PENINGKATAN KEAMANAN TRANSMISI REAL TIME VIDEO SURVEILLANCE MENGGUNAKAN SECURE SOCKET LAYER

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

Masuk: 06 Juli 2019, Revisi masuk: 20 Juli 2019, Diterima: 21 Juli 2019

ABSTRACT

Security is a very important aspect of data exchange. Usually, the data in video surveillance is transmitted only for certain parties. The data must accepted to entitled user with maintained confidentiality, and avoid from packet sniffing by others. Therefore, to secure the data in video surveillance, it needs a data encryption method to hide information.SSL (Secure Socket Layer) is reliable for securing a real-time data or video transmission. SSL can be implemented on a webserver that has public hosting. In this study, Zoneminder video surveillance system 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 no degradation on QoS and video quality.

Keywords**:** *Data transmission, Real time, SSL, Video surveillance, Zoneminder.*

INTISARI

Keamanan merupakan aspek yang sangat penting dalam pertukaran data video pengawasan. Pada umumnya, data video pengawasan hanya dikirim kepada pihak tertentu saja. Data harus sampai pada pihak yang berhak dengan kerahasiaan yang tetap terjaga, tanpa diketahui oleh pihak-pihak yang tidak berkepentingan. Untuk menjaga keamanan dan kerahasiaan data video pengawasan, perlu adanya metode enkripsi data untuk menyembunyikan informasi dari pihak ketiga. SSL (*Secure Socket Layer*) merupakan metode yang handal dalam mengamankan transmisi data / video secara real-time. SSL dapat diimplementasikan pada webserver yang memiliki public hosting. Pada penelitian ini, diimplementasikan Zoneminder *video surveillance system* pada webserver, dimana SSL diterapkan untuk enkripsi pada transmisi data antara server Zoneminder dan client. Hasil penelitian menunjukkan bahwa video pengawasan yang terlindungi SSL aman dari *packet sniffing* dan hasil perbandingan peforma tidak menunjukkan penurunan kualitas.

Kata-kata kunci: Real time, SSL, Transmisi data, Video surveillance, Zoneminder.

PENDAHULUAN

Video Streaming adalah sebuah jenis layanan yang dapat langsung mengolah data yang diterima tanpa menunggu seluruh data selesai terkirim. Ide dasar dari video streaming adalah membagi paket video ke dalam beberapa bagian, mentransmisikan paket tersebut, kemudian penerima dapat mendecode dan memainkan potongan paket file video tanpa harus menunggu seluruh file terkirim ke mesin penerima (Satwika, 2011).

Surveillance dalam Bahasa Inggris memiliki arti “pengawasan, penjagaan, pengamatan”. Video surveillance merupakan video yang digunakan untuk keperluan pengawasan, dan direkam menggunakan kamera. Kamera pengintai adalah teknologi yang dirancang sebagai alat pemantauan keamanan.Kamera pengintai telah diterapkan di banyak teknologi dan dalam beberapa versi seperti CCTV, IP Camera, maupun WebCam (Illyan dkk., 2016).

Kemajuan teknologi membuat penggunaan video pengawasan

(*surveillance*) dalam kehidupan sehari-hari semakin penting guna meningkatkan keamanan dan kerahasiaan bagi penggunanya. *Surveillance system* merupakan teknologi yang dipakai untuk meningkatkan pengawasan pada tempat atau lokasi yang lepas dari jangkauan penglihatan atau tempat tersebut sedang ditinggalkan sehingga tidak ada yang bisa mengawasi secara langsung contohnya rumah atau tempat kerja.

Video pengawasan banyak digunakan untuk merekam gambar pada suatu kegiatan/kejadian oleh instansi seperti perbankan, perkantoran, pertahanan negara, dan lain-lain. Masalah yang sering terjadi dalam pengiriman video real-time terletak pada kemungkinan bahwa informasi yang dipertukarkan dapat diakses oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu kerahasiaan menjadi hal yang penting.

Kerahasiaan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Perlindungan kerahasiaan data 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. Integritas dalam video surveillance menjadi hal yang penting karena apabila tidak terpenuhi dapat mengakibatkan masalah terjadinya manipulasi serta penghapusan terhadap data asli. Salah satu solusi untuk menghindari resiko penyerangan terhadap informasi adalah dengan melakukan tindakan enkripsi menggunakan SSL atau Secure Socket Layer.

Secure Socket Layer adalah salah satu metode keamanan dalam bentuk sebuah protokol yang berada di atas Transmission Control Protocol/Internet Protocol (TCP/IP) yang berfungsi untuk mengamankan browsing web, mengelola keamanan transmisi dan juga dapat menjamin keamanan dalam pengiriman data dan pengaksesan informasi pada saat client dan server sedang melakukan pertukaran informasi lewat internet (Monica, 2015). Setiap kali pengunjung web mengunjungi situs yang aman menggunakan teknologi SSL, menciptakan sebuah tautan yang terenkripsi antara sesi browser client dan web server. SSL menjadi standar industri untuk komunikasi web yang aman dan digunakan untuk melindungi web.

Penelitian ini bertujuan untuk mengimplementasikan suatu metode untuk mengamankan integritas data real-time video surveillance menggunakan Secure Socket Layer. Karena perangkat Video Surveillance yang digunakan adalah sebuah IP Camera, maka dibutuhkan webserver untuk menempatkan Zoneminder Video Surveillance System. Webserver akan meneruskan akses yang sudah terlindungi SSL secara publik dari IP Camera ke Client. Dengan diimplementasikannya SSL pada Real-time video surveillance ini diharapkan dapat melindungi integritas data video dari pihak-pihak yang tidak berwenang.

Penelitian terdahulu terkait dengan pengamanan video pengawasan pernah dilakukan oleh Yong-Hua, dkk. (2013) yang mendesain dan mengimplementasikan metode untuk sistem video surveillance berbasis cloud. Prototipe sistem video surveillance berbasis cloud dibangun di jaringan kampus menggunakan teknologi cloud, termasuk kontrol akses tugas mesin virtual, penyimpanan data-data terdistribusi, dan metode komunikasi aktif basis data. Penelitian berikutnya dilakukan oleh Widyantara, dkk. (2015) dengan membangun aplikasi VSS (Video Surveillance System) yang memudahkan monitoring setiap IP Camera. Aplikasi tersebut 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. Illyan, dkk. (2016) merancang sistem pengamanan data pada video Surveillance, dengan teknik enkripsi menggunakan VEA (Video Encryption Algorithm) dan kunci tertentu, lalu memberikan hak akses secara aman kepada orang yang benar-benar berhak.

Kemudian dilakukan analisis kinerja algoritma VEA pada parameter waktu proses enkripsi dan dekripsi, serta waktu tunda (delay).

Penelitian terkait pengamanan video surveillance pernah dilakukan oleh Pranata, dkk. (2015) untuk menganalisis sejauh mana SSL dapat mengamankan data di jaringan. Ketika komputer mengirim data melalui jaringan, maka data dikirimkan dalam bentuk paket. Ancaman keamanan yang dilakukan oleh sniffer adalah kemampuannya untuk menangkap semua paket yang masuk dan keluar melalui jaringan, yang meliputi kata sandi, nama pengguna dan masalah sensitif lainnya. Penelitian ini menganalisis informasi berupa paket data berbentuk ASCI seperti *username* dan *password*. Sedangkan Wulandari (2016) melakukan penelitian untuk menganalisis kualitas layanan (*Quality of Service/QoS*) jaringan dengan mengukur seberapa baik jaringan dan upaya untuk menentukan karakteristik dan sifat layanan. QoS 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.

Hasad dan Paronda (2016) menganalisis dan melakukan optimasi terhadap kinerja sistem pada transmisi data rate video streaming melalui jaringan Bluetooth Piconet Pervasive, dengan symbian OS pada sisi client. Hasil penelitian menunjukkan bahwa semakin besar interferensi Wi-Fi pada jaringan bluetooth piconet pervasive, maka kualitas video yang diterima di *client* (telepon seluler) semakin berkurang, ditandai dengan semakin besarnya nilai rata-rata *packet loss* yang didapatkan selama video streaming.

Rifai, dkk. (2016) melakukan analisis protokol RTSP yang diimplementasikan pada sebuah raspberry pi sebagai *live streaming serve*r untuk *video surveillance system* yang terintegrasi dengan camera pengawas. Hasil penelitian menunjukkan bahwa protokol RTSP memiliki kelebihan dalam kualitas output video tetapi untuk kinerja lebih baik protokol RTMP karena nilai *delay*-nya lebih kecil sehingga pengiriman data lebih cepat. Kehandalan raspberry pi sebagai *live streaming server* memiliki stabilitas yang baik saat menjalankan video streaming pada jaringan *video surveillance system* yang diakses oleh *user* atau *client*.

Muryanti dan Affandi (2018) membuat sistem keamanan *video on demand* (VoD) yang mengimplementasikan Video Encryption Algorithm (VEA). Metode ini membaca frame pada suatu video, kemudian dari masing-masing frame tersebut dibaca dalam bit-bit, dan dilakukan operasi XOR dengan *byte* kunci tertentu. Setelah itu, VEA dituliskan pada file VoD. Hasil pengujian menunjukkan bahwa video yang terenkripsi dengan perubahan panjang kunci tidak berpengaruh terhadap *delay* tetapi berpengaruh terhadap kualitas video.

Berdasarkan tinjauan pustaka di atas, dikembangkan implementasi SSL pada *live-stream video surveillance* menggunakan aplikasi Zoneminder dan Apache Webserver. Implementasi SSL pada *Real-time video surveillance* diharapkan dapat melindungi integritas data video dari pihak-pihak yang tidak berwenang.

Alat-alat yang digunakan dalam penelitian ini meliputi perangkat keras, perangkat lunak, dan perangkat pendukung lainnya. Perangkat keras terdiri dari IP camera, komputer server, dan komputer klien. Perangkat lunak yang digunakan berupa Apache web server versi 2.4.35, Zoneminder versi 1.29.0, *web browser*, Media player, serta Wireshark untuk pemantauan lalu lintas jaringan. Data yang diperlukan dalam penelitian ini adalah hasil analisis kinerja *Real-time Video Surveillance*; antara lain *Packet loss, Troghput, Delay,* dan *Jitter.*

Metode pengumpulan data yang digunakan dalam penelitian ini yaitu: (1) Metode observasi, dengan melakukan pengamatan cara kerja perangkat lunak, perangkat keras, dan jaringan yang digunakan dan (2) Metode studi pustaka, dengan melakukan pengumpulan data dan referensi yang berkaitan dengan penelitian dan perangkat yang digunakan.

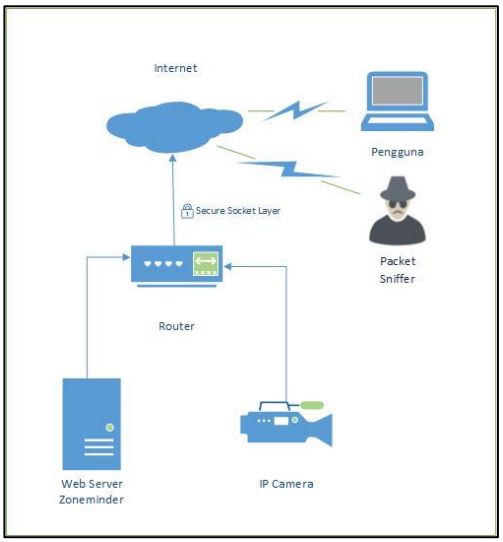
Langkah-langkah penelitian menerapkan konsep *waterfall* untuk meminimalisir kesalahan pada setiap langkah penelitian, yang terdiri dari: (1) Analisis, (2) Perancangan sistem, (3) Pengembangan sistem, (4) Pengujian sistem, (5) Analisis keamanan dan kinerja, serta (6) Implementasi sistem.

PEMBAHASAN

Zoneminder merupakan *Real-time Video Surveillance System* berbasis PHP yang dapat diimplementasikan pada webserver. Zoneminder berfungsi sebagai aplikasi untuk melakukan pemantauan suatu lokasi indoor atau outdoor menggunakan IP Camera sebagai media pemantauan. Dalam penelitian ini Zoneminder diimplementasikan pada apache2 webserver dengan *server* berbasis linux debian 8.

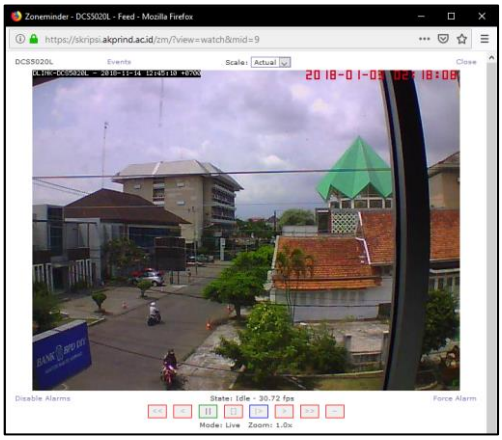
Gambar 1 merupakan rancangan arsitektur sistem yang menunjukkan video diakses oleh pengguna secara publik menggunakan jaringan internet. Akses yang dituju adalah Web server Zoneminder. Zoneminder akan melakukan *stream data* ke IP Camera yang telah terdaftar di sistem Zoneminder dan mengirim data yang telah dienkripsi oleh SSL kembali ke *client*

.



Gambar 1. Rancangan arsitektur sistem Simulasi Real-Time Video Surveillance pada Zoneminder

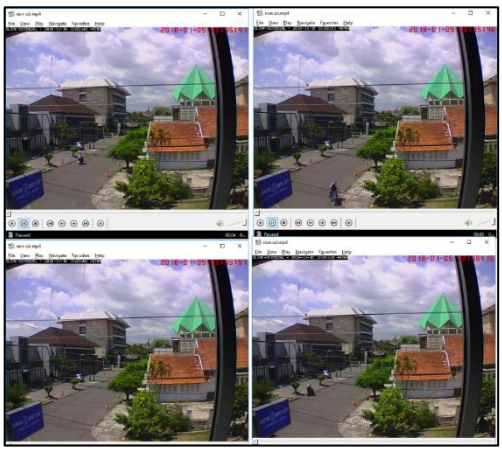
Simulasi *Real-time Video Surveillance* dilakukan dengan menjalankan *Live Stream* pada *web browser* Mozila Firefox. Pengguna juga dapat mengontrol pergerakan kamera menggunakan fitur Control pada Zoneminder. Simulasi *Real-time Video Surveillance* pada Zoneminder ditunjukkan pada Gambar 2.



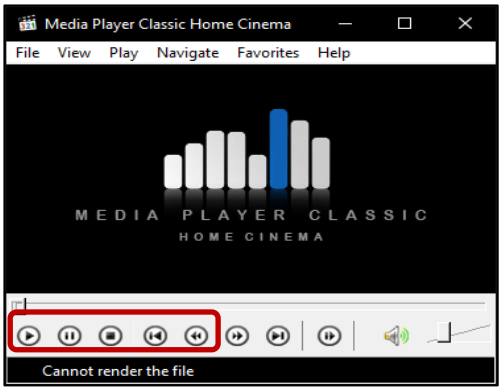
Gambar 2. Simulasi pada Zoneminder

Hasil Pengujian Packet Sniffing

Pada hasil *replay* video yang tidak terlindungi SSL diambil 4 frame berbeda dan hasilnya masih dapat di-*replay* seperti ditunjukkan pada Gambar 3. Sedangkan hasil *replay* video yang terlindungi SSL, file video yang telah disimpan tidak dapat di-*replay* menggunakan media player seperti ditunjukkan pada Gambar 4.

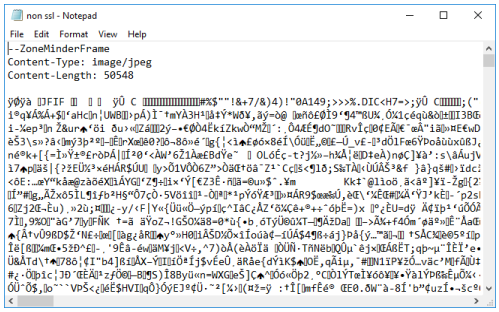


Gambar 3. Proses *replay* pada *packet* Wireshark tanpa SSL



Gambar 4. Proses *replay* pada packet Wireshark dengan SSL

Gambar 4 menunjukkan data video yang terlindungi SSL telah terenkripsi, sehingga jika *raw* data video diubah menjadi file video maka 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 video yang terlindungi SSL dan yang tidak ditunjukkan pada Gambar 5 dan 6.



Gambar 5. Hasil inspeksi *text editor* pada file video tanpa SSL

Berdasarkan hasil inspeksi file video yang tidak terlindungi SSL, masih terdapat informasi dari video yang dapat dibaca seperti ditunjukkan pada Gambar 5 yaitu berupa informasi *content-type* dan *content-length*. Informasi *Content-type* menunjukkan bahwa file tersebut berupa image/jpeg, dengan ukuran file sebesar 50548 *bytes*. Sedangkan hasil inspeksi video yang terlindungi SSL tidak ada informasi yang dapat dibaca seperti yang ditunjukkan pada Gambar 6.

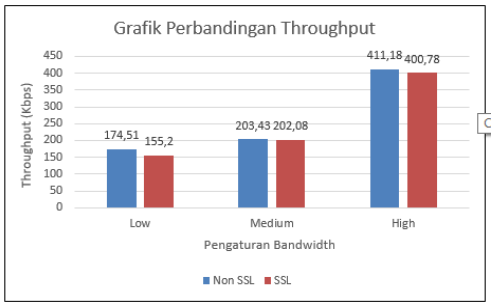
Gambar 6. Hasil inspeksi *text editor* pada file video dengan SSL

Berdasarkan hasil pengujian dapat disimpulkan bahwa proses *packet sniffing* pada SSL tidak berhasil karena video hasil *packet sniffing* tidak dapat di-*replay* menggunakan aplikasi media player serta tidak memiliki informasi yang dapat dibaca pada aplikasi text editor. Sedangkan hasil *packet sniffing* tanpa SSL berhasil dibaca karena hasil video dapat di-*replay* menggunakan aplikasi media player serta memiliki informasi yang dapat dibaca pada *text editor*.

Perbandingan *Quality of Service*

Perbandingan *Throughput*

Gambar 7 memperlihatkan grafik penggunaan *bandwidth/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 ditunjukkan tidak signifikan.

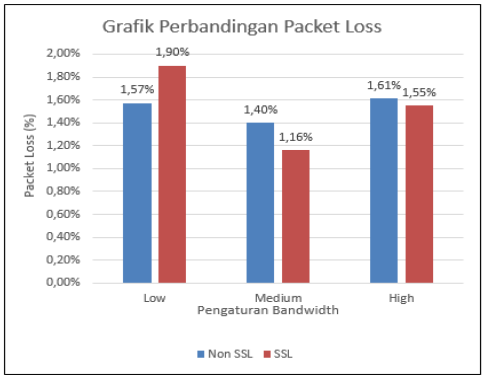


Gambar 7. Perbandingan *throughput*

Perbandingan *Packet Loss*

Gambar 8 menunjukkan bahwa tidak ada perbedaan *packet loss* yang signifikan antara sistem yang tidak terlindungi SSL dan yang terlindungi

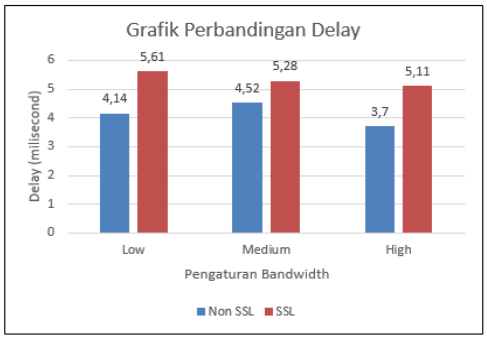
SSL. Perbedaan tersebut lebih disebabkan karena faktor trafik jaringan dan *data collision*.



Gambar 8. Perbandingan *packet loss*

Perbandingan *Delay*

Gambar 9 menunjukkan bahwa *delay* dari sistem yang terlindungi SSL lebih besar dibandingkan dengan sistem yang tidak terlindungi SSL. Hal tersebut disebabkan karena enkripsi memerlukan proses lebih lama sehingga menyebabkan delay, dibandingkan dengan transmisi data yang tanpa enkripsi SSL.



Gambar 9. Perbandingan *delay*

Perbandingan Jitter

Gambar 10 menunjukkan bahwa *jitter* pada sistem yang terlindungi SSL lebih besar dibandingkan dengan sistem yang tidak terlindungi SSL. Hal tersebut disebabkan karena proses enkripsi dari SSL menyebabkan waktu tunda yang lebih tinggi dibandingkan dengan transmisi data yang tanpa enkripsi SSL.

Perbandingan *QoS* dari server Zoneminder yang terlindungi SSL dan yang tidak telindungi SSL menunjukkan angka yang tidak signifikan; dengan perbandingan *throughput* 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* dibandingkan dengan server Zoneminder yang tidak terlindungi SSL. Sedangkan perbandingan *packet loss* pada server Zoneminder yang terlindungi SSL lebih tinggi 0,33% pada pengaturan *bandwidth low*, pada *bandwidth medium* lebih rendah 0,24%, dan untuk pengaturan high lebih rendah 0,06% jika dibandingkan dengan server Zoneminder yang tidak terlindungi SSL. Pada parameter *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. Parameter *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.

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka diperoleh kesimpulan sebagai berikut:

1. SSL mampu melindungi keamanan data *real-time video surveillance* karena 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*.
2. Berdasarkan hasil perbandingan *troughput, delay, packet loss,* dan *jitter* dapat disimpulkan bahwa selisih perbandingan *Quality of Service* dari server Zoneminder yang terlindungi SSL dan yang tidak telindungi SSL menunjukkan angka yang tidak signifikan.

DAFTAR PUSTAKA

Hasad, A. dan Paronda, A. H., 2016, Analisis Keamanan Sistem Pada Transmisi Data Rate Video Streaming Melalui Jaringan Bluetooth Piconet Pervasive, *Journal of Electrical and Electronics*, vol 4, hal. 99-102.

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, hal. 2179-2185.

Monica, S. U, 2015, Secure Communication using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks, *Procedia Computer Science*, vol. 70, hal. 808-813.

Muryanti, S. D. P., dan Affandi, A., 2018, Rancang Bangun Sistem Keamanan Konten Video on Demand (VoD) Pada Internet Protocol Television (IPTV) Menggunakan Video Encryption Algorithm (VEA), *Digilib ITS*, hal. 1-6

Pranata, Abdillah, L. A., dan Ependi, U., 2015, Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan, *Student Colloquium Sistem Informasi & Teknik Informatika*, Universitas Bina Darma, hal. 1-6.

Rifai, M. H, Irawan, B., dan Saputra, R. E., 2016, Analisis Performansi RTSP Live Streaming Server Berbasis Raspberry Pi untuk Video Surveillance System, *e-Proceeding of Engineering*, vol. 3, hal. 2268-2275.

Satwika, I. K. S. 2011, *Proses Video Streaming dengan Protocol Real Time Streaming Protocol (RTSP)*, Universitas Udayana.

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, hal. 41-46.

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, hal. 162-172.

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, hal. 40-47.

BIODATA PENULIS

Catur Iswahyudi, S.Kom., S.E., M.Cs., **MTA**, lahir di Kudus tanggal 19 Juni 1973, menyelesaikan studi S1 tahun 2000 di Jurusan Teknik Informatika IST AKPRIND Yogyakarta dan S1 Jurusan Manajemen di Universitas Terbuka tahun 2004, dan S2 tahun 2005 di Jurusan Ilmu Komputer UGM. Saat ini bertugas sebagai Dosen Tetap di Jurusan Teknik Informatika IST AKPRIND Yogyakarta dengan jabatan akademik Lektor pada bidang minat jaringan komputer dan keamanan jaringan.

Nanda Adi Pratama, S.Kom., lahir di Abepura tanggal 27 Mei 1996, menyelesaikan studi S1 tahun 2018 di Jurusan Teknik Informatika IST AKPRIND Yogyakarta, dengan bidang minat jaringan komputer.

Joko Triyono, S.Kom., **M.Cs.**, lahir di Magelang tanggal 6 Agustus 1967, menyelesaikan studi S1 tahun 2001 di Jurusan Teknik Informatika IST AKPRIND Yogyakarta, dan S2 tahun 2010 di Jurusan Ilmu Komputer UGM. Saat ini bertugas sebagai Dosen Tetap di Jurusan Teknik Informatika IST AKPRIND Yogyakarta dengan jabatan akademik Asisten Ahli pada bidang minat jaringan komputer.