

**IMPLEMENTASI KEAMANAN TRANSFER DATA PADA WEB
SERVER MENGGUNAKAN OPENSLL DI DINAS KOMUNIKASI DAN
INFORMATIKA BANGKA SELATAN**

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

ATMA LUHUR

PANGKALPINANG

2019

LEMBAR PENGESAHAN SKRIPSI

**IMPLEMENTASI KEAMANAN TRANSFER DATA PADA WEB
SERVER MENGGUNAKAN OPENSLL DI DINAS KOMUNIKASI DAN
INFORMATIKA BANGKA SELATAN**

Yang Diperiapkan dan disusun oleh

**RANGGA
1511500017**

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 04 Juli 2019

Dosen Penguji II



**Chandra Kirana, M.Kom
NIDN. 0228108501**

Dosen Pembimbing



**Dian Novianto, M.Kom
NIDN. 0209119001**

Kaprodi Teknik Informatika



**R. Burham Isnanto F., S.Si, M.Kom
NIDN. 0224048003**

Dosen Penguji I



**R. Burham Isnanto F., S.Si, M.Kom
NIDN. 0224048003**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 11 Juli 2019

KETUA STMIK ATMA LUHUR PANGKALPINANG



Dr. Husni Teja Sukmana, ST., M.Sc

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NIM : 1511500017
Nama : RANGGA
Judul Skripsi : IMPLEMENTASI KEAMANAN TRANSFER DATA
PADA *WEB SERVER* MENGGUNAKAN *OPENSSL* DI
DINAS KOMUNIKASI DAN INFORMATIKA
BANGKA SELATAN

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri, dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 20 Juni 2019



(Kangga)

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu(S1) pada Program Studi Teknik Informatika STMIK Atma Luhur.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada :

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia
2. Bapak dan ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Dr. Husni Teja Sukmana, S.T., M.Sc. selaku Ketua STMIK Atma Luhur.
5. Bapak R. Burham Isnanto Farid, S.Si., M.Kom selaku Kaprodi Teknik Informatika.
6. Bapak Dian Novianto, M.Kom selaku dosen pembimbing skripsi.
7. Toni Pratama, SE., MM selaku Sekretaris yang telah memberikan izin riset skripsi di Kominfo Bangka Selatan
8. Saudara , sahabat-sahabatku dan kawan-kawan Angkatan 2015 yang telah memberikan dukungan moral untuk terus menyelesaikan skripsi ini

Semoga Allah Swt membalas kebaikan dan selalu mencurahkan hidayah serta taufiknya , Amin.

Pangkalpinang, 20 Juni 2019

Penulis

ABSTRACT

At the beginning of its development, computer networks were only used for sending e-mail between universities for research purposes and for sharing printer usage in a company. To meet these objectives, the aspect of network security at that time did not receive important attention. Users of computer networks have to invest not little to access the Internet. The internet has had a huge influence on the dissemination of information, so that more and more people are accessing data through the internet along with developments, computer networks have been used for a long time for more complex things such as banking, trading and many others. And all of that uses Internet media. The security aspect of communication through computer networks is becoming increasingly important especially because of the many activities of exchanging confidential information through the Internet. To avoid sniffing (tapping) or other crimes, this final project is made to implement the security of data transfer on web servers using OpenSSL.

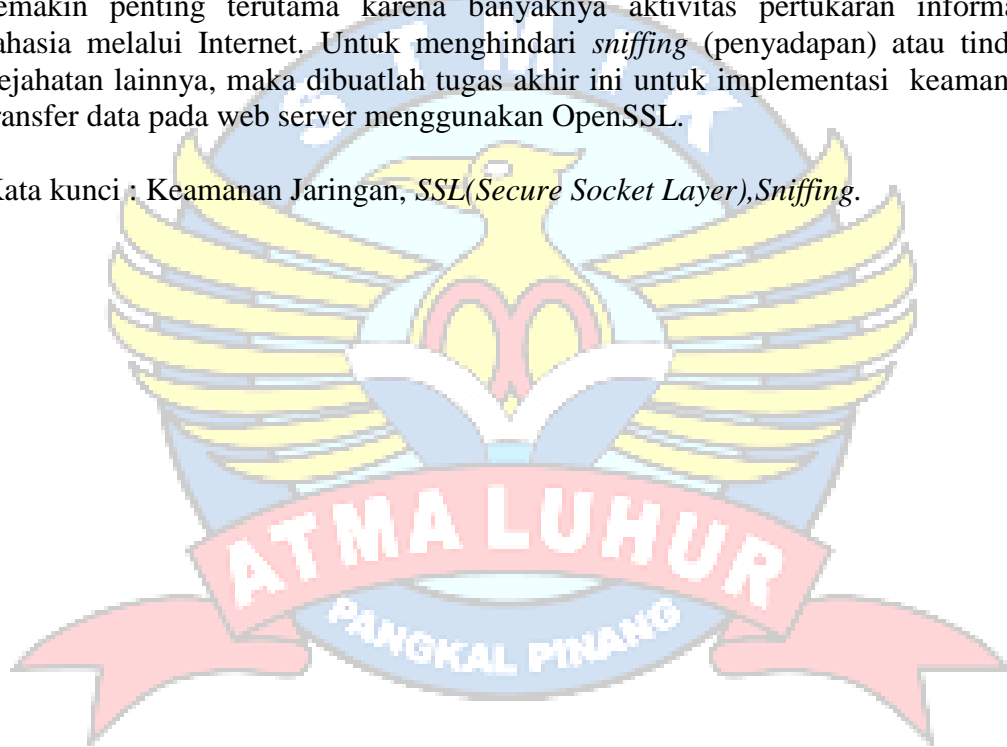
Keywords: Network Security, SSL (Secure Socket Layer), Sniffing.



ABSTRAK

Pada awal perkembangannya jaringan komputer hanya digunakan untuk pengiriman *e-mail* antar perguruan tinggi untuk keperluan riset dan untuk berbagi penggunaan *printer* dalam suatu perusahaan. Untuk memenuhi tujuan tersebut, aspek keamanan jaringan pada saat itu tidak mendapat perhatian penting. Pengguna jaringan komputer harus mengeluarkan investasi yang tidak sedikit untuk mengakses Internet. Internet telah memberikan pengaruh yang sangat besar pada penyebaran informasi, sehingga semakin banyak orang yang mengakses data melalui internet seiring dengan perkembangan, jaringan komputer telah digunakan sejak lama untuk hal-hal yang lebih kompleks seperti untuk perbankan, untuk perdagangan dan masih banyak lainnya. Dan semua itu menggunakan media Internet. Aspek keamanan dalam komunikasi melalui jaringan komputer menjadi semakin penting terutama karena banyaknya aktivitas pertukaran informasi rahasia melalui Internet. Untuk menghindari *sniffing* (penyadapan) atau tindak kejahatan lainnya, maka dibuatlah tugas akhir ini untuk implementasi keamanan transfer data pada web server menggunakan OpenSSL.

Kata kunci : Keamanan Jaringan, *SSL*(*Secure Socket Layer*),*Sniffing*.



DAFTAR ISI

| | Halaman |
|--|-------------|
| JUDUL | i |
| LEMBAR PERNYATAAN | ii |
| LEMBAR PENGESAHAN | iii |
| KATA PENGANTAR..... | iv |
| ABSTRACT | v |
| ABSTRAK | vi |
| DAFTAR ISI..... | vii |
| DAFTAR GAMBAR..... | x |
| DAFTAR TABEL | xii |
| DAFTAR SIMBOL | xiii |
| BAB I PENDAHULUAN | |
| 1.1. Latar Belakang..... | 1 |
| 1.2. Rumusan Masalah..... | 2 |
| 1.3. Batasan Masalah | 3 |
| 1.4. Tujuan dan Manfaat Penelitian..... | 3 |
| 1.5. Sistematika Penulis Laporan | 4 |
| BAB II LANDASAN TEORI | |
| 2.1. Model Pengembangan Jaringan..... | 5 |
| 2.1.1. Model PPDIOO | 5 |
| 2.1.2. Prepare | 6 |
| 2.1.3. Plan | 6 |
| 2.1.4. Design..... | 6 |
| 2.1.5. Implement | 7 |
| 2.1.6. Operate..... | 7 |
| 2.1.7. Optimize | 7 |
| 2.2. Tools Pengembangan Sistem..... | 7 |
| 2.2.1. Unified Modelling Language(UML) | 7 |
| 2.2.2. Use Case Diagram..... | 10 |

| | |
|---|----|
| 2.2.3. Activity Diagram | 11 |
| 2.2.4. Deployment Diagram | 12 |
| 2.3. Teori Pendukung..... | 12 |
| 2.3.1. Jaringan Komputer | 12 |
| 2.3.2. Internet | 13 |
| 2.3.3. Protokol Jaringan | 14 |
| 2.3.4. Hypertext Transfer Protokol(HTTP)..... | 15 |
| 2.3.5. Hypertext Transfer Protokol Secure(HTTPS)..... | 16 |
| 2.3.6. Server | 17 |
| 2.3.7. Web Server..... | 18 |
| 2.3.8. Konsep Keamanan Jaringan..... | 19 |
| 2.3.9. Acaman Keamanan Web Server | 19 |
| 2.3.10. Jenis-jenis Ancaman Web Server | 20 |
| 2.3.11. Secure Socket Layer | 22 |
| 2.3.12. Public Key Infrastructure(PKI) | 23 |
| 2.3.13. Transport Layer Security(TLS) | 25 |
| 2.3.14. Kriptografi | 26 |
| 2.3.15. Panjang Kunci Yang aman | 26 |
| 2.3.16. Algoritma RSA | 27 |
| 2.3.17. Pengguna RSA..... | 27 |
| 2.4. Penelitian Terdahulu..... | 28 |

BAB III METODOLOGI PENELITIAN

| | |
|---|----|
| 3.1. Metode Pengembangan Sistem..... | 33 |
| 3.2. Alat Bantu Pengembangan Sistem | 37 |

BAB IV PEMBAHASAN

| | |
|--------------------------------|----|
| 4.1. Sejarah Singkat | 38 |
| 4.2. Struktur Organisasi | 38 |
| 4.3. Analisis | 39 |
| 4.4. Rancangan Sistem..... | 40 |
| 4.5. Tahapan Implementasi..... | 42 |

| | |
|---|----|
| 4.6. Tahap-Tahap Pembuatan Sertifikat SSL dan Instalasi | 49 |
| 4.7. Hasil Dan Pembahasan | 52 |

BAB V PENUTUP

| | |
|----------------------|----|
| 5.1. Kesimpulan..... | 62 |
| 5.2. Saran | 62 |

| | |
|-----------------------------|-----------|
| DAFTAR PUSTAKA | 63 |
|-----------------------------|-----------|

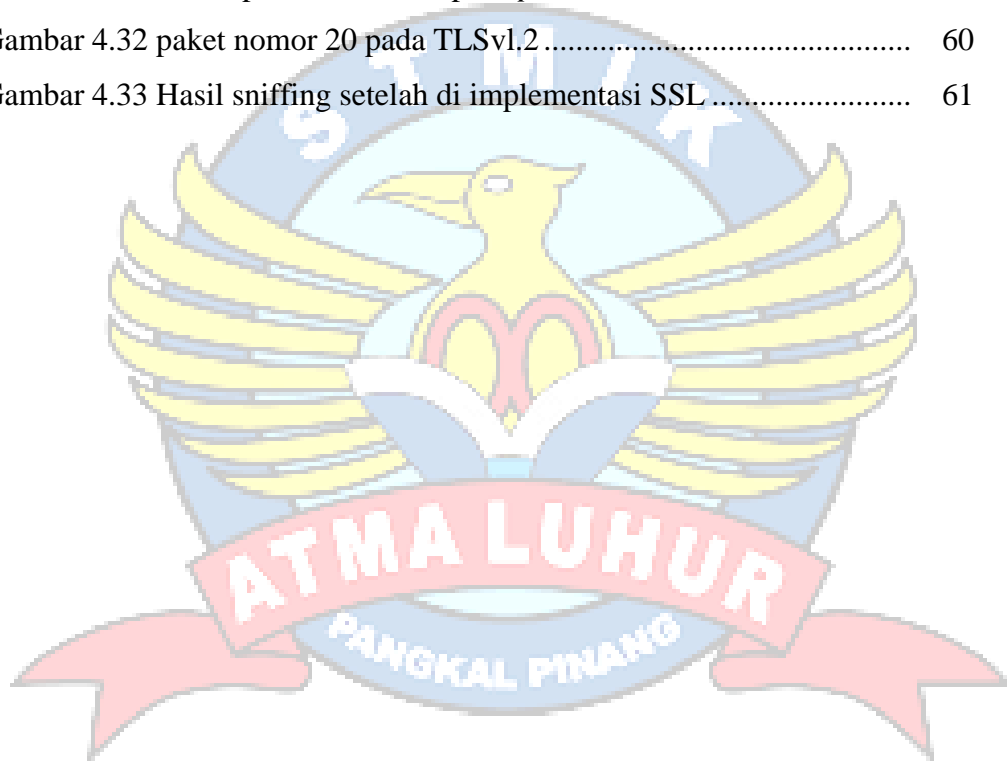
| | |
|----------------------|--------------|
| LAMPIRAN..... | |
|----------------------|--------------|



DAFTAR GAMBAR

| | Halaman |
|--|---------|
| Gambar 2.1 Metodologi PPDIOO..... | 6 |
| Gambar 2.2 Use Case Diagram..... | 11 |
| Gambar 2.3 Activity Diagram..... | 11 |
| Gambar 2.4 Deployment Diagram..... | 12 |
| Gambar 2.5 Tujuh Layer Berserta Urutannya..... | 15 |
| Gambar 2.6 Struktur Pohon Hirarki CA (<i>Certification Authority</i>)..... | 25 |
| Gambar 3.1 Metodologi PPDIOO..... | 33 |
| Gambar 4.1 Struktur Organisasi Kominfo Bangka Selatan..... | 39 |
| Gambar 4.2 Topologi Jaringan..... | 40 |
| Gambar 4.3 Use Case Diagram..... | 41 |
| Gambar 4.4 Activity Diagram..... | 41 |
| Gambar 4.5 Deployment Diagram..... | 42 |
| Gambar 4.6 Tampilan Pengaturan Address..... | 43 |
| Gambar 4.7 Tampilan Merestart Network..... | 44 |
| Gambar 4.8 Tampilan Instalasi Apache2..... | 44 |
| Gambar 4.9 Tampilan Hasil Apache2..... | 45 |
| Gambar 4.10 Tampilan Proses Instalasi Mysql..... | 45 |
| Gambar 4.11 Tampilan Proses Instalasi Php..... | 46 |
| Gambar 4.12 Tampilan Proses Instalasi Phpmyadmin..... | 46 |
| Gambar 4.13 Tampilan Db Kominfo..... | 48 |
| Gambar 4.14 Tampilan Db 192..... | 48 |
| Gambar 4.15 Tampilan Nama Domain..... | 49 |
| Gambar 4.16 Tampilan General New Key..... | 49 |
| Gambar 4.17 Tampilan Private Key..... | 50 |
| Gambar 4.18 Tampilan From untuk membuat CSR..... | 51 |
| Gambar 4.19 Tampilan CSR..... | 51 |
| Gambar 4.20 Tampilan Wireshark..... | 52 |
| Gambar 4.21 Tampilan <i>Capture Interfaces</i> | 53 |
| Gambar 4.22 Tampilan <i>website</i> belum terimplementasi SSL..... | 53 |

| | |
|--|----|
| Gambar 4.23 Tampilan gambar paket data | 54 |
| Gambar 4.24 Detail paket nomor 662 pada protocol TCP..... | 55 |
| Gambar 4.25 Detail paket nomor 662 pada <i>protocol</i> TCP..... | 55 |
| Gambar 4.26 hasil <i>sniffing</i> | 56 |
| Gambar 4.27 <i>website</i> sesudah di implementasi <i>SSL</i> | 57 |
| Gambar 4.28 paket data untuk website HTTPS | 57 |
| Gambar 4.29 Detail paket nomor 17 pada protocol TCP..... | 58 |
| Gambar 4.30 Detail paket nomor 18 pada protocol TCP..... | 59 |
| Gambar 4.31 Detail paket nomor 19 pada <i>protocol</i> TCP..... | 59 |
| Gambar 4.32 paket nomor 20 pada TLSv1.2 | 60 |
| Gambar 4.33 Hasil <i>sniffing</i> setelah di implementasi <i>SSL</i> | 61 |





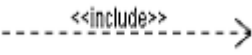

DAFTAR TABEL

| | |
|---|----|
| Tabel 2.1 Daftar Simbol Use Case Diagram..... | 8 |
| Tabel 2.2 Daftar Simbol Activity diagram..... | 9 |
| Tabel 2.3 Daftar Simbol <i>Deployment Diagram</i> | 10 |
| Tabel 3.1 Perencanaan Anggaran..... | 36 |







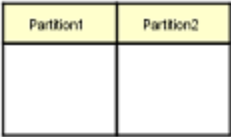

DAFTAR SIMBOL

Tabel 2.1 Daftar Simbol Use Case Diagram

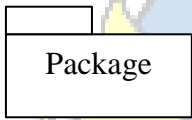
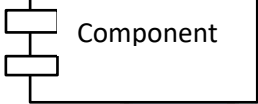

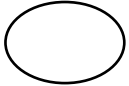

| No | Gambar | Nama | Keterangan |
|----|---|--------------------|--|
| 1 |  | <i>Actor</i> | Menunjukkan <i>user</i> yang akan menggunakan sistem baru |
| 2 |  | <i>Association</i> | Menghubungkan <i>link</i> antar <i>element</i> |
| 3 |  | <i>Include</i> | Menunjukkan bahwa suatu <i>use case</i> seluruhnya merupakan fungsionalitas dari <i>use case</i> lainnya |
| 4 |  | <i>Use case</i> | Menunjukkan proses yang terjadi pada sistem baru |

Tabel 2.2 Daftar Simbol Activity diagram

| No. | Gambar | Nama | Keterangan |
|-----|---|--------------------|--|
| 1 |  | <i>Start Point</i> | Titik awal, untk memulai suatu aktivitas |
| 2 |  | <i>End Point</i> | Titik akhir, untuk mengakhiri aktivitas |
| 3 |  | <i>Activity</i> | Menandakan sebuah aktivitas |
| 4 |  | <i>Decision</i> | Pilihan untuk mengambil keputusan |

| | | | |
|---|---|-------------------|---|
| 5 |  | <i>Swimlane</i> | Menunjukkan yang bertanggung jawab dalam melakukan aktivitas |
| 6 |  | <i>Transition</i> | Menggambarkan aliran perpindahan kontrol antara <i>activity</i> |

Tabel 2.3 Daftar Simbol *Deployment Diagram*

| No | Gambar | Nama | Keterangan |
|----|---|-------------------|---|
| 1. |  | Package | Package merupakan sebuah bungkusan dari suatu atau lebih komponen. |
| 2. |  | Komponen | Pada <i>Deployment</i> diagram komponen-komponen yang ada diletakkan didalam <i>node</i> untuk memastikan keberadaan posisi mereka. |
| 3. |  | <i>Dependency</i> | Kebergantungan antara komponen, arah pahan mengarah pada komponen yang dipakai. |
| 4. |  | <i>Interface</i> | Sebagai atarmuka komponen agar tidak mengakses langsung komponen. |
| 5. |  | <i>Link</i> | Relasi antar node. |