunyai ukuran 4 bit. S-Box ke-I digunakan pada round ke (i mod 8). Sehingga setiap S-Box digunakan 4 kali dalam enkripsi satu block.

- Transformasi Linear

Transformasi linear menggunakan matriks dari serpent. Output bit ke- i adalah hasil dari XOR bit input ke posisi masing-masing elemen dari matriks. Berikut adalah matriks transformasi linear:

Permutasi Akhir

Permutasi akhir menggunakan cara yang sama dengan permutasi awal namun dengan matriks yang berbeda. Berikut adalah matriks permutasi akhir:

2.4.2 Enkripsi Mode Bitslice

Dalam mode bitslice, pelaksanaan setiap tahap tidak dipisahkan menjadi fungsi individu, tetapi digabungkan menjadi satu fungsi. cipher terdiri hanya dari 32 putaran. Berikut adalah enkripsi dari proses algoritma Serpent Bitslice Mode:

Operasi Key Mixing

Di setiap putarannya, subkey 128-bit ⬚dikirim secara eksklusif saat data berada di antara data ⬚

S-Box

Kombinasi 128-bit input dan kunci dianggap sebagai 4 word dari 32-bit. The S-box, yang diimplementasikan sebagai logical operation diterapkan untuk 4 word, dan hasilnya adalah output 4 word . CPU ini digunakan untuk mengeksekusi 32 salinan dari S-box secara bersamaan, dengan menggunakan ⬚⬚⊕ ⬚.

Permutasi Akhir

32 bit dalam setiap word output linear dikombinasikan, dengan:

⬚, ⬚, ⬚, ⬚ := ⬚ ⬚⊕ K_1)
⬚ := ⬚ <<< 13
⬚ := ⬚ <<< 3
⬚ := ⬚ ⊕ ⬚ ⊕ ⬚
⬚ := ⬚ ⊕ ⬚ ⊕ (⬚ << 3)
⬚ := ⬚ <<< 1
⬚ := ⬚ <<< 7
⬚ := ⬚ ⊕ ⬚ ⊕
⬚ := ⬚ ⊕ ⬚ ⊕ (⬚ << 7)
⬚ := ⬚ <<< 5
⬚ := ⬚ <<< 22
⬚ := ⬚, ⬚, ⬚, ⬚ …[2]

2.4.3 Dekripsi Standar dan Bitslice Mode

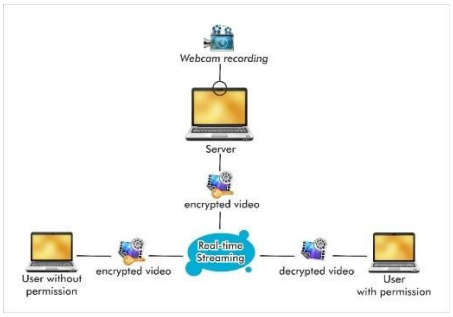
Proses dekripsi dari kedua mode ini adalah sama dengan cara enkripsi nya, hanya saja terdapat beberapa perbedaan seperti:

1. Substitusi S-Box menggunakan S-box inverse dengan urutan terbalik (dimulai dari S-Box inverse ke tujuh sampai nol).
2. Transformasi linear menggunakan transformasi linear inverse.
3. Permutasi awal menggunakan permutasi akhir, dan permutasi akhir menggunakan permutasi awal.
4. Kunci setiap round nya di gunakan secara terbalik.

III. IMPLEMENTASI DAN PENGUJIAN

3.1 Gambaran Umum Sistem

Pada gambar sistem dibangun sebagai ilustrasi dari *surveillance* kamera yang di gantikan oleh wabcam.



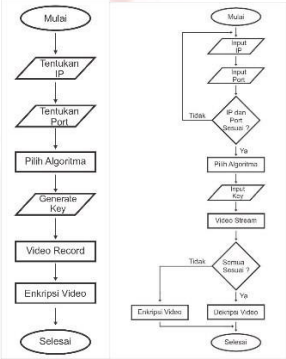
Gambar 2.1 Flow Aplikasi

Perancangan sistem dibuat menggunakan dua user, yaitu sebagai server dan sebagai client. Server berperan untuk merekam gambar melalui webcam, yang nantinya hasil rekaman tersebutlah yang akan diproses untuk di enkripsi dan di transmisikan kepada client. Proses enkripsi dan dekripsi dilakukan secara selektif, dengan menggunakan algoritma serpent.

3.2 Diagram Alir Sistem Aplikasi

Diagram Alir dari sistem aplikasi real-time video streaming secara keseluruhan dari sisi server dan juga client.

Diagram Alir Server dan Client



Gambar 3.2.1 Alur Server dan Client

Perancangan Enkripsi Selektif

Enkripsi dilakukan dengan cara memilih atau menyeleksi sebagian nilai bit yang akan diproses. Sebagian nilainya dibiarkan saja tanpa terenkripsi agar mengurangi beban proses sehingga bisa memangkas sebagian waktu enkripsi.

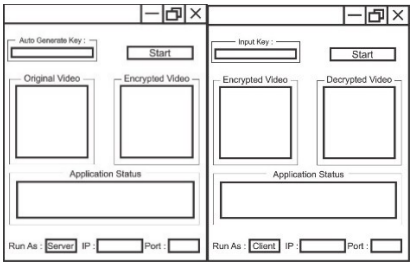
3.4 Sistem Enkripsi dan Dekripsi Algoritma Serpent

Data yang di rekam melalui kamera merupakan Data Raw. Data Raw adalah data mentah yang didapatkan dari berbagai sumber data dan informasi, yang belum diolah maupun di encode dalam bentuk ekstensi data. Data tersebut kemudian di convert menjadi byte dikombninasikan dengan tahap enkripsi serpent (permutasi awal, 32round SP-network, dan permutasi akhir).

3.5 Perancangan Antarmuka

Rancangan antarmuka yang akan dibangun dalam sistem ini adalah seperti berikut :

Tampilan perancangan server dan client:



3.6 Pengujian

Melakukan serangkaian uji coba untuk mengukur parameter performansi algoritma dengan kondisi scenario kondisi siang tak banyak gerak, siang banyak gerak, malam tak banyak gerak dan malam banyak gerak. Parameter yang diuji yaitu :

1. Delay
Delay adalah waktu yang dibutuhkan oleh sebuah paket data terhitung dari saat pengiriman oleh transmitter sampai saat diterima oleh receiver.
Delay = panjang paket ÷ bandwith
2. *Avalanche effect*
Avalanche Effect adalah perubahan satu bit pada plaintext atau key yang menyebabkan perubahan yang signifikan terhadap ciphertext.

$$Avalanche\ Effect = \frac{\sum \text{bit berubah}}{\sum \text{bit total}} * 100\%$$

3. *Datarate*
Datarate adalah variasi delay, yaitu perbedaan selang waktu kedatangan antar paket di terminal tujuan. Nilai jitter yang direkomendasikan oleh ITU – T Y.1541 adalah dibawah 50 ms.
4. Bandwidth
Bandwidth adalah suatu ukuran dari banyaknya informasi yang dapat mengalir dari server ke client dalam suatu waktu tertentu.

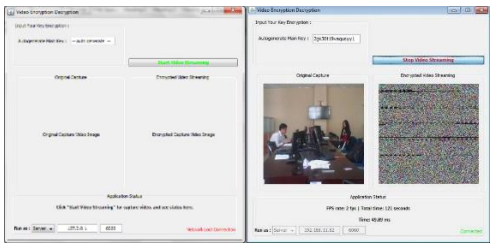
$$bandwidth = \frac{\sum bits}{s}$$

5. Troughput
Troughput adalah bandwidth yang sebenarnya (aktual) yang diukur dengan satuan waktu tertentu dan pada kondisi jaringan tertentu yang digunakan untuk melakukan transfer file dengan ukuran tertentu.
6. Jitter
Jitter merupakan variasi dari suatu delay antara blok-blok yang berurutan atau selisih antara delay yang pertama dengan delay selanjutnya.
Jitter = { Delay akhir – Delay sebelumnya }

IV. IMPLEMENTASI DAN PENGUJIAN SISTEM

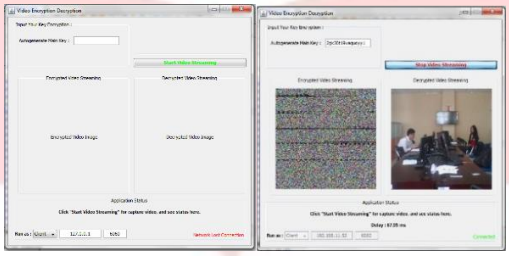
4.1 Implementasi Antarmuka Server

Implementasi antarmuka /user interface merupakan tampilan dari aplikasi video yang akan menampilkan video asli dan video terenkripsi pada sisi server, serta video terenkripsi dan terdekripsi pada sisi server. Berikut adalah tampilan antar muka yang telah di implementasikan :



4.2 Tampilan client

Tampilan Client setelah memulai untuk streaming. Pada tampilan client menampilkan video dalam dua kondisi, yaitu kondisi terenkripsi dan video yang telah terdekripsi.



4.5 Pengujian Performansi

Pada sistem ini dilakukan pengujian performa yang bertujuan untuk menganalisa performansi sitem. Pengujian performansi tersebut diantaranya yaitu delay, data rate, frame rate, bandwidth, jitter, dan avalanche effect.

No.	Hasil Pengujian
1.	Delay : 772.42 ms Data Rate : 393,733.16 bps Bandwidth : 0.39 Mbps Jitter : 0.77 ms
2.	Delay : 194.54 ms Data Rate : 1,563,346 bps Bandwidth : 1.56 Mbps Jitter : 0.19 ms
3.	Delay : 68.74 ms Data Rate : 4,424,638.5 bps Bandwidth : 4.42 Mbps Jitter : 0.07 ms
4.	Delay : 104.29 ms Data Rate : 2,916,242.5 bps Bandwidth : 2.92 Mbps Jitter : 0.1 ms
5.	Delay : 277.43 ms Data Rate : 1,096,216.25 bps Bandwidth : 1.1 Mbps Jitter : 0.28 ms

Percobaan	Plaintext	Ciphertext	Bit Berubah	AE (%)
1.	1DE28EFF77 17E70701A1 B17144024D 0038FC8407	AC95E8727F C38FF04098 818098AEAF B7AC19C0F	56	53.75
2.	0694B50FD2 EE70B694FF 93361557D6 3AD809EAD	1DE28EFF77 17E70701A1 B17144024D 0038FC8407	67	44.53
3.	7287FF2DBC 7F3D5D5F2 D579A24987 09FFF158464	E5AFC99B7 11BD18FB1 A88E056237 059D09AB1	70	54.68

V. PENUTUP

Kesimpulan yang dapat diambil dari penelitian Tugas Akhir ini adalah :

1. Berdasarkan hasil pengujian waktu delay, terbukti bahwa enkripsi selektif dengan algoritma serpent cukup memuaskan. Walaupun proses nya berat, namun rata-rata delay yang diperoleh tidak lebih dari 1 detik.
2. Berdasarkan hasil pengujian yang telah dilakukan cahaya mempengaruhi frame rate. Semakin terang cahaya yang direkam, semakin banyak pula frame rate yang dihasilkan.
3. Berdasar hasil pengujian system dinyatakan berhasil real-time berdasar data yang diperoleh dengan rata-rata dari delay adalah 68 ms, datarate adalah 4,235,673 bps, bandwidth adalah 4,737 Mbps, jitter adalah 0,158245274 ms.

VI. DAFTAR PUSTAKA

[1] Akhyar, Fikaril.”**Rabbit Algorithm for Video on Demand**”, Apwimob , Telkom University, 2015

[2] Andreas, Ross. Biham, Eli. Knudsen, Lars**. Serpent: A Proposal for the Advanced Encryption Standard**. Cardis, 1998

[3] Munir, Rinaldi, “**Pengembangan Algoritma Enkripsi Selektif Citra Digital dalam Ranah Spasial dengan Mode CBC-like Berbasiskan Chaos**”, Sekolah Teknik Elektro dan Informatika ITB, Bandung, 2012.

[4] Pratama, Arief. “**Enkripsi Selektif Video MPEG dengan Algoritma Serpent**”. Jurusan Teknik Informatika Sekolah Teknik Elektro dan Informatika ITB, Bandung.

[5] Ramdan, Alwi Alfiansyah dan R. Munir. “**Selective Encryption Algorithm Implementation for Video Call on Skype Client**”. Informatics Engineering, Bandung Institute of Technology.

[6] Ramdan, Alwi Alfiansyah dan R. Munir. “**Selective Encryption Algorithm Implementation for Video Call on Skype Client**”. Informatics Engineering, Bandung Institute of Technology.

[7] S.B.D.Julian, “**Analisa Sistem Video on Demand (VoD) pada Asymmetric Digital Suncriber Line (ADSL)**”.

[8] Selany, Siska.” **Sosemanuk Algorithm for Encryption and Decryption Video on Demand (VoD)**”, Apwimob, Telkom University, 2015.

[9] Supriatna Asep, Siallagan Manahan P. dan Irawan Budhi, “**Analisis dan Implementasi Keamanan Metode Enkripsi Algoritma Serpent**”, Jurusan Teknik Informatika, Universitas Komputer Indonesia.

[10] T. I. P. S. Endro Ariyanto, “**Analisa Implementasi Algoritma Stream Cipher Sosemanuk dan Dicing dalam Proses Enkripsi Data**,” 2008.