IMPLEMENTASI *SECURE SOCKET LAYER* PADA *REAL-TIME VIDEO SURVEILLANCE* MENGGUNAKAN ZONEMINDER DAN APACHE WEBSERVER

Nanda Adi Pratama[1], Joko Triyono[2], Catur Iswahyudi[3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri
Institut Sains & Teknologi AKPRIND Yogyakarta
[1]prataman79@gmail.com, [2] jack@akprind.ac.id, [3]catur@akprind.ac.id

ABSTRACT

Security is a very important aspect of data exchange. Usually, the data in video surveillance is transmitted shown only for certain parties. the data must accepted to entitled user with maintained confidentiality, without known by other people who want to see. Therefore, to secure the data in video surveillance, it needs a data encryption method, which is the science of hiding information.

One method that is quite reliable for securing a real-time data transmission is SSL (Secure Socket Layer). SSL can be implemented on a webserver that has public hosting. In this study, Zoneminder video surveillance system will be implemented on the web server, then SSL will encrypt the transmitted data between the Zoneminder server and the client.

The results shows that surveillance videos protected by SSL, safe from packet sniffing actions and performance comparison results shows no significant results.

Keywords : *SSL, Zoneminder, video surveillance, real-time, data transmission*.

INTISARI

Keamanan merupakan aspek yang sangat penting bagi jalannya pertukaran data dalam *video surveillance*. Pada umumnya data *video surveillance* yang dikirim hanya ditunjukan bagi pihak-pihak tertentu saja. Suatu data harus sampai pada pihak yang berhak dengan kerahasiaan yang tetap terjaga, tanpa harus diketahui oleh pihak-pihak yang tidak berkepentingan. Oleh karena itu untuk menjaga keamanan dan kerahasiaan data *video surveillance*, perlu adanya metode enkripsi data, yang merupakan ilmu untuk menyembunyikan informasi dari pihak ketiga.

Salah satu metode yang cukup handal dalam mengamankan transmisi data secara *real-time* adalah SSL (Secure Socket Layer). SSL dapat diimplementasikan pada webserver yang memiliki *public hosting*. Pada penelitian ini, akan diimplementasikan Zoneminder *video surveillance system* pada webserver, kemudian SSL akan melakukan enkripsi pada transmisi data antara server Zoneminder dan *client*.

Hasil penelitian menunjukkan bahwa video surveillance yang terlindungi SSL, aman dari tindakan packet sniffing dan hasil perbandingan peforma tidak menunjukkan hasil yang signifikan.

Kata Kunci : SSL, Zoneminder, *video surveillance, real-time*, transmisi data.

PENDAHULUAN

Kemajuan teknologi membuat penggunaan *video surveillance* dalam kehidupan sehari-hari semakin penting guna meningkatkan keamanan dan *privacy* bagi penggunanya. Adanya *video real-time* yang berfungsi merekam suatu gambar pada suatu kegiatan tentu penting bagi beberapa instansi seperti perbankan, perkantoran, pertahanan negara, dan lain-lain.

Masalah yang terjadi dalam sistem yang telah diterapkan terletak pada 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

Kerahasiaan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Dapat diperoleh dengan memberi akses terbatas pada informasi atau dengan penyandian informasi sehingga tidak memiliki arti apapun bagi pihak yang tidak berhak tersebut. Jika kerahasiaan ini tidak terpenuhi mengakibatkan adanya penyalahgunaan wewenang oleh pihak yang tidak sah.

Pentingnya integritas dalam sebuah *video surveillance* karena apabila tidak terpenuhi dapat mengakibatkan terjadinya manipulasi maupun penghapusan terhadap data asli. Salah satu solusi untuk menghindari resiko penyerangan terhadap informasi adalah dengan melakukan tindakan enkripsi menggunakan SSL atau *Secure Socket Layer*.

SSL atau *Secure Socket Layer* adalah cara sebuah situs web membuat sambungan aman dengan browser web pengguna. Setiap kali seorang *surfer web* mengunjungi situs yang aman yang menggunakan teknologi SSL, menciptakan sebuah *link* yang terenkripsi antara sesi *browser client* dan *web server*. SSL adalah standar industri untuk komunikasi web yang aman dan digunakan untuk melindungi jutaan web setiap hari.

Dalam penelitian ini akan diimplementasikan suatu metode untuk mengamankan integritas data dari sebuah *Real-time Video Surveillance* menggunakan *Secure Socket Layer*. Namun dikarenakan Perangkat *Video Surveillance* yang digunakan adalah sebuah *IP Camera*, maka dibutuhkan sebuah *Webserver* untuk menempatkan *Zoneminder Video Surveillance System*. *Webserver* akan meneruskan akses yang sudah terlindungi *Secure Socket Layer* secara Publik dari *IP Camera* ke *Client*.

Dari permasalahan tersebut, maka muncul sebuah gagasan untuk mengimplementasikan *Secure Socket Layer* pada sebuah *Real-time Video Surveillance* yang dibantu dengan *Zoneminder* dan *Apache Webserver* sebagai topik penelitian untuk skripsi. Dengan diimplementasikannya SSL pada *Real-time video surveillance* ini diharapkan dapat melindungi integritas data *Real-time video surveillance* dari pihak-pihak yang tidak berwenang.

TINJAUAN PUSTAKA

Penelitian ini menggunakan pustaka hasil-hasil penelitian sebelumnya yang relevan, yaitu penelitian Yong-Hua (2014), Widyantara (2015), Illyan (2016), Pranata (2015) dan Wulandari (2016).

Penelitian yang dilakukan oleh Yong-Hua (2014) bertujuan untuk mendesain dan mengimplementasikan metode untuk sistem *video surveillance* berbasis *cloud* menggunakan karakteristik *cloud computing*. Seperti komputasi paralel, ruang penyimpanan yang besar dan mudah diperluas. Arsitektur sistem dan modul fungsi dibangun, dan prototipe sistem *video surveillance* berbasis *cloud* didirikan di jaringan kampus menggunakan teknologi kunci, termasuk kontrol akses tugas mesin virtual, penyimpanan data-data terdistribusi, dan metode komunikasi aktif basis data. Namun dalam penelitian ini belum ada metode untuk mengamankan integritas data dari *video surveillance* itu sendiri.

Penelitian yang dilakukan oleh Widyantara (2015) bertujuan untuk mengusulkan sebuah aplikasi VSS (*Video Surveillance System*) untuk memudahkan memonitoring setiap *IP Camera*. Aplikasi yang telah diusulkan memadukan konsep sistem informasi geografis berbasis web dengan *Google Maps API* (Web-GIS). Aplikasi VSS dibangun dengan fitur-fitur smart meliputi peta ip-camera*, live streaming event*, informasi pada *info window* dan *marker cluster*. Namun dalam penelitian ini juga belum ada metode untuk mengamankan kerahasiaan data dari sistem *video surveillance* itu sendiri.

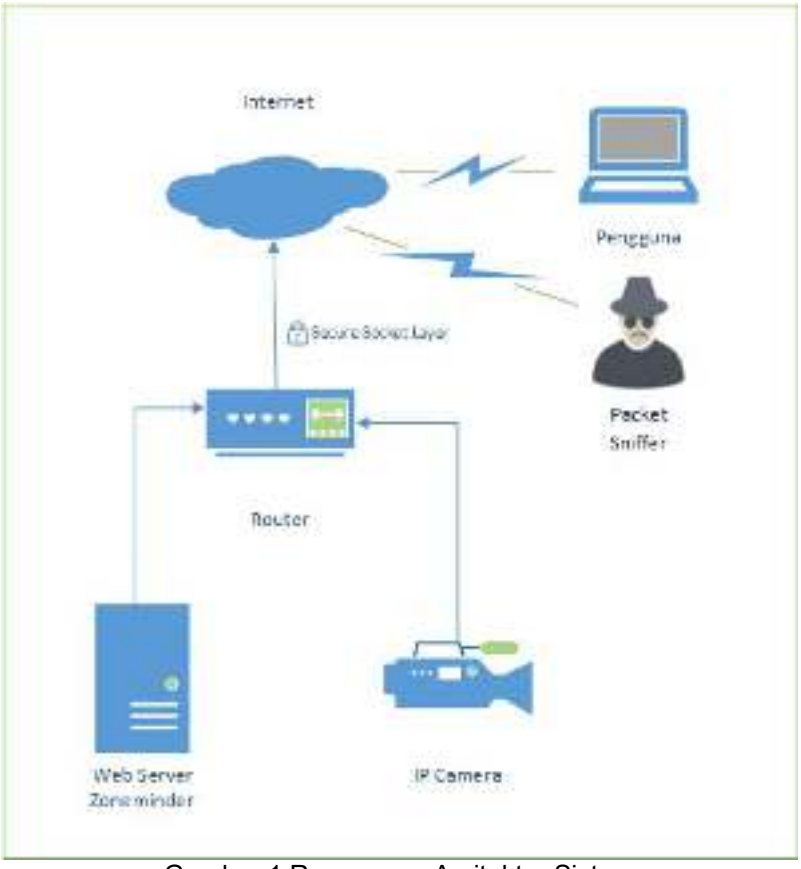
Penelitian yang dilakukan oleh Illyan (2016) bertujuan untuk merancang suatu system pengamanan data pada *video Surveillance*, dengan cara mengenkripnya menggunakan VEA (*Video Encryption Algorithm*) dan kunci tertentu, lalu memberikan hak akses secara aman kepada orang yang benar-benar berhak tersebut. Kemudian menganalisa performansi dari algoritma VEA dalam hal waktu proses enkripsi dan dekripsi, maupun delay-nya.

Penelitian yang dilakukan oleh Pranata (2015) bertujuan untuk menganalisis sejauh mana SSL dapat mengamankan data di jaringan. Ketika komputer mengirim data melalui jaringan, data dikirimkan dalam bentuk paket. Ancaman keamanan yang disajikan oleh *sniffer* adalah kemampuan mereka untuk menangkap semua paket yang masuk dan keluar melalui jaringan, yang meliputi kata sandi, nama pengguna dan masalah sensitif lainnya. Namun dalam penelitian ini informasi yang dianalisa adalah paket yang berupa informasi bersifat ASCI seperti *username* dan *password*.

Penelitian yang dilakukan oleh Wulandari (2016) bertujuan untuk menganalisis *Quality of Service* agar dapat mengukur seberapa baik jaringan dan upaya untuk menentukan karakteristik dan sifat layanan. *Quality of Service* mengacu pada kinerja Paket IP melalui satu atau lebih jaringan. Kinerja jaringan komputer dapat bervariasi karena beberapa masalah, seperti masalah *bandwidth*, *latensi* dan *jitter*, yang dapat membuat efek besar untuk banyak aplikasi.

Penelitian yang telah disebutkan di atas akan menjadi referensi dalam penimplemetasian SSL pada *Live-stream Video Surveillance* Menggunakan Zoneminder dan Apache Webserver. Perbedaan penelitian ini dengan referensi yang telah disebutkan adalah objek yang diimplementasikan yakni SSL (*Secure Socket Layer*) pada *Real-time Video Surveillance*.

Rancangan arsitektur sistem



Gambar 1 Rancangan Arsitektur Sistem

Pada Gambar 1 merupakan rancangan arsitektur sistem yang dimana Sistem akan diakses oleh pengguna secara publik menggunakan jaringan internet, akses yang dituju pengguna adalah Webserver Zoneminder. Zoneminder akan melakukan stream data ke *IP Camera* yang telah terdaftar di sistem Zoneminder dan mengirim data *stream* yang telah di enkripsi oleh SSL kembali ke Client.

PEMBAHASAN

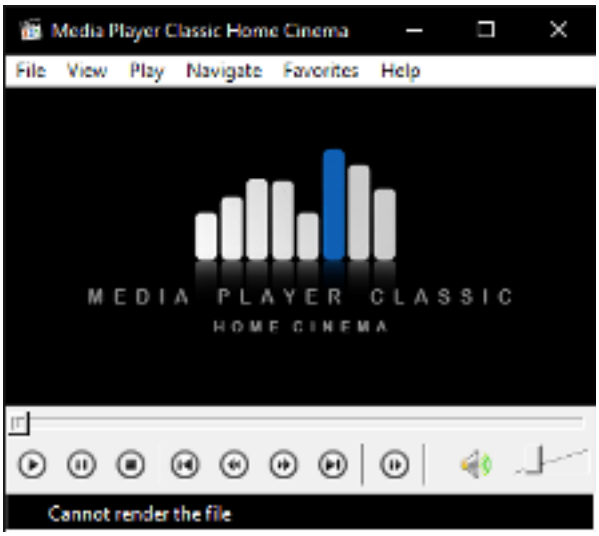
Simulasi *Real-Time Video Surveillan*ce pada Zoneminder

Simulasi *Real-time Video Surveillance* dilakukan dengan mejalankan Live Stream pada web browser Mozila Firefox. Pengguna juga dapat mengontrol pergerakan kamera dengan menggunakan fitur *Control* pada Zoneminder. Simulasi *Real-time Video Surveillance* pada Zoneminder dapat ditunjukan pada gambar 2.

Gambar 2 Simulasi *Real-Time Video Surveillan*ce pada Zoneminder

Hasil Pengujian Packet Sniffing

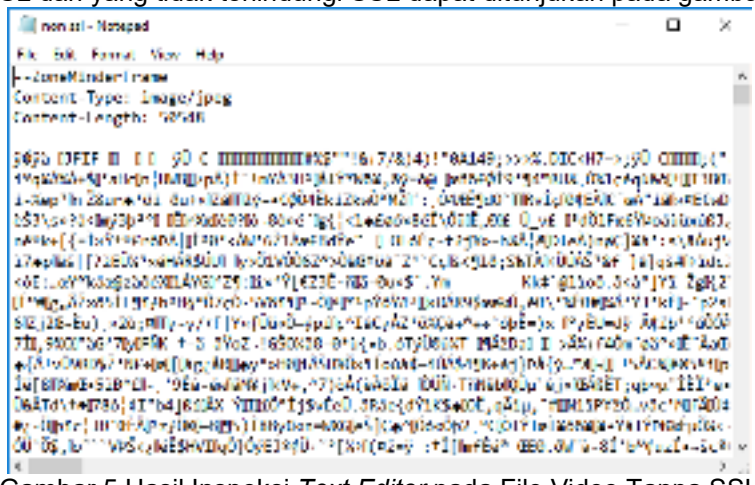
Gambar 3 Proses *Replay* Pada Packet Wireshark Tanpa SSL



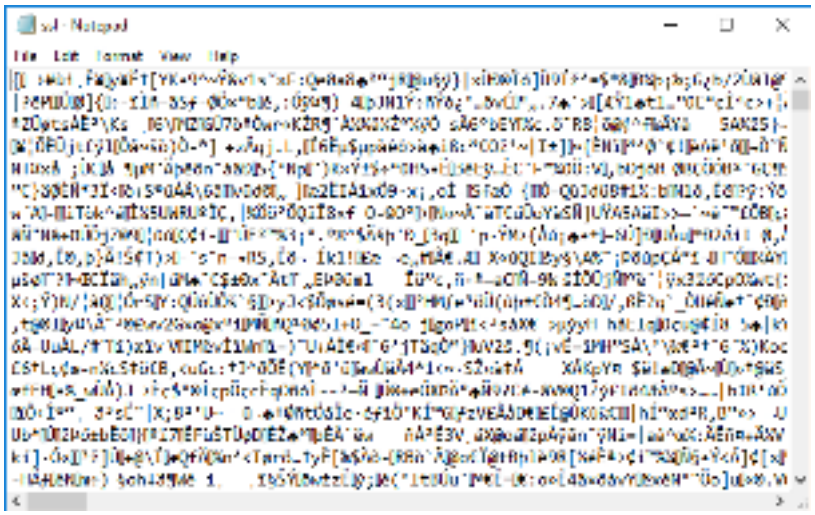
Gambar 4 Proses *Replay* Pada Packet Wireshark Menggunakan SSL

Pada hasil *replay* video yang tidak terlindungi SSL diambil 4 *frame* berbeda dan hasilnya masih dapat di*replay* seperti yang dapat ditunjukan pada gambar 3, sedangkan hasil *replay* video yang terlindungi SSL, file video yang telah disimpan tidak dapat di*replay* menggunakan media player seperti yang dapat ditunjukan pada gambar 4. Dikarenakan data video yang terlindungi SSL telah dienkripsi, maka jika raw data video diubah menjadi file video hasilnya video tersebut tidak dapat di*replay* menggunakan aplikasi *media player*.

Untuk memperkuat bukti keamanan SSL, maka dilakukan inspeksi dari setiap hasil video menggunakan aplikasi *text editor.* Hasil inspeksi pada hasil video yang terlindungi SSL dan yang tidak terlindungi SSL dapat ditunjukan pada gambar 5 dan 6.



Gambar 5 Hasil Inspeksi *Text Editor* pada File Video Tanpa SSL



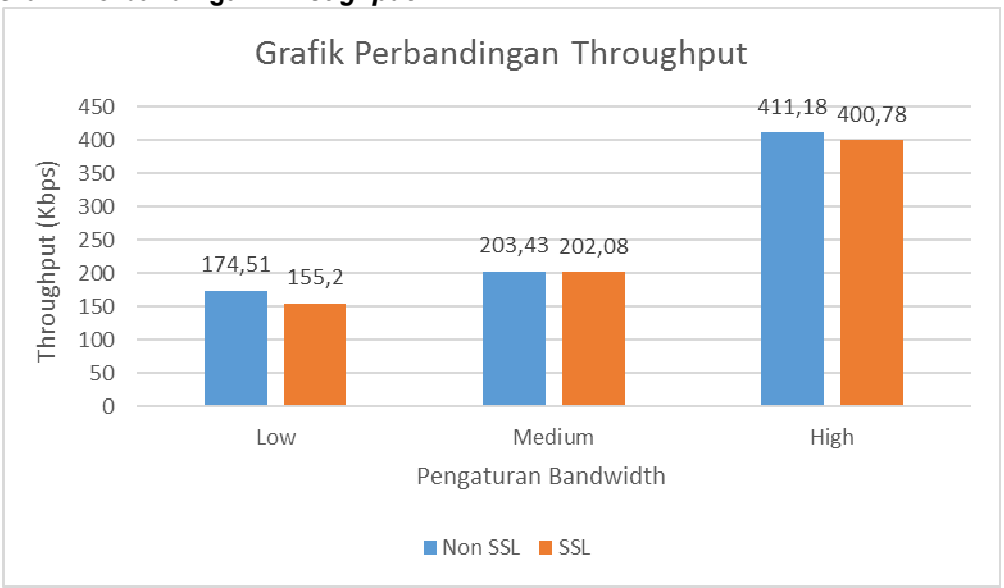
Gambar 6 Hasil Inspeksi *Text Editor* pada File Video SSL

Dari hasil inspeksi file video yang tidak terlindungi SSL, masih terdapat informasi dari video yang dapat dibaca seperti yang dapat ditunjukan pada gambar 5, sedangkan hasil inspeksi video yang terlindungi SSL tidak ada informasi yang dapat dibaca seperti yang ditunjukan pada gambar 6.

Dengan ini dapat disimpulkan bahwa proses *packet sniffing* pada SSL tidak berhasil dikarenakan video hasil *packet sniffing* tidak dapat di*replay* menggunakan aplikasi media player juga tidak memiliki informasi yang dapat dibaca pada aplikasi *text editor*, sedangkan *packet sniffing* tanpa SSL berhasil karena hasil video dapat di*replay* menggunakan aplikasi media player juga memiliki informasi yang dapat dibaca pada aplikasi *text editor*.

Grafik Perbandingan *Quality of Service* Berdasarkan Kualitas

Grafik Perbandingan *Throughput*

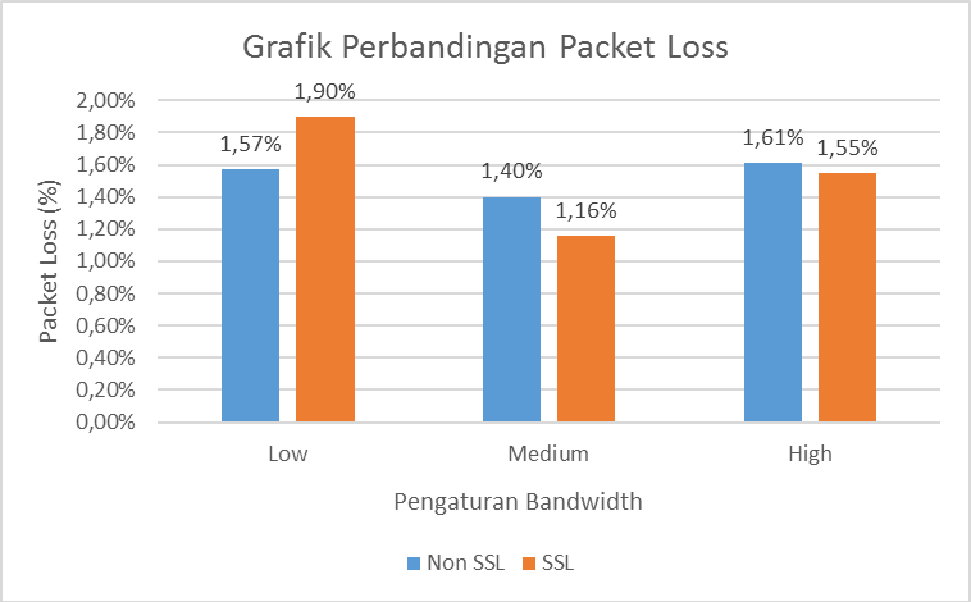


Gambar 7 Grafik Perbandingan *Throughput*

Dari grafik *throughput* pada gambar 7 dapat ditunjukan bahwa penggunaan *bandwidth* atau *throughput* pada SSL lebih rendah dibandingkan tanpa perlindungan SSL, diasumsikan karena proses enkripsi dari SSL membutuhkan *bandwidth* yang lebih

kecil dibandingkan dengan proses transmisi data tanpa enkripsi namun hasil yang ditunjukan sangat tidak signifikan.

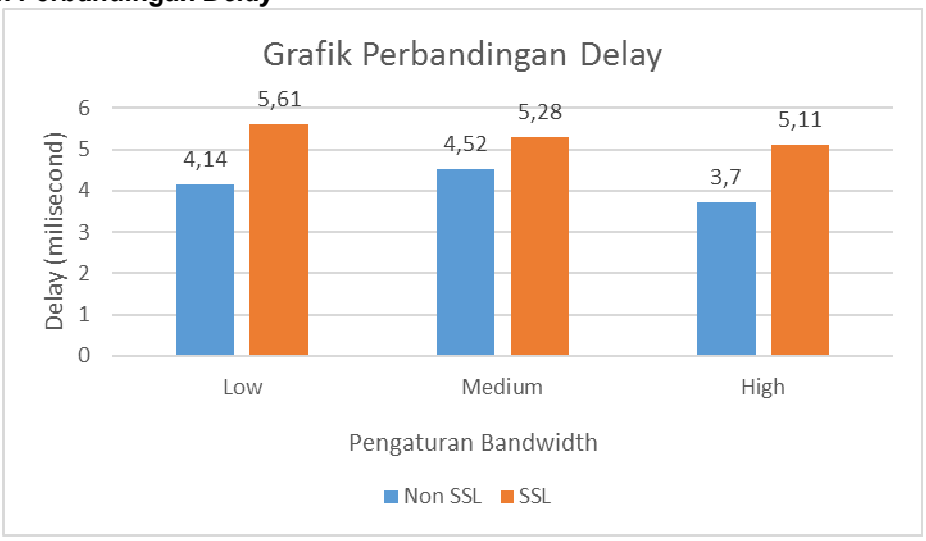
Grafik Perbandingan *Packet Loss*



Gambar 8 Grafik Perbadingan *Packet Loss*

Dari grafik perbandingan *packet loss* pada gambar 8 dapat ditunjukan bahwa tidak ada perbandingan yang signifikan antara sistem yang tidak terlindungi SSL dan yang terlindugi SSL. Diasumsikan karena tidak ada pengaruh dari proses enkripsi SSL terhadap *Packet Loss* yang dihasilkan, melainkan faktor yang mempengaruhi terjadinya *packet loss* adalah kesalahan pada perangkat keras, trafik jaringan yang *overload*, dan *collision data*.

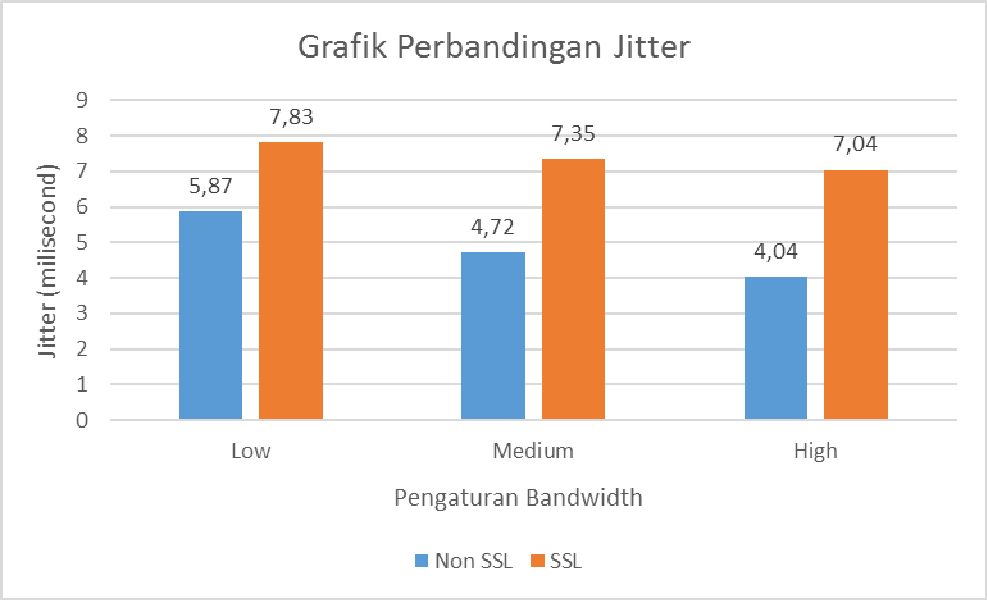
Grafik Perbandingan *Delay*



Gambar 9 Grafik Perbandingan *Delay*

Dari grafik perbandingan *delay* pada gambar 9 dapat ditunjukan bahwa delay dari sistem yang terlindungi SSL lebih besar dibandingkan dengan sistem yang tidak terlindungi SSL, diasumsikan karena proses enkripsi dari SSL menghasilkan *delay* yang lebih tinggi jika dibandingkan dengan transmisi data yang tanpa enkripsi SSL.

Grafik Perbandingan *Jitter*



Gambar 10 Grafik Perbandingan *Jitter*

Dari grafik perbandingan *jitter* pada gambar 10 dapat ditunjukan bahwa *jitter* dari sistem yang terlindungi SSL lebih besar dibandingkan dengan sistem yang tidak terlindungi SSL, diasumsikan karena proses enkripsi dari SSL menghasilkan jitter yang lebih tinggi dibandingkan dengan transmisi data yang tanpa enkripsi SSL.

Dari setiap hasil perbandingan dapat disimpulkan bahwa selisih perbandingan *Quality of Service* dari server Zoneminder yang terlindungi SSL dan yang tidak telindungi SSL menunjukkan angka yang tidak signifikan.

KESIMPULAN

Dari penelitian yang telah dilakukan, maka diperoleh beberapa kesimpulan sebagai berikut:

1. Implementasi Zoneminder pada Apache webserver berjalan dengan baik, berikut juga dengan implementasi SSL pada server zoneminder.
2. SSL mampu melindungi keamanan data dari *real-time video surveillance* dikarenakan video hasil *packet sniffing* tidak dapat di*replay* menggunakan aplikasi media player dan tidak memiliki informasi yang dapat dibaca pada aplikasi *text editor*. Sedangkan, *packet sniffing* tanpa SSL berhasil karena hasil video dapat di*replay* menggunakan aplikasi media player dan memiliki informasi yang dapat dibaca pada aplikasi *text editor*.
3. Hasil perbandingan *throughput* atau *bandwidth* pada server Zoneminder yang terlindungi SSL lebih rendah 19,31 Kbps untuk pengaturan *low*, 1,35 Kbps untuk pengaturan *medium*, dan 10,40 Kbps untuk pengaturan *high* jika dibandingkan server Zoneminder yang tidak terlindungi SSL.
4. Hasil perbandingan *packet loss* pada server Zoneminder yang terlindungi SSL lebih tinggi 0,33% pada pengaturan *bandwidth low,* sedangkan untuk pengaturan *bandwidth medium* lebih rendah 0,24%, dan untuk pengaturan *high* lebih rendah 0,06% jika dibandingkan dengan server Zoneminder yang tidak terlindungi SSL.
5. Hasil perbandingan *delay* pada server Zoneminder yang terlindungi SSL lebih tinggi 1,47 ms untuk pengaturan *low*, 0,76 ms untuk pengaturan *medium*, dan 1,41 ms untuk pengaturan *high* jika dibandingkan dengan server Zoneminder yang tidak terlindungi SSL.
6. Hasil perbandingan *jitter* pada server Zoneminder yang terlindungi SSL lebih tinggi 1,96 ms untuk pengaturan *low*, 2,63 ms untuk pengaturan *medium*, dan 3,00 ms

untuk pengaturan *high* jika dibandingkan dengan server Zoneminder yang tidak terlindungi SSL.

7. Hasil perbandingan data *Quality of Service* berdasarkan durasi diperoleh selisih angka yang kecil atau tidak signifikan.

DAFTAR PUSTAKA

Illyan, D. F., Nasution, S. M., dan Siswo, A. 2016. Pengamanan Data Video Surveillance Secara Real-Time Menggunakan Video Encryption Algorithm. e-Proceeding of Engineering Vol. 3, No. 2, 2016.

Pranata, H. Abdillah, L.A. Ependi, U. 2015. Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. Student Colloquium Sistem Informasi & Teknik Informatika. Agustus 2015.

Widyantara,I. M. O. Wedanti, N. U. dan Swamardika, I. B. A. 2015. Desain dan Implementasi Aplikasi Video Surveillance System Berbasis Web-SIG. Jurnal Teknologi Elektro Vol. 14, No. 1, 2015.

Wulandari, R. 2016. Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon – Lipi). Jurnal Teknik Informatika dan Sistem Informasi. Vol. 2, No. 2, 2016.

Yong-Hua, X., Wan S.Y., He Y., dan Su D. 2013. Design and Implementation of a Prototype Cloud Video Surveillance System. Journal of Advanced Computational Intelligence and Intelligent Informatics Vol. 18, No. 1, 2013.