ISSN. 1412-0100 VOL 17, NO 1, APRIL 2016

Implementasi Digital Rights Management pada Media-Streaming sebagai Pelindung Data Digital

Surya Michrandi Nasution[1], R, Rumani M[2], Agus Virgono[3]
Gedung Barung Ruang TE1.02.08, Universitas Telkom, Jl. Telekomunikasi No.1, Bandung 40257
[1,2,3,4] Program Studi Sistem Komputer, Fakultas Teknik Elektro – Universitas Telkom, Bandung
[1]michrandi@telkomuniversity.ac.id, [2]rumani@telkomuniversity.ac.id,
[3]avirgono@telkomuniversity.ac.id

Abstrak

Pembajakan pada konten digital saat ini sudah menyebabkan kerugian pada beberapa perusahaan recording company atau production house. Digital Rights Management (DRM) merupakan salah satu upaya untuk menghentikan pembajakan. DRM dapat berperan untuk memberikan pilihan untuk mengkontrol dalam penggunaan hak cipta dari sebuah konten digital. Pada system ini, DRM diintegrasikan dengan algoritma kriptografi untuk mengamankan pesan khususnya dalam pengiriman dan penerimaan data streaming. Sistem serial key dan authentication key dirancang untuk membangun system kerja DRM. Kedua kunci ini memberikan kemampuan kepada sebuah server untuk mengenali jenis client yang menggunakan fasilitas yang diberikan oleh server. Fasilitas yang diberikan kepada setiap tipe client berbeda sesuai dengan tipe client itu sendiri. Sistem DRM dapat dibentuk dengan menerapkan system yang dihasilkan dalam penelitian ini yang membutuhkan dua kunci tambahan sebagai media verifikasi client. Pemilahan jenis pengguna dan data berdasarkan kunci serial dan kunci autentikasi dapat berjalan 100% berdasarkan pengujian fungsional. Jumlah frame maksimum yang dapat diacak dalam sistem ini adalah 2070 frame. Hasil kemiripan dari hasil pengembalian data acak didapatkan dengan menyebarkan kuisioner dan mendapatkan nilai 2,59 dari skala 4 yang berarti hasil pengembalian data dapat dikatakan mirip.

Kata kunci— *Digital Rights Management, DRM, Video Streaming, Kriptografi, Keamanan Sistem*

Abstract

Piracy in digital content cause loss for several recording company or profuction house. Digital Rights Management (DRM) is one of the ways to stop piracy. DRM can act as a choice for controlling copyright usage in digital content. In this system, DRM integrated with cryptography algorithm for securing message, especially for sending and receiveing data stream. Serial key and authentication key is designed for building DRM system. Both of the keys provide the server to recognize the type of client who used the system. Every type of client will received different feature of the system. DRM system can be formed by applying two additional keys for client's verification. The selection of clients and data based on serial key and authentication key successfully works based on functional testing. Maximum frame that can be encrypted in this system is 2070 frames. The result of similarity testing is taken from questionnaire and got 2,59 from 4 which means the result of data's decryption is similar.

Keywords— *Digital Rights Management, DRM, Video Streaming, Cryptography, Secure System*

1. PENDAHULUAN

Digital Rights Management (DRM) merupakan sebuah teknologi yang digunakan untuk menetapkan kendali akses dari sebuah *software*, konten audio, konten video, ataupun data *digital* lainnya [1,2]. DRM juga merupakan teknologi akses kontrol yang digunakan oleh penerbit dan pemegang hak cipta terhadap keterbatasan isi dari media *digital* [3]. Penggunaan DRM sempat menjadi kontroversi, misalnya pada kasus *software* yang dengan sengaja dibagikan secara gratis. Penggunaan DRM dapat

dikombinasikan dengan enkripsi dengan menggunakan algoritma kriptografi dan watermarking, hal ini ditujukan untuk menghindari serangan dari pembajakan [4].

Penggunaan DRM pada konten visual dan audio adalah cara yang tepat untuk melindungi hak cipta bagi pencipta konten tersebut. Dalam DRM ditentukan siapa pemegang sebuah hak cipta dari sebuah data, dan siapa saja yang berhak untuk mengakses data tersebut [5,9]. Hal ini disebabkan karena tingginya tingkat pembajakan oleh oknum-oknum tertentu yang bertujuan mendapatkan konten tersebut dengan percuma. Dengan tingginya tingkat pembajakan membuat tingkat penjualan media fisik seperti *tape cassete*, CD audio, VCD, ataupun DVD, menjadi surut. Pada DRM juga diatur identifikasi pengguna yang dibentuk agar sesuai dengan aturan yang berlaku pada sistem [6].

Contoh penggunaan sistem DRM dapat dilihat pada sistem operasi Windows. Pada beberapa sistem operasi Windows terdapat beberapa jenis sistem operasi yang disesuaikan dengan *serial number*. Pada contoh kasus lain, pada aplikasi iTunes, pemutar musik dapat dijalankan dengan seketika tetapi untuk memanfaatkan fitur musik *online* untuk mendengarkan musik terbaru pengguna harus melakukan *log in* ke dalam aplikasinya dengan menggunakan Apple ID yang dimiliki pengguna [7]. Pada contoh kasus lain, beberapa pemutar video atau musik *streaming*, penggunaan DRM dapat menentukan kelayakan pengguna agar dapat dibatasi hak aksesnya.

Pada umumnya sistem keamanan pada media konten yang bersifat *streaming* hanya ditentukan dengan proses *log in* saja. Hal ini dapat saja dibobol oleh para *hacker* dikarenakan *session* pada saat *log in* dapat dicuri dengan menerapkan teknik penyerangan seperti XSS yang melakukan penyerangan dengan melakukan suntikan *script* yang berasal dari sisi pengguna. Sistem pengamanan tambahan dibutuhkan untuk mengatasi hal-hal tersebut. Selain kunci tambahan, sistem media *streaming* dapat pula ditambahkan fitur enkripsi dengan menggunakan algoritma kriptografi [4]. Jika hanya memanfaatkan kriptografi saja, maka hal tersebut tidaklah cukup. Untuk melakukan perlindungan terhadap data digital, enkripsi hanya melindungi data tersebut saat data sedang dikirim, bukanlah saat data tersebut dapat disalin, saat disalin kita dapat mengambil data yang sudah didekripsi [8].

Pada sistem ini, dibuat sebuah media *streaming* yang memiliki fitur pengamanan dengan cara memberikan kunci tambahan dan melakukan penerapan enkripsi pada video. Kunci tambahan tersebut merupakan kunci serial dan kunci autentikasi. Kunci-kunci inilah yang membuat client memiliki hak yang pantas untuk melihat atau memiliki video tersebut.

Pada sistem yang dibuat memiliki dua jenis pengguna, member dan premium. Kedua jenis pengguna ini menentukan jenis video yang diputarkan oleh server. Dalam implementasinya, pengamanan pada video dilakukan pengamanan dan pemisahan antara data video dan data audio, yang kemudian data video dilakukan enkripsi dan kemudian diputarkan ke pengguna. Pengguna dengan tipe member hanya mendapatkan sample data video dan diterapkan tanpa pengamanan sistem. Pengamanan sistem ini diterapkan untuk tipe pengguna.

2. METODE PENELITIAN

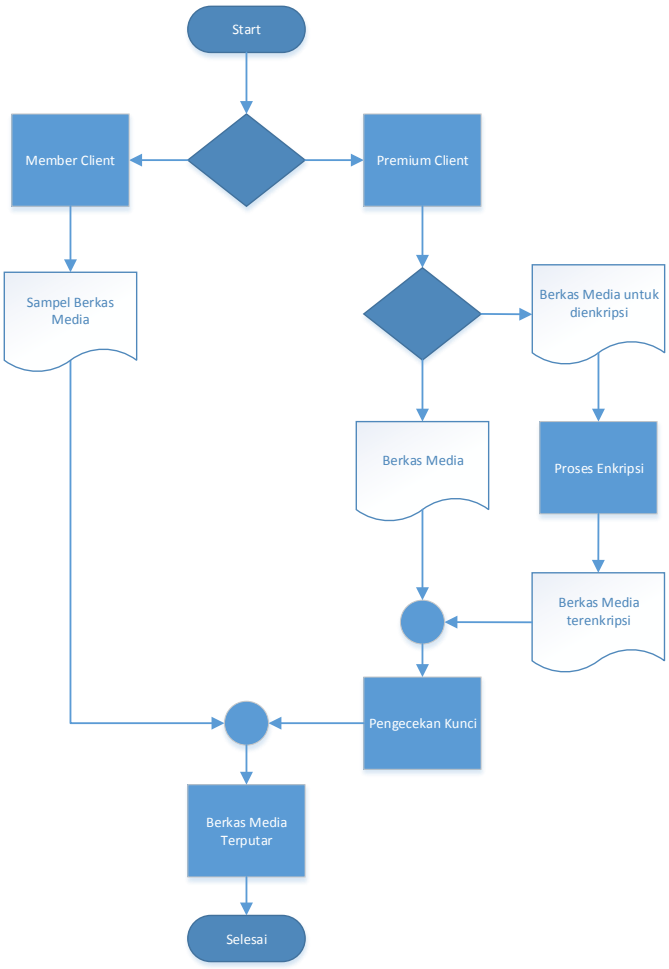
2.1. Perancangan Sistem

Untuk mendukung pembuatan sistem media *streaming* dengan penerapan *Digital Rights Management*, maka system diimplementasi ke dalam sebuah *website*. Berikut beberapa pertimbangan implementasi sistem dengan menggunakan website:

1. *Website* dapat mendukung pemutaran media streaming dengan berbagai macam format video.
2. Pembuatan dan penggunaan kunci dapat diatur lebih sederhana dibandingkan dengan menggunakan media *player* yang dapat memutarkan data melalui jaringan.
3. *Website* dapat diakses oleh beberapa pengguna secara serentak tanpa harus melakukan instalasi program khusus.
4. *Website* dapat diintegrasikan dengan *database* yang dapat membantu melakukan penggolongan pengguna ke beberapa kelas tertentu.

Sistem enkripsi pada konten video dilakukan dengan bantuan aplikasi MatLab. Pemilihan bahasa pemrograman ini mengacu pada sifat MatLab yang beroperasi berdasarkan matriks yang sesuai dengan sistem video yang memiliki layer RGB dimana setiap *frame* yang ada dapat dibaca sebagai matriks.

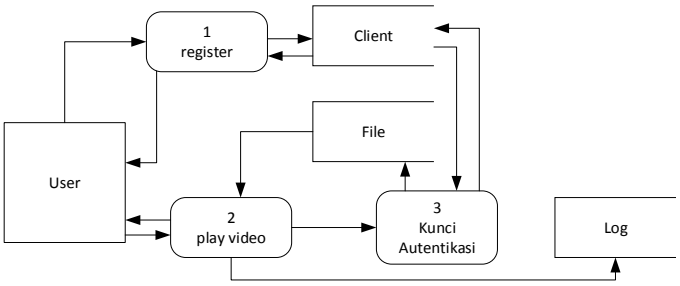
Pada Gambar 1, dapat dilihat proses keseluruhan dari sistem media *streaming* dengan DRM. Server telah menentukan dua jenis pengguna yaitu member dan premium yang nantinya dibedakan perilaku penggunanya. Pada pengguna member hanya diputarkan *sample* video saja, sedangkan pada pengguna premium akan diterapkan kunci tambahan untuk mendapatkan pemutaran video utuh. Apabila pengguna telah mendaftarkan diri ke dalam *website*, maka sistem akan membangkitkan kunci serial yang akan diberikan kepada pengguna. Kunci serial merupakan hasil enkripsi dengan menggunakan fungsi hash MD5. Serial key hanya dibuat sekali saja setelah pengguna premium mendaftarkan dirinya. Kunci autentikasi juga dibuat dengan menggunakan enkripsi dengan menggunakan fungsi hash MD5. Sistem kunci autentikasi berbeda dengan kunci serial yang hanya dibuat satu kali. Kunci autentikasi selalu dibuat ketika seorang pengguna melakukan permintaan data kepada server. Sistem enkripsi video terjadi apabila pengguna premium memasukkan kunci autentikasi yang salah, maka pengguna tersebut diputarkan video yang telah terenkripsi.



Gambar 1 Flowchart Sistem

2.2. Perancangan Website Streaming dengan DRM

Pada perancangannya, server melakukan penyimpanan data *sample* video dan data video utuh. Kemungkinan penyerangan pada website diminimalisir dengan kunci autentikasi yang diintegrasikan dengan *mail* server yang secara otomatis melakukan pembangkitan kunci setiap pengguna melakukan permintaan data ke server. Apabila kunci autentikasi yang dimasukkan tidak sesuai, maka data yang terputar adalah data yang telah diacak.



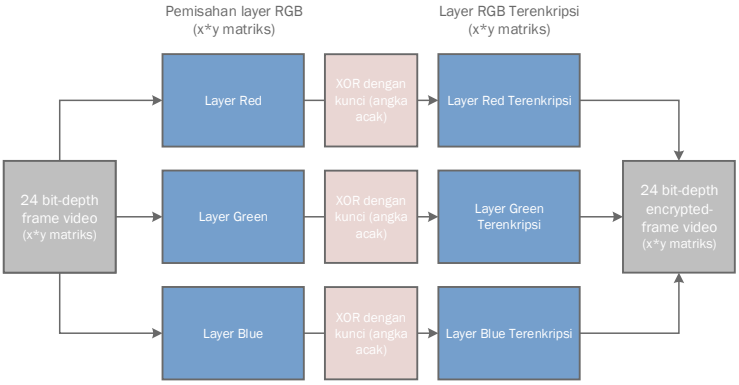
Gambar 2 Data Flow Sistem DRM

2.3. Perancangan Enkripsi Data

Sistem enkripsi data yang ada pada sistem merupakan sebuah pendukung untuk membuat sistem media *streaming* ini menjadi semakin aman. Untuk mendapatkan hasil enkripsi, sebuah data (*message*) harus dioperasikan dengan kunci (K) tertentu dan dilakukan dengan metode tertentu pula seperti yang dapat dilihat pada persamaan (1). Dalam penelitian ini enkripsi dilakukan dengan melakukan dekomposisi video, yang kemudian dibaca bit-bit nya dan dilakukan proses logika XOR.

$$E = K(m) \tag{1}$$

Sebuah video terdiri dari *frame* citra dan audio. Dalam setiap *frame* citra terdapat layer RGB yang menyimpan *bit-bit* dalam bentuk matriks. Layer-layer ini yang dibaca *bit* nya dan dilakukan enkripsi. Pada Gambar 3, dijabarkan proses enkripsi video yang telah diambil data citranya yang berbentuk kumpulan *frame*, proses enkripsi dilakukan untuk setiap *frame* video yang juga terdiri dari tiga *layer* warna, yaitu *red*, *green*, dan *blue*.



Gambar 3 Sistem Enkripsi Data Video

Untuk setiap *layer* yang telah berbentuk matriks, setiap posisi dioperasikan seperti pada persamaan (2). Terdapat tiga buah data acak ($C_{(x,y)}$) yang akan merepresentasikan matriks warna *red*, *green*, dan *blue* yang merupakan hasil dekomposisi dari *frame* citra. Matriks yang dioperasikan memiliki kedalaman warna 8 bit untuk satu *layer* pada tiap *frame*. Untuk lebih detail proses enkripsi pada tiap *frame* citra untuk setiap *layer* yang ada dapat dilihat pada Gambar 4.

$$C(x,y) = M(x,y) \oplus Km \tag{2}$$

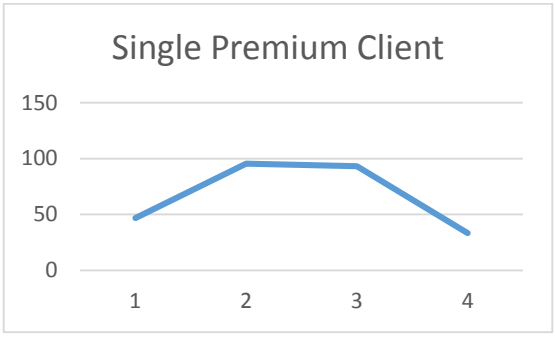
$$\begin{Bmatrix} C_{(0,0)} & C_{(0,1)} & \dots & C_{(0,n)} \\ C_{(1,0)} & C_{(1,1)} & \dots & C_{(1,n)} \\ C_{(2,0)} & C_{(2,1)} & \dots & C_{(2,n)} \\ C_{(m,0)} & C_{(m,1)} & \dots & C_{(m,n)} \end{Bmatrix} \oplus \begin{Bmatrix} K_{(0,0)} & K_{(0,1)} & \dots & K_{(0,n)} \\ K_{(1,0)} & K_{(1,1)} & \dots & K_{(1,n)} \\ K_{(2,0)} & K_{(2,1)} & \dots & K_{(2,n)} \\ K_{(m,0)} & K_{(m,1)} & \dots & K_{(m,n)} \end{Bmatrix} = \begin{Bmatrix} E_{(0,0)} & E_{(0,0)} & \dots & E_{(0,n)} \\ E_{(1,0)} & E_{(1,1)} & \dots & E_{(1,n)} \\ E_{(2,0)} & E_{(2,1)} & \dots & E_{(2,n)} \\ E_{(m,0)} & E_{(m,1)} & \dots & E_{(m,n)} \end{Bmatrix}$$

Gambar 4 Matriks Pengolahan Frame Citra

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Penggunaan Bandwidth

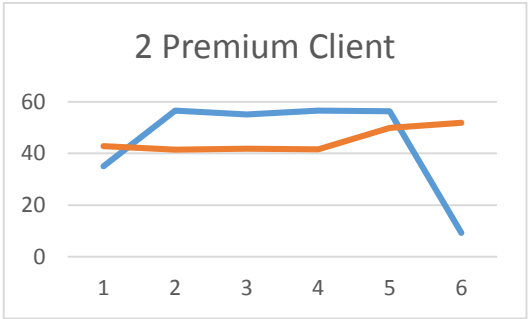
Penggunaan *bandwidth* dihitung dengan skenario satu dan dua pengguna yang melakukan akses ke dalam server secara bersamaan. Pengujian ini dilakukan dalam *isolated network*. Uji coba yang dilakukan dengan melakukan *stream* data sebesar 268 MB. Pengujian pertama dilakukan disaat kunci autentikasi yang dimasukkan dengan benar. Dapat dilihat dari tabel 1, rata-rata penggunaan *bandwidth* untuk satu pengguna premium adalah 67,15 Mbps, dan tabel 2 melihatkan rata-rata penggunaan *bandwidth* untuk dua pengguna adalah 44,84 Mbps.



Gambar 5 Penggunaan *Bandwidth* 1 Pengguna Premium

Tabel 1 Penggunaan *Bandwidth* 1 Pengguna Premium

Time(s)	*Bandwidth* (Mbps)
1	46,7
2	95,5
3	93,2
4	33,2
Rata-rata	67,15

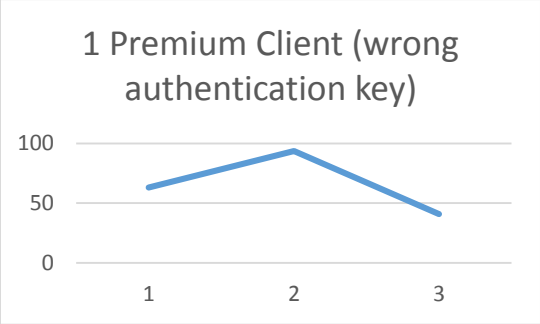


Gambar 6 Penggunaan *Bandwidth* 2 Pengguna Premium

Tabel 2 Penggunaan *Bandwidth* 2 Pengguna Premium

Time(s)	*Bandwidth* (Mbps) Pengguna 1	*Bandwidth* (Mbps) Pengguna 2
1	35	42,8
2	56,5	41,4
3	55,1	41,8
4	56,6	41,6
5	56,3	49,9
6	9,2	51,9
Rata-rata	44,78	44,9

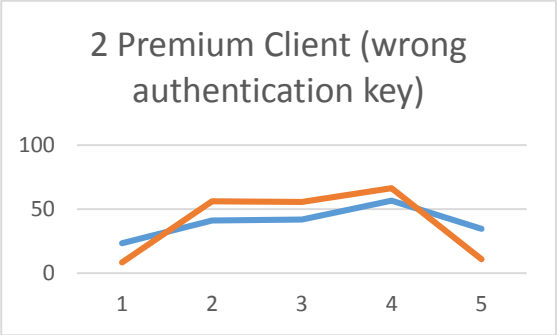
Uji coba berikutnya dilakukan untuk mengetahui penggunaan *bandwidth* disaat seorang pengguna premium memasukkan kunci autentikasi yang salah. Pada implementasinya data yang diputarkan ke pengguna berbeda dengan sebelumnya. Data yang diputarkan tidak memiliki suara di dalamnya. Data yang dikirimkan ke pengguna adalah sebesar 197 MB. Dapat dilihat dari tabel 3, rata-rata penggunaan *bandwidth* untuk satu pengguna premium adalah 65,9 Mbps, dan tabel 4 melihatkan rata-rata penggunaan *bandwidth* untuk dua pengguna adalah 39,59 Mbps.



Gambar 7 Penggunaan *Bandwidth* 1 Pengguna Premium (Kunci Salah)

Tabel 3 Penggunaan *Bandwidth* 1 pengguna premium (kunci salah)

Time(s)	*Bandwidth* (Mbps)
1	63,1
2	93,8
3	40,8
Rata-rata	65,9



Gambar 8 Penggunaan *Bandwidth* 2 Pengguna Premium (Kunci Salah)

Tabel 4 Penggunaan *Bandwidth* 2 Pengguna Premium

Time(s)	*Bandwidth* (Mbps) Pengguna 1	*Bandwidth* (Mbps) Pengguna 2
1	23,5	8,4
2	41,3	56,1
3	41,9	55,8
4	56,7	66,5
5	34,8	10,9
Rata-rata	39,64	39,54

3.2 Pengujian Kunci Serial dan Autentikasi

Kunci serial adalah kunci yang didapatkan pada saat pengguna melakukan pendaftaran dirinya ke dalam website. Tabel 5 merupakan hasil rekaman catatan yang berasal dari sistem. Pada tabel tersebut ditunjukkan seorang pengguna premium melakukan proses *log in* pada *website*. Pada proses pertama pengguna memasukkan kunci serial dan kunci autentikasi dengan benar sehingga sistem mengenalinya sebagai pengguna premium. Pada proses login berikutnya, pengguna memasukkan kunci serial yang tidak sesuai sehingga mengakibatkan pengguna dianggap sebagai pengguna member. Pada tabel 6, dilakukan pengujian fungsional untuk kunci serial, hasil yang didapatkan adalah kunci serial berfungsi 100% sesuai yang diharapkan.

Tabel 5 Pengujian Kunci untuk Pengguna Premium

```
User Activity

2009-08-02 01:23:16 premium succesfull login as member with serial key serial_key_asal (wrong
serial key)
2009-08-02 01:22:47 premium succesfull login as member with serial key (wrong serial key)
2009-08-02 01:21:05 premium succesfull login as premium with serial key
ef1a87cd1ab005b3329016ea5c31bc57 and authen key 41f2dc482441c620bf2b82b60b49e862
```

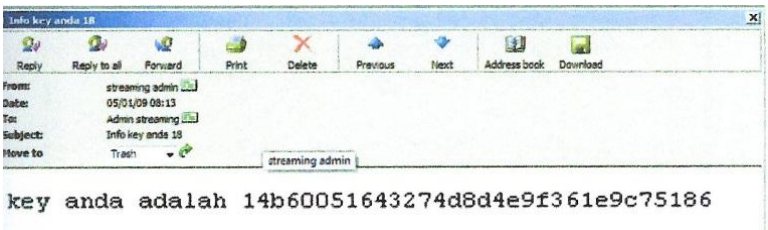
Tabel 6 Pengujian Fungsional Kunci Serial

Data Masukan			Keluaran Yang Diharapkan	Hasil Pengamatan	Kesimpulan
Username	Password	Kunci Serial			
✓	✓	-	Member	Member	Diterima
✓	✓	✓	Member	Member	Diterima
✓	✓	×	Member	Member	Diterima
✓	✓	-	Member	Member	Diterima
✓	✓	×	Member	Member	Diterima
✓	✓	✓	Premium	Premium	Diterima

Sistem pengamanan media *streaming* dengan DRM diintegrasikan dengan *mail server* yang bertugas untuk mengirimkan kunci autentikasi pada saat pengguna melakukan permintaan pemutaran data. Kunci ini selalu disimpan pada *database* dan selalu berubah setiap pengguna melakukan permintaan data. Penggunaan kunci autentikasi sengaja dibuat secara *private*, hanya diketahui oleh server dan pengguna saja. Kunci autentikasi ini berfungsi untuk menentukan data mana yang disajikan ke pengguna. Kunci autentikasi merupakan enkripsi angka dari 0 (nol) hingga 1000000 dengan menggunakan fungsi *hash* MD5. Gambar 9 merupakan perolehan kunci autentikasi yang didapatkan dari *mail* server yang dikirimkan ke pengguna. Kunci autentikasi dapat memilah data mana yang ditampilkan ke pengguna, hal ini sesuai dengan hasil pengujian fungsional pada tabel 7.

Tabel 7 Pengujian Fungsional Kunci Autentikasi

Data Masukan	Keluaran Yang Diharapkan	Hasil Pengamatan	Kesimpulan
Kunci Autentikasi			
Benar	Data video lengkap diputar	Data video lengkap terputar	Diterima
Salah	Data video acak diputar	Data video acak terputar	Diterima



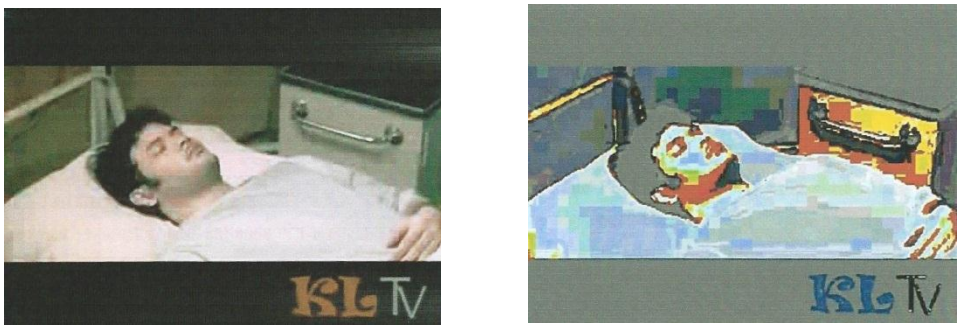
Gambar 9 Kunci Autentikasi yang Diterima Pengguna

3.3 Pengujian Enkripsi Data

Enkripsi dengan proses logika XOR dilakukan pada sebuah *frame* yang berukuran 320x240 piksel dan memiliki kedalaman warna sebesar 24 bit dimana masing-masing layer memiliki kedalaman warna 8 bit. Pada proses enkripsi ini dipilih kunci bernilai 100 yang akan dikonversi menjadi *binary*, dan akan dilakukan enkripsi terhadap layer-layer dalam *frame* tersebut. Pada hasil pengujiannya, dalam salah satu *layer* terdapat 310 piksel yang tidak berubah, hal ini dikarenakan bit input yang ada pada layer tersebut bernilai 0 (nol), sehingga menghasilkan output yang sama dengan kunci, yaitu 100. Dapat dilihat dari tabel 7, rata-rata persentase piksel yang bernilai 100 pada ketiga layer adalah 0,004001%.

Tabel 8 Perbandingan Perubahana Piksel antar *Layer*

Layer	Piksel Bernilai 100	Total Piksel	Persentase
1	310	76800	0,004036%
2	328	76800	0,00427%
3	284	76800	0,00370%
Rata - Rata			0,004001%



Gambar 10 Hasil Frame Data Video Sebelum (Kiri) dan Sesudah (Kanan) Enkripsi

Terlihat dari Gambar 10, hasil enkripsi pada data video cukup tinggi. Dalam sistem ini perhitungan *Avalanche Effect* (AE) bukanlah sesuatu yang penting, dikarenakan dalam sistem ini yang dibutuhkan adalah enkripsi pada data video. Pada tabel 8 ditunjukkan beberapa jenis video yang dapat diacak. Berdasarkan hasil uji coba pada beberapa video, aplikasi pendukung membutuhkan *memory* yang tinggi untuk melakukan enkripsi video dengan jumlah *frame* yang tinggi. Hal ini disebabkan server harus melakukan komputasi untuk 230.400 piksel untuk tiap *frame*.

Tabel 9 Jenis-jenis Video yang Dapat Dienkripsi

Video	*Frame per Second* (fps)	Durasi (s)	Total *Frame*	Hasil
1	10	149	1490	OK
2	30	260	7800	*Out of Memory*
3	25	278	6950	*Unable to locate decompressor to decompress video stream*
4	30	69	2070	OK
5	30	138	4140	*Out of Memory*

Pada uji coba untuk proses dekripsi, terdapat kesalahan dalam beberapa *frame* video. Hal ini terjadi karena kompresi yang digunakan dalam pembuatan video dengan aplikasi tidak dapat mengembalikan data secara sempurna setelah *bit-bit* setiap *layer* dikembalikan ke bentuk asalnya. Untuk melakukan pengujian dari kualitas *frame* dekripsi, dilakukan penyebaran kuisioner kepada 30 orang secara acak. *Frame* yang diujikan diambil secara acak dari video 1 dan diambil sebanyak 30 *frame*. Pada tabel di bawah, diperlihatkan kualitas *frame* video hasil dekripsi. Untuk menilai kualitas diberikan

pilihan 1 sampai dengan 4 yang merepresentasikan nilai sangat tidak mirip hingga sangat mirip. Hasil rata-rata menunjukkan bahwa hasil dekripsi bernilai 2,59 yang artinya frame-frame tersebut masih dapat dikatakan mirip.

Gambar 11 Hasil Perbandingan Frame Asli, Frame Enkripsi, dan Frame Dekripsi

Tabel 10 Perbandingan Kualitas *Frame* Asli – *Frame* Hasil Dekripsi

No Frame	Kualitas (1-4)	No *Frame*	Kualitas (1-4)	No *Frame*	Kualitas (1-4)	No *Frame*	Kualitas (1-4)	No *Frame*	Kualitas (1-4)
1	2,7	7	2,63	13	2,67	19	3,03	25	2,8
2	2,47	8	1,67	14	3,33	20	2,47	26	2,43
3	2,13	9	2,83	15	2,43	21	2,47	27	2,7
4	2,5	10	2,37	16	2,83	22	2,83	28	1,97
5	2,2	11	2,83	17	2,73	23	3,3	29	1,97
6	2,93	12	3,13	18	2	24	2,7	30	2,8
								Rata-rata	2,59

4. KESIMPULAN

Setelah melakukan implementasi dan analisa pada sistem ini, maka terdapat beberapa kesimpulan yang dapat diperoleh, yaitu :

1. Pada jaringan yang terisolasi, penggunaan *bandwidth* untuk satu pengguna premium adalah 67,15 Mbps dan untuk dua pengguna premium adalah 44,84 Mbps. Pada kasus pengguna premium dengan kasus salah kunci autentikasi, bandwidth yang dibutuhkan untuk satu pengguna adalah 65,9 Mbps, dan 39, 59 Mbps untuk dua pengguna.
2. Penggolongan jenis pengguna dan pemilahan pemutaran data berdasarkan kunci serial dan kunci autentikasi dapat berjalan dengan yang diharapkan. Berdasarkan pengujian fungsional kunci serial dan autentikasi dapat berjalan 100%.
3. Proses enkripsi dengan menggunakan aplikasi bergantung dengan perangkat keras yang digunakan, dalam sistem ini proses enkripsi dapat dilakukan untuk *frame* yang berjumlah 2070. Dibutuhkan *memory* lebih banyak untuk melakukan enkripsi dengan jumlah *frame* yang lebih banyak.
4. Hasil dekripsi dari video terenkripsi bernilai 2,59 yang berarti hasil pengembalian masih mirip atau serupa dengan video aslinya.

5. SARAN

Terdapat beberapa hal yang dapat dikembangkan dari penelitian ini, yaitu:

1. Melakukan implementasi proteksi pada serangan *SQL Injection*, memberikan tambahan kunci yang dapat memperkuat sistem DRM.
2. Implementasi data *digital* cukup satu saja, sehingga dapat menghemat penyimpanan pada server. Sistem dapat melakukan pemotongan, enkripsi, dan dekripsi secara otomatis.
3. Melakukan enkripsi data dengan menggunakan algoritma kriptografi yang lain.

DAFTAR PUSTAKA

[1] Bechtold, Stefan, 2003, *The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems*, Springer, Berlin.

[2] Yu, Yang, et al., 2011, Enterprise Digital Rights Management: Solutions against Information Theft by Insiders.

[3] Godwin, Michael, 2006, Digital Rights Management: A Guide for Librarian, American Library Association.

[4] Thanh, Ta Minh, et al., 2013, An Incomplete Cryptography based Digital Rights Management with DCFF. The Proceeding of International Conference on Soft Computing and Software Engineering. San Francisco.

[5] Iannella, Renato, 2001, Digital Rights Management (DRM) Architectures, D-Lib Magazine. Volume 7 number 6.

[6] Helberger, Natali, et al., 2004, Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations, Consumer Acceptability of DRM Solutions. Europe.

[7] Adrian, Aloysius, 2009, Digital Rights Management Terapan Serta Ancamannya, Institut Teknologi Bandung, Bandung.

[8] Coyle, Karen, 2003, The Technology of Rights: Digital Rights Management. The Library of Congress.

[9] d'Ornellas, Marcos C., 2008, Applying Digital Rights Management to Complex Content Management Systems, 11th IEEE International Conference on Computational Science and Engineering, Brazil.