SECURE SOCKET LAYER UNTUK KEAMANAN DATA REKAM MEDIS *TUMOR* OTAK PADA HEALTH INFORMATION SYSTEM

Novi*, Zaini
Jurusan Teknik Elektro, Fakultas Teknik, Universitas Andalas
*Corresponding author, e-mail : shenovi00@gmail.com

Abstrak—Penelitian ini bertujuan untuk membangun sistem keamanan data rekam medis tumor otak pada *Health Information System* (HIS) dengan mengimplementasikan protokol *Secure Socket Layer* (SSL) pada saluran komunikasi antara *client* dan *server* untuk mencegah terjadinya penyusupan pada lalu lintas data di internet. Sertifikat SSL dirancang menggunakan *tool OpenSSL* dengan algoritma RSA (*Rivest-Shamir-Adleman*) dan enkripsi AES (*Advance Encryption Standard*) 256 bit, kemudian ditanamkan melalui bahasa pemrograman *Python* pada mini *computer Raspberry Pi* yang berfungsi sebagai *server* pada sistem. Hasil pengujian menunjukkan bahwa protokol SSL dapat mengenkripsi saluran komunikasi dan mengamankan data dari teknik *sniffing* dan *attacking* selama terjadinya proses pertukaran data di jaringan internet.

Kata Kunci : Secure Socket Layer, Keamanan Data, *Raspberry Pi.*

Abstract—This research aims to build a data security system medical records of brain tumor on Health Information System (HIS) by implementing the Secure Socket Layer (SSL) protocol on the communication channel between the client and server to prevent the infiltration of data traffic on the internet. SSL certificates are designed using Open SSL tool with RSA (Rivest-Shamir-Adleman) algorithm and 256 bit AES (Advance Encryption Standard) encryption, then implanted through the Python programming language on Raspberry Pi mini computer acting as a server on the system. The test result showed that the SSL protocol to encrypt and secure data communication channels from sniffing and attacking techniques during the data exchange process in the internet network.

Keywords : Secure Socket Layer, Data Security, Raspberry Pi.

1. PENDAHULUAN

Seiring dengan kemajuan teknologi informasi, juga terjadi inovasi teknologi yang begitu cepat di bidang kesehatan. Inovasi teknologi yang memungkinkan digitalisasi dan otomatisasi pada proses pencatatan medis. Otomatisasi ini lebih dikenal dengan *Health Information System* (HIS). HIS [1] adalah upaya terpadu untuk mengumpulkan, memproses, melaporkan dan menggunakan informasi kesehatan untuk menentukan kebijakan dan pengambilan keputusan, tindakan program, serta penelitian.

HIS [2] berisi semua informasi kesehatan, mulai dari perawatan, pengobatan, data administrasi, dan keuangan. Selain itu, pada HIS juga terdapat data-data sensitif yang bersifat rahasia, salah satu diantaranya adalah data rekam medis tumor otak. Rekam medis [3] ini tidak hanya berisi catatan dari identitas pasien, tetapi juga menjelaskan hubungan yang khusus antara pasien dan dokter. Seperti mengenai pemeriksaan terhadap pasien, diagnosa penyakit yang diderita oleh pasien, pengobatan yang diberikan oleh dokter dan tindakan medis lainnya yang wajib dilindungi dari pembocoran sesuai dengan kode etik kedokteran dan peraturan perundang-undangan yang berlaku.

Data rekam medis tumor otak pada HIS akan dipakai oleh berbagai pengguna di rumah sakit, diantaranya adalah dokter, perawat, apoteker, bagian administrasi, dan lain sebagainya. Data ini diakses melalui jaringan internet. Tanpa adanya protokol keamanan yang tepat, tentunya data-data rekam medis tumor otak pada HIS bisa saja disadap dan disalahgunakan oleh berbagai pihak, contohnya perusahaan asuransi, pengusaha, dan orang atau organisasi yang tertarik memanfaatkan data ini untuk kepentingan pribadi.

Oleh sebab itu, maka *Secure Socket Layer* (SSL) merupakan pilihan yang tepat sebagai

Received date 2017-05-31, Revised date 2017-07-22, Accepted date 2017-07-23
DOI : 10.25077/jnte.v6n3.405.2017

sistem keamanan data yang akan melindungi data rekam medis tumor otak selama diakses melalui jaringan internet. SSL [4] merupakan teknologi keamanan data yang tangguh dengan menggunakan konsep enkripsi, dan sampai saat ini telah dipercaya untuk keamanan data-data yang sensitif, seperti perbankan *web*, perdagangan saham, dan *e-commerce*.

SSL telah digunakan pada beberapa penelitian sebelumnya, salah satu diantaranya adalah "*Data Security in Cloud Oriented Application Using SSL Protocol*" yang dilakukan oleh Irvin Singh Dua dan dipublikasikan di *International Journal of Application or Innovation in Engineering & Management* tahun 2013. Penelitian ini merancang SSL untuk mengamankan data di aplikasi berorientasi *cloud* sehingga data tersebut tidak dapat diakses oleh pengguna yang tidak sah ketika ditransfer dari *server* ke *browser*. Tetapi di penelitian ini masih ditemukan beberapa kekurangan, diantaranya adalah kualitas dari SSL yang dirancang masih sangat lemah untuk dapat mengamankan data. Karena SSL dirancang hanya dengan memanfaatkan beberapa fitur sederhana yang terdapat pada sistem operasi *Windows*, yaitu *Microsoft.NET Framework* dan *class SslStream*. Ruang lingkup dari SSL ini pun sangat terbatas, yaitu hanya bisa digunakan pada sistem operasi *Windows* saja.

Pada penelitian ini penulis merancang SSL menggunakan *tool OpenSSL* dengan algoritma RSA (*Rivest-Shamir-Adleman*) dan enkripsi AES (*Advance Encryption Standard*) 256 bit, kemudian ditanamkan melalui bahasa pemrograman *Phyton* pada mini *computer Raspberry Pi* dan diharapkan dapat menyempurnakan beberapa penelitian sebelumnya.

2. TINJAUAN PUSTAKA

2.1. Keamanan Data

Keamanan data [5] merupakan suatu tindakan digital yang diterapkan untuk melindungi dan mencegah akses tidak sah ke komputer, database, dan situs *web.* Ukuran teknologi untuk keamanan data yang paling utama adalah enkripsi, dimana data digital, perangkat lunak maupun perangkat keras, dan *hard drive* dienkripsi sehingga tidak dapat diakses oleh pengguna yang tidak sah.

Salah satu metode yang paling sering dijumpai dalam mempraktikkan keamanan data adalah penggunaan otentikasi. Dengan otentikasi, pengguna harus memberikan kata sandi, kode, data biometrik, atau beberapa bentuk data lainnya untuk memverifikasi identitas sebelum mengakses sistem atau data yang diberikan.

Keamanan data juga sangat penting untuk catatan perawatan kesehatan, sehingga advokat kesehatan dan praktisi medis di AS dan negara-negara lain bekerja untuk menerapkan privasi rekam medis dengan menciptakan kesadaran tentang hak pasien terkait dengan pelepasan data ke laboratorium, dokter, rumah sakit, dan fasilitas medis lainya.

2.2. *Secure Socket Layer* (*SSL*)

Secure Socket Layer [6] 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.

Teknologi SSL menggunakan konsep kriptografi kunci publik untuk bisa mencapai komunikasi yang aman antara *server* dan *client.* Kedua pihak yang berkomunikasi (*server* dan *client)* saling mengirimkan data yang disamarkan dengan teknik enkripsi, dan untuk membaca data tersebut digunakan kunci yang hanya dimiliki oleh kedua pihak yang sedang berkomunikasi saja. Sehingga apabila ada pihak lain yang mencoba untuk menyadap, data tidak akan terbaca.

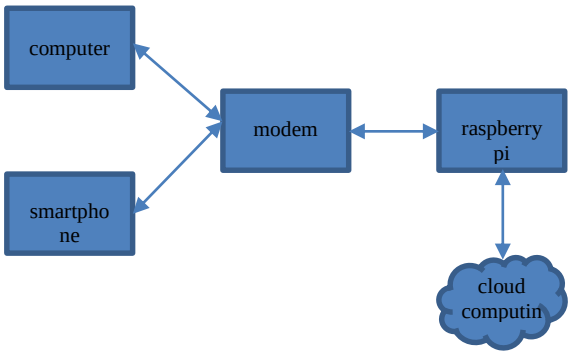
2.3. Raspberry Pi

Raspberry Pi [7] adalah komputer mini yang berukuran kecil sebesar kartu ATM dan dapat berfungsi sama dengan *Personal Computer* (PC), sehingga dapat digunakan sebagai *server* pada sistem. Layaknya sebuah PC, *Raspberry Pi* juga membutuhkan *Operating System* (OS) agar dapat digunakan. OS ini disimpan dalam *Secure Digital* (SD) *Card* yang juga berfungsi sebagai media penyimpanan data seperti halnya *hard disk*. OS yang digunakan untuk *Raspberry Pi* merupakan varian dari OS *Linux*.

3. METODOLOGI

3.1. Perancangan Sistem

Perancangan sistem secara umum dapat dilihat pada blok diagram berikut ini

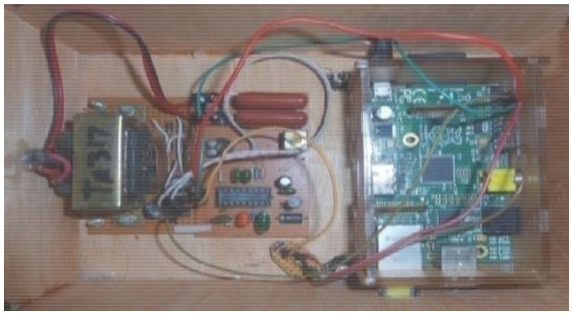


Gambar 1. Blok Diagram Sistem

Gambar 1 merupakan blok diagram sistem secara keseluruhan. Data rekam medis tumor otak yang tersimpan pada *cloud computing* dapat diakses melalui *computer* atau *smartphone* dengan menggunakan jaringan internet. *Raspberry Pi* dan *Modem* akan bekerja sama sehingga dapat berfungsi sebagai *server* yang akan melayani setiap permintaan dari *client*.

Ketika *client* mengajukan permintaan koneksi terhadap *server*, maka *server* akan memberikan sertifikat SSL. Selanjutnya akan terjadi proses pertukaran data antara *client* dan *server* dengan menggunakan proses enkripsi melalui protokol SSL.

3.2. Perancangan *Hardware*



Gambar 2. Perancangan *Hardware*

Gambar 2 merupakan perancangan *hardware* yang terdiri dari dua komponen utama yaitu *Modem* dan *Raspberry Pi*. *Raspberry Pi* [8] berkomunikasi dengan *Modem* menggunakan komunikasi serial. *Modem* ini menggunakan IC LM1893 dengan tipe modulasi *Binary Frekuency Shift Keying* yang dapat berkomunikasi dua arah. *Modem* memiliki tiga pin antarmuka dengan *Raspberry Pi*, yaitu TX (pin 17), RX (pin 12), dan *selector* (pin 5). TX *Modem* dihubungkan dengan PD.1 (TXD) pada *Raspberry Pi*, RX *Modem* dihubungkan dengan PD.0 (RXD) pada *Raspberry Pi*, dan *selector* dihubungkan ke PD.2 pada *Raspberry Pi*.

Fungsi *selector* pada *Modem* adalah sebagai pemilih mode *Modem*, kerja *Modem* sebagai pengirim atau sebagai penerima. Ketika *selector* pada *Modem* bernilai *high* maka *Modem* dikondisikan sebagai pengirim, pada saat *Modem* bekerja sebagai pengirim maka *input* data serial yang terhubung pada pin TX akan dimodulasi secara BFSK. Data hasil modulasi kemudian ditransmisikan melalui lalu lintas data ke *client*. Sebaliknya ketika *selector* pada *Modem* bernilai *low* maka *Modem* dikondisikan sebagai penerima. Kerja *Modem* saat sebagai penerima adalah kebalikan ketika *Modem* sebagai pengirim. Jika ada data yang masuk maka data akan didemodulasi oleh *Modem* sehingga data dapat dikenali oleh *Raspberry Pi*. Kemudian data hasil demodulasi tersebut disalurkan pada pin RX yang dihubungkan ke pin RXD pada *Raspberry Pi*.

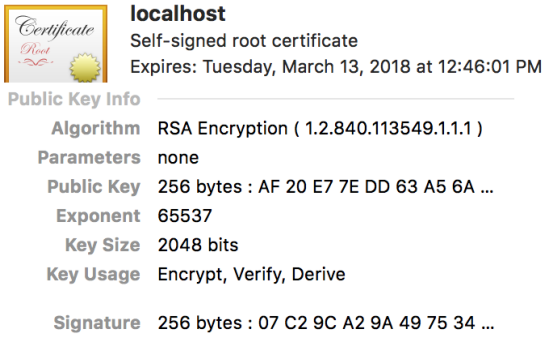
Raspberry Pi digunakan sebagai *web server* yang akan melayani permintaan pengguna melalui *web browser* berupa tampilan halaman *web* yang telah ditanamkan dalam modul *Raspberry Pi*. Tampilan halaman *web* yang ditampilkan tersebut digunakan sebagai antar muka untuk mengakses data rekam medis tumor otak pada aplikasi HIS.

3.3. Perancangan *Software*

Perancangan *software* terdiri dari beberapa bagian yaitu :

1. Instalasi OS
2. Instalasi *Web Server*
3. Konfigurasi sertifikat SSL

Sertifikat SSL dirancang menggunakan algoritma RSA (*Rivest-Shamir-Addleman*) dan enkripsi AES (*Advance Encryption Standard*) 256 bit dengan menggabungkan beberapa *class* yang terdapat pada *OpenSSL* dan aplikasi *Keytool* yang merupakan bawaan dari *Java SDK*.

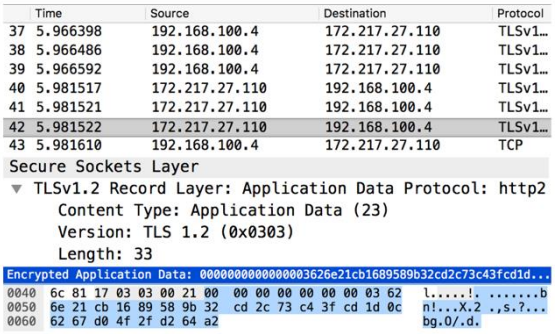


Gambar 3. Desain Sertifikat SSL

4. HASIL DAN PEMBAHASAN

4.1. Kerahasiaan Data

Untuk menguji apakah kerahasiaan data dapat terjaga setelah menggunakan protokol SSL pada sistem, maka digunakan metode *sniffing*. *Sniffing* [9] merupakan jenis serangan yang bersifat pasif, karena pada teknik *sniffing* penyerang tidak melakukan tindakan apa-apa selain memantau data yang lewat pada saluran komunikasi antara *client* dan *server*.



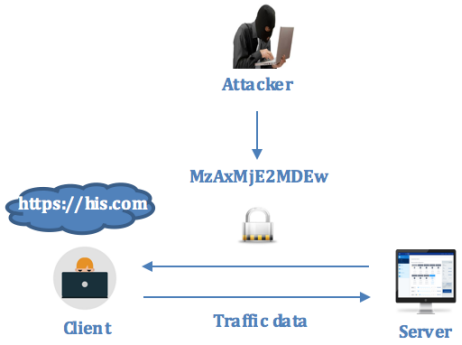
Gambar 4. *Sniffing*

Pada gambar 4 dapat dilihat bahwa data telah dienkripsi oleh protokol SSL, ketika dilakukan pengujian melalui teknik *sniffing* yang terlihat hanya berupa sandi-sandi tertentu. Dimana sandi-sandi tersebut hanya bisa dimengerti oleh dua pihak yang sedang berkomunikasi yaitu *client* dan *server*, sehingga data tidak dapat terbaca dan disalah gunakan oleh pihak-pihak yang tidak berkepentingan.

Dengan demikian maka dapat disimpulkan bahwa protokol SSL telah memberikan keamanan yang berlapis terhadap data rekam medis tumor otak yang diakses melalui jaringan internet, dan dapat menjamin keamanan data terutama dalam hal kerahasiaan.

4.2. Keutuhan Data

Data yang dikirim melalui jaringan internet diharapkan tidak akan mengalami perubahan yang disebabkan oleh tindak kejahatan dari pihak-pihak yang tidak berwenang, sehingga data tetap utuh ketika sampai di tujuan. Oleh sebab itu maka dilakukan simulasi serangan dengan metode *Man-In-The-Middle* (MITM *attack*), yang bertujuan untuk menguji keutuhan data. MITM *attack* [10] merupakan suatu jenis serangan yang bersifat aktif dan sangat berbahaya, karena penyerang tidak hanya bisa menyadap data di jaringan internet tetapi juga bisa mencegat dan mengubah bahkan memalsukan data.

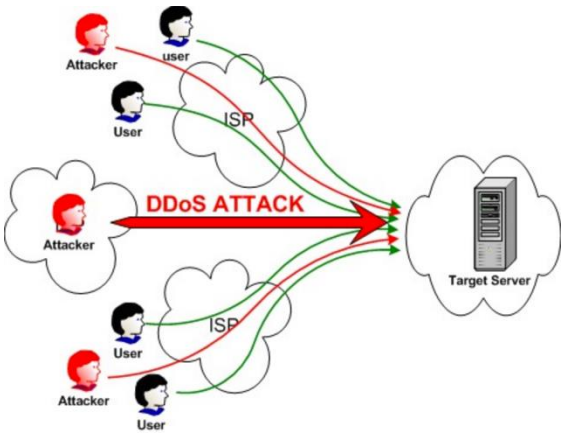


Gambar 5. *Man-In-The-Middle attack*

Pada simulasi serangan di gambar 5 dapat dilihat bahwa penyerang (*attacker*) mencoba untuk masuk ke saluran komunikasi data antara *client* dan *server*. Tetapi penyerang tidak berhasil menembus masuk ke saluran komunikasi data karena data rekam medis tumor otak pada sistem HIS telah dikunci oleh protokol SSL. Oleh sebab itu maka dapat disimpulkan bahwa protokol SSL berhasil menjaga keutuhan data di jaringan internet.

4.3. Ketersediaan Data

Untuk menguji ketersediaan data pada *server*, maka dilakukan pengujian dengan simulasi serangan *Denial of Service*. *Denial of Service attack* [11] adalah suatu jenis serangan yang dapat melumpuhkan sistem, karena serangan ini dilakukan secara beramai-ramai dan terorganisir dengan baik.



Gambar 6. *Denial of Service attack*

Gambar 6 menjelaskan cara kerja *Denial of Service attack*. Penyerang (*attacker*) memberi perintah kepada semua pasukannya untuk membuat permintaan ke *server*. Bila pasukan yang dikuasai oleh penyerang sangat besar, maka *web server* akan dibanjiri permintaan sehingga menjadi sangat sibuk dan tidak bisa diakses oleh *client* sebagai pengguna yang sah. Karena serangan *Denial of Service* tujuan sebenarnya adalah untuk mencegah agar *client* tidak bisa terhubung ke *server*.

Tetapi karena saluran komunikasi antara *client* dan *server* telah dilindungi oleh protokol SSL, maka *client* tetap bisa mengakses data di *server*. Karena protokol SSL dapat mendeteksi pengguna yang sah pada sistem melalui sertifikat SSL dan pertukaran kunci enkripsi yang dilakukan pada sesi koneksi. *Server* akan melakukan pemeriksaan *username* dan *password* yang diberikan *client*, jika terdaftar baru *server* akan bersedia melanjutkan sesi komunikasi dengan memberikan data yang diminta oleh *client*.

Dengan demikian maka dapat ditarik suatu kesimpulan bahwa serangan *Denial of Service* tidak mempengaruhi kinerja SSL pada sistem, sehingga data rekam medis tumor otak pada *server* HIS tetap bisa diakses oleh *client* dengan lancar

4.4. *Service Respon Time* (*SRT*) Sistem

Pengujian SRT bertujuan untuk mengetahui lamanya waktu yang diperlukan oleh *server* untuk merespon permintaan dari *client*.

Tabel 4. Pengujian SRT sistem

No.	*Request*	tanpa SSL (nilai rata-rata per second)	dengan SSL (nilai rata-rata per second)
1.	Proses *log in* sistem	0.0011	0.0015
2.	*Form* dokter	0.0004	0.0008
3.	*Form* konsultasi	0.0005	0.0017
4.	*Form* laboratorium	0.0005	0.0018
5.	*Form* obat	0.0003	0.0004
6.	*Form* pasien	0.0005	0.0024
7.	*Form* rekam medis	0.0005	0.0017
8.	*Form* tindakan	0.0004	0.0015
9.	Proses *log out* sistem	0.0006	0.0017

Pada Tabel 4 terlihat adanya perbedaan SRT antara saluran komunikasi yang menggunakan SSL dengan saluran komunikasi yang tanpa SSL. Pada saluran komunikasi yang menggunakan SSL, SRT lebih lambat. Hal ini disebabkan karena adanya penambahan *layer* SSL pada lapisan protokol komunikasi. Tetapi perbedaan ini tidak terlalu signifikan dan saluran komunikasi dengan SSL masih tetap dapat berjalan dengan baik.

Hasil pengujian dari beberapa simulasi serangan yang telah dilakukan terhadap sistem menunjukkan bahwa implementasi SSL dapat melindungi sistem dari pembobolan. Sistem menjadi lebih aman dan sulit untuk di *attack* karena SSL dirancang dengan menggabungkan algoritma RSA dan enkripsi AES berkekuatan 256 bit. Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima, dalam hal ini n = a x b. Nilai a dan b panjangnya lebih dari 100 digit. Dengan demikian hasil kali n = a x b akan berukuran lebih dari 200 digit. Usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi yang sangat lama, dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma RSA dan kecepatan komputer satu milidetik. Jadi semakin panjang ukuran kunci yang dibuat, semakin sulit untuk membobol suatu sistem.

5. KESIMPULAN

Berdasarkan hasil dari serangkaian pengujian dan analisa yang telah dilakukan dalam penelitian ini maka dapat diambil beberapa kesimpulan yaitu sebagai berikut :

1. SSL dapat mengenkripsi saluran komunikasi antara *client* dan *server* sehingga data rekam

medis tumor otak pada aplikasi HIS tidak dapat disadap oleh pihak-pihak yang tidak berkepentingan.

2. SSL mampu mengamankan data dari berbagai aspek keamanan yaitu :
   a. Kerahasiaan data
   b. Keutuhan data
   c. Ketersediaan data

DAFTAR PUSTAKA

[1] Health Information System (HIS), http://phinnetwork.org/resources/health-information-systems-his/ diakses 17 Mei 2017

[2] Liang Xiao, Bo Hu, Madalina Croitoru, Paul Lewis, Srinandan Dasmahaputra, *A Knowledgeable Security Model for Distributed Health Information Systems*, Journal Computers and Security, vol. 29, no. 3, pp. 331-349, 2010

[3] LeRouge C., Mantzana V., & Wilson E.V, *Healthcare Information Systems Research, Relevations and Visions*, European Journal of Information Systems, vol. 16, pp. 669-671, 2007

[4] Alnatheer A., Mohammed, *Secure Socket Layer (SSL) Impact on Web Server Performance*, Journal of Advances in Computer Networks, vol. 2, no. 3, pp. 211-217, 2014

[5] Data Security, https://www.technopedia.com/defenition/2646/data-security/ diakses 18 Mei 2017.

[6] Monica, Shucita Upadhyaya, *Secure Communication using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks*, Procedia Computer Science, vol. 70, pp. 808-813, 2015

[7] Rahmad Dawood, Said Fairuz Qiana, Sayed Muchail, *Kelayakan Raspberry Pi sebagai Web Server*, Jurnal Rekayasa Elektrika, vol. 11, no. 1, 2014

[8] Serial in Raspberry Pi. http://elinux.org/Rpi_Serial_Connection#Connections_and_signal_levels. Diakses 23 Mei 2017

[9] Mathur Ajay, Kr. Sharma Sudhir, Mishra Amit, *Sniffing A Major Threat to Secure Socket Layer and its Detection*, International Journal of Computer Applications, 2011

[10] Pateriya Kumar Pushpendra, Kumar S. Srijith, *Analysis on Man in the Middle Attack on SSL*, International Journal of Computer Applications, vol. 45, no. 23, 2012

[11] Gunasekhar T., Rao Thirupathi K., Saikiran P., Lakshmi P.V.S., *A Survey on Denial of Service Attacks*, International Journal of Computer Science an Information Technologies, vol. 5, no. 2, 2014

Biodata Penulis

Novi, S.Kom, Menyelesaikan pendidikan S-1 di STMIK Indonesia Jurusan Sistem Informasi dan saat ini sedang menempuh pendidikan S2 pada Fakultas Teknik Jurusan Teknik Elektro Universitas Andalas.

Zaini, Ph.D, Dosen Senior dan Peneliti di Jurusan Teknik Elektro, Universitas Andalas, Padang, Indonesia. Menyelesaikan pendidikan S-3 di University of Bradford pada tahun 2012. Ia juga menjadi pembicara yang diundang di European Conference on Braking, Lille Prancis, 2010.