Jurnal CyberTech

Vol.x. No.x, September 201x, pp. xx~xx

P-ISSN : 1978-6603

E-ISSN : 2615-3475

Implementasi Digital Signature Pada Lampiran Kelengkapan Dokumen Pengeluaran Menggunakan Algoritma Rivest Shamir Adleman Di Klinik Kecantikan London Beauty Center Medan

Akbar Setiawan[*], Azanuddin[**], Trinanda Syahputra[**]

* Program Studi Mahasiswa, STMIK Triguna Dharma

** Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info

Article history:

Received Apr 05th, 2020

Revised Apr xxth, 2020

Accepted Apr xxth, 2020

Keyword:

Digital Signature

Lampiran Kelengkapan Dokumen Pengeluaran

Rivest Shamir Adleman

ABSTRACT

Perkembangan teknologi saat ini di bidang komunikasi sangat pesat di Indonesia, membuat semua orang dapat terhubung satu dengan yang lainnya, baik itu dalam bentuk data, text, suara, video dan multimedia lainnya. Lampiran kelengkapan dokumen pengeluaran merupakan suatu dokumen yang penting bagi London beauty center. Karena di dalamnya berisikan informasi mengenai nota penjualan, nota tindakan dokter, laporan tindakan dokter dan lain-lain. Yang setiap bulannya dikirim dari setiap cabang ke pusat. Hal inilah yang kemudian sering memunculkan manipualsi terhadap lampiran kelengkapan dokumen pengeluaran tersebut, baik secara data maupun pencetakannya. Dengan adanya pemalsuan tersebut untuk meningkatkan pengamanan, menghindari pemalsuan dokumen dan menjaga keaslian lampiran kelengkapan dokumen pengeluaran, akan dibuat suatu mekanisme pengaman pada lampiran kelengkapan dokumen pengeluaran dengan menyertakan digital signature didalamnya untuk menjaga keutuhan dan otentikasi dari lampiran kelengkapan dokumen pengeluaran tersebut. Digital signature dapat berfungsi untuk menguji keutuhan dan otentikasi suatu dokumen digital, serta dapat mendeteksi perubahan dokumen dari hasil manipulasi. Salah satu cara untuk melakukan digital signature pada dokumen yaitu dengan menggunakan fungsi enkripsi algoritma RSA, dari fungsi enkripsi algoritma RSA tersebut nantinya akan menghasilkan digital signature.

Corresponding Author: *First Author

Nama : Akbar Setiawan
Program Studi : Sistem Informasi
Kampus : STMIK Triguna Dharma
Email : akbarsetiawan.id@gmail.com

1. PENDAHULUAN

Perkembangan teknologi saat ini di bidang komunikasi sangat pesat di Indonesia, membuat semua orang dapat terhubung satu dengan yang lainnya, baik itu dalam bentuk *data*, *text*, suara, *video* dan multimedia lainnya. Dengan perkembangan yang pesat ini memicu terjadinya tindakan kejahatan dari orang yang memiliki kepentingan lain untuk mencuri atau menduplikat informasi dokumen penting suatu perusahaan [1].

Lampiran kelengkapan dokumen pengeluaran merupakan suatu dokumen yang penting bagi *London beauty center*. Karena di dalamnya berisikan informasi mengenai nota penjualan, nota tindakan dokter, laporan tindakan dokter dan lain-lain. Yang setiap bulannya dikirim dari setiap cabang ke pusat. Hal inilah yang kemudian sering memunculkan manipualsi terhadap lampiran kelengkapan dokumen pengeluaran tersebut, baik secara data maupun pencetakannya.

Dengan adanya pemalsuan tersebut untuk meningkatkan pengamanan, menghindari pemalsuan dokumen dan menjaga keaslian lampiran kelengkapan dokumen pengeluaran, akan dibuat suatu mekanisme pengaman pada lampiran kelengkapan dokumen pengeluaran dengan menyertakan *digital signature* didalamnya untuk menjaga keutuhan dan otentikasi dari lampiran kelengkapan dokumen pengeluaran tersebut. *Digital signature* dapat berfungsi untuk menguji keutuhan dan otentikasi suatu dokumen digital, serta dapat mendeteksi perubahan dokumen dari hasil manipulasi. Salah satu cara untuk melakukan *digital signature* pada dokumen yaitu dengan menggunakan fungsi enkripsi algoritma RSA, dari fungsi enkripsi algoritma RSA tersebut nantinya akan menghasilkan *digital signature.*

2. KAJIAN PUSTAKA

2.1 Lampiran Kelengkapan Dokumen Pengeluaran

Dokumen merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain. Dokumen meliputi berbagai kegiatan yang diawali dengan bagaimana suatu dokumen dibuat, dikendalikan, diproduksi, disimpan, didistribusikan, dan digandakan. Dokumen yang ada di *London beauty center* Medan terdiri dari arus pendapatan harian, laporan tindakan dokter, nota persetujuan tindakan dokter, nota klinik sekaligus apotek dan potongan *credit card*. Dokumen ini setiap bulannya dikirim ke *London beauty center* pusat yang berada di kota Yogyakarta yang bertujuan untuk memvalidasi dokumen atas pengeluaran dan pemasukan setiap harinya maupun bulannya yang ada di setiap cabang *London beauty center*.

2.2 Kriptografi

Salah satu sarana komunikasi manusia adalah tulisan dan suara. Tulisan atau suara bertujuan untuk menyampaikan suatu pesan kepada pembaca atau penerima. Pesan itu sendiri adalah suatu informasi atau kabar yang dapat dibaca atau dimengerti isi dan maknanya. Sebelum ditemukan suatu media untuk mengolah atau mendokumentasikan suatu pesan atau informasi, pengiriman pesan atau informasi dari suatu tempat ke tempat yang lain sudah ada terjadi. Dengan cara berkembangnya mengirim suatu pesan atau informasi, berkembang pula cara menyembunyikan pesan atau informasi dan bagaimana orang lain tidak mengetahui isi pesan atau informasi walaupun pesan atau infomasi tersebut ditemukan. Disinilah lahir suatu ilmu baru di sebut kriptografi [2].

2.3 *Digital Signature*

Salah satu konsep pada kriptografi modern adalah digital signature. Cara kerja dan kegunaan digital signature mirip dengan tanda tangan dalam versi nyata, yaitu untuk memberikan kepastian keaslian dan persetujuan dokumen oleh penanda tangan. Dalam digital signature, tanda tangan adalah dalam bentuk digital yang digunakan untuk mensahkan sebuah dokumen digital. Prinsip yang digunakan dalam tanda tangan digital ini adalah dokumen yang dikirimkan harus ditandatangani oleh pengirim dan tanda tangan bisa diperiksa oleh penerima untuk memastikan keaslian dokumen yang dikirimkan. Fungsinya adalah untuk melakukan verifikasi terhadap data yang dikirim [3].

2.4 Algoritma RSA

Rivest, Shamir dan Adleman atau disingkat RSA adalah sebuah *public key cipher* yang dibuat oleh tiga orang peneliti dari MIT (*Massachusetts Institute of Technology*) pada tahun 1978. Peneliti tersebut antara lain Ron Rivest, Adi Shamir dan Leonard Adleman. *Cipher* ini memiliki 2 kunci, yaitu kunci publik dan kunci *private* atau rahasia. Keamanan *cipher* RSA ini terletak pada sulitnya menfaktorkan bilangan yang besar menjadi faktor-faktor prima [4].

2.4.1 Membangkitkan Kunci RSA

Untuk menggunakan RSA terlebih dahulu pendeskripsi membangkitkan sepasang kunci yaitu kunci *public* dan kunci *private*. Hal pertama yang dilakukan algoritma pembangkit kunci adalah membangkitkan 2 bilangan prima besar. Pembangkitan bilangan prima besar menggunakan algoritma pengujian bilangan prima misalnya algoritma Miller-Rabin. Agar sistem kriptografi RSA aman diperlukan bilangan prima yang besar sehingga $n = p \times q$ sangat sulit untuk difaktorisasi. Untuk p dan q bilangan prima bersifat rahasia, $n = p, q$ tidak bersifat rahasia, $\varphi(n) = (p - 1)(q - 1)$ bersifat rahasia, e (kunci enkripsi) bersifat tidak rahasia, d (kunci dekripsi) bersifat rahasia, m (*plaintext*) bersifat rahasia, dan c *(chipertext)* bersifat tidak rahasia. Algoritma membangkitkan kunci RSA sebagai berikut:

1. Menentukan dua bilangan prima, dengan nama:
   p dan q
2. Menghitung nilai modulus (n):
   $n = p \times q$
3. Menghitung nilai *totient* (φ) n:
   $\varphi(n) = (p-1) \times (q-1)$
4. Menentukan nilai e dengan syarat (*greater common divisor) gcd* (e, $\varphi(n)$) = 1
   Dimana e = bilangan prima, dan $1 < e < \varphi(n)$.
5. Mencari nilai *deciphering exponent* (d), maka:
   $d = (1 + (k \times \varphi(n)) / e)$
   Nilai k merupakan sembarang angka untuk pencarian hingga dihasilkan suatu nilai *integer* atau bulat. Dengan mencoba nilai k = 1,2,3 dan seterusnya hingga diperoleh nilai d yang bulat.
6. Dari langkah-langkah yang sudah diuraikan sebelumnya, maka nilai n, e, dan d telah didapatkan sehingga pasangan kunci telah terbentuk.

2.4.2 Proses Enkripsi

Enkripsi adalah proses mengamankan *data* atau informasi, dengan kata lain mengacak *data* atau informasi agar tidak dapat dibaca oleh pihak lain. Enkripsi dapat dilakukan dengan rumus $C = M^e \bmod n$ [5].

2.4.3 Proses Dekripsi

Dekripsi merupakan kebalikan dari enkripsi yaitu cara mengkonversi dokumen atau *data* yang setelah di enkripsi kembali menjadi *data* aslinya sehingga dapat dipahami atau dimengerti kembali maknanya. Dekripsi dapat dilakukan dengan rumus $M = C^d \bmod n$.

3. METODOLOGI PENELITIAN

3.1 Pengumpulan *Data* (*Data Collecting*)

Di dalam teknik pengumpulan *data* dilakukan dengan dua tahapan yaitu sebagai berikut:

1. Observasi

Kegiatan observasi dalam penelitian ini dilakukan dengan tinjauan langsung ke klinik kecantikan *London beauty center* Medan. Di klinik tersebut dilakukan analisis masalah serta kebutuhan yang diperlukan dengan cara mengamati langsung prosedur pembuatan lampiran kelengkapan dokumen pengeluaran, yang dilakukan oleh pegawai yang ada di klinik tersebut.

2. Wawancara

Teknik pengumpulan *data* yang selanjutnya dilakukan adalah wawancara. Wawancara merupakan kegiatan tanya jawab yang dilakukan dengan narasumber.

3.2 Deskripsi Data Dari Penelitian


PEMERINTAH KOTA MEDAN
DINAS KEBERSIHAN DAN PERTAMANAN
JL. PINANG BARIS NO. 114 TELP. (061) 8452022 - MEDAN 20127
TANDA BUKTI PEMBAYARAN RETRIBUSI PELAYANAN KEBERSIHAN
Perda No. 10 Tahun 2012
NO. PELANGGAN : 107010001009
NAMA :
ALAMAT : Jl. H. Zainul Arifin
LINGKUNGAN :
KELURAHAN : SUKA DAMAI
KECAMATAN : MEDAN POLONIA
WILAYAH : I SERI : AA 017686
TARIF DASAR : 49.500
TARIF KHUSUS : 0
JUMLAH : 49.500
Terbilang EMPAT PULUH SEMBILAN RIBU LIMA RATUS RUPIAH
UNTUK PEMBAYARAN
KODE FILE :
BLN / THN : Juni 2019
GOLONGAN :
KEPALA DINAS KEBERSIHAN DAN PERTAMANAN KOTA MEDAN
Ir. MUHAMMAD HUSNI, SE, M.SI
PEMBINA TK. I
NIP. 19680705 199503 1 002
TANDA BUKTI PEMBAYARAN RETRIBUSI YANG SAH ADALAH YANG DITERBITKAN DINAS KEBERSIHAN DAN PERTAMANAN KOTA MEDAN

Gambar 3.1 Contoh Data Retribusi Kebersihan

3.3 Membangkitkan Kunci Algoritma RSA

1. Membangkitkan kunci algoritma RSA dengan menentukan dua bilangan prima *p* dan *q*:
   p = 13
   q = 31
2. Menghitung nilai modulus (*n*):
   n = *p x q*
   n = 13 *x* 31
   n = 403

3. Menghitung nilai *totient* (φ) *n*:
   φ (*n*) = (*p* - 1) *x* (*q* - 1)
   φ (*n*) = (13 - 1) *x* (31 - 1)
   φ (*n*) = 12 *x* 30
   φ (*n*) = 360
4. Menentukan nilai *e*, dimana *e* bilangan prima dengan syarat *gcd*:
   gcd (*e*, φ (*n*)) = 1
   gcd (7, 360) = 1
   e = 7
5. Mencari nilai *deciphering exponent* (*d)* dimana *(d)* bilangan bulat:
   d = (1 + (*k x φ* (*n*)) / *e*)
   d = (1 + (*2 x* 360) / 7)
   d = 721 / 7
   d = 103
6. Dalam lampiran kelengkapan dokumen ini yang dijadikan *plaintext* dalam enkripsi ini adalah tanggal, nomor surat dan jumlah lampiran.

3.4 Proses Enkripsi

Tabel 3.1 *Plaintext* dan Kode Desimal ASCII

Plaintext	**Kode Desimal ASCII**
0	48
5	53
-	45
1	49
2	50
-	45
2	50
0	48
1	49
9	57
A	65
.	46
1	49
2	50
/	47
L	76
B	66
C	67
-	45
M	77
E	69
D	68
A	65
N	78
/	47
X	88
I	73
I	73
/	47
2	50
0	48
1	49
9	57
8	56

Setelah *plaintext* diubah ke kode ASCII desimal selanjutnya proses enkripsi dengan rumus $C = M^e \ mod \ n$ yaitu sebagai berikut:

$C_1 = M^e \bmod n$
$= 48^7 \bmod 403$
$= 74$

$C_2 = M^e \bmod n$
$= 53^7 \bmod 403$
$= 300$

$C_3 = M^e \bmod n$
$= 45^7 \bmod 403$
$= 267$

$C_4 = M^e \bmod n$
$= 49^7 \bmod 403$
$= 257$

$C_5 = M^e \bmod n$
$= 50^7 \bmod 403$
$= 379$

$C_6 = M^e \bmod n$
$= 45^7 \bmod 403$
$= 267$

$C_7 = M^e \bmod n$
$= 50^7 \bmod 403$
$= 379$

$C_8 = M^e \bmod n$
$= 48^7 \bmod 403$
$= 74$

$C_9 = M^e \bmod n$
$= 49^7 \bmod 403$
$= 257$

$C_{10} = M^e \bmod n$
$= 57^7 \bmod 403$
$= 398$

$C_{11} = M^e \bmod n$
$= 65^7 \bmod 403$
$= 234$

$C_{12} = M^e \bmod n$
$= 46^7 \bmod 403$
$= 240$

$C_{13} = M^e \bmod n$
$= 49^7 \bmod 403$
$= 257$

$C_{14} = M^e \bmod n$
$= 50^7 \bmod 403$
$= 379$

$C_{15} = M^e \bmod n$
$= 47^7 \bmod 403$
$= 70$

$C_{16} = M^e \bmod n$
$= 76^7 \bmod 403$
$= 236$

$C_{17} = M^e \bmod n$
$= 66^7 \bmod 403$
$= 326$

$C_{18} = M^e \bmod n$
$= 67^7 \bmod 403$
$= 284$

$C_{19} = M^e \bmod n$
$= 45^7 \bmod 403$
$= 267$

$C_{20} = M^e \bmod n$
$= 77^7 \bmod 403$
$= 116$

$C_{21} = M^e \bmod n$
$= 69^7 \bmod 403$
$= 121$

$C_{22} = M^e \bmod n$
$= 68^7 \bmod 403$
$= 68$

$C_{23} = M^e \bmod n$
$= 65^7 \bmod 403$
$= 234$

$C_{24} = M^e \bmod n$
$= 78^7 \bmod 403$
$= 39$

$C_{25} = M^e \bmod n$
$= 47^7 \bmod 403$
$= 70$

$C_{26} = M^e \bmod n$
$= 88^7 \bmod 403$
$= 88$

$C_{27} = M^e \bmod n$
$= 73^7 \bmod 403$
$= 44$

$C_{28} = M^e \bmod n$
$= 73^7 \bmod 403$
$= 44$

$C_{29} = M^e \bmod n$
$= 88^7 \bmod 403$
$= 70$

$C_{30} = M^e \bmod n$

$= 50^7 \ mod \ 403$
$= 379$

$C_{31} = M^e \ mod \ n$
$= 48^7 \ mod \ 403$
$= 74$

$C_{32} = M^e \ mod \ n$
$= 49^7 \ mod \ 403$
$= 257$

$C_{33} = M^e \ mod \ n$
$= 57^7 \ mod \ 403$
$= 398$

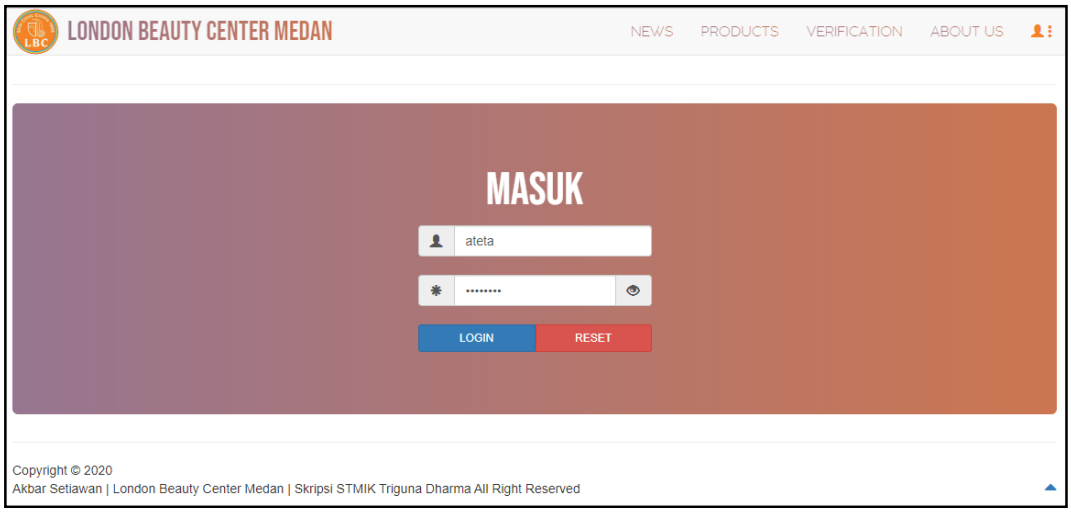
$C_{34} = M^e \ mod \ n$
$= 56^7 \ mod \ 403$
$= 56$

Tabel 3.2 Hasil Enkripsi

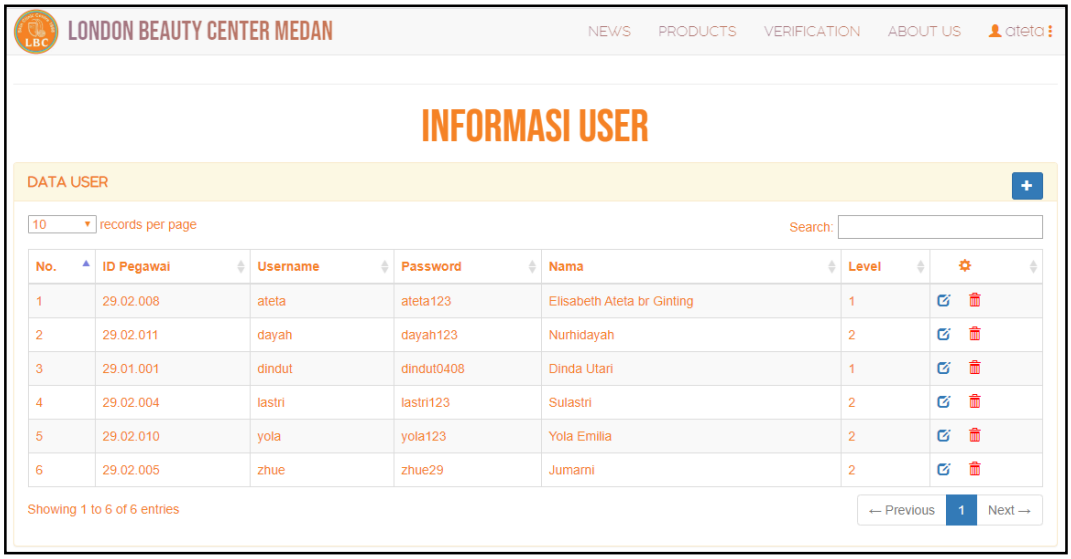
Plaintext	**Kode Desimal ASCII**	***Ciphertext***	**Kode *Hexadecimal* ASCII**
0	48	74	4A
5	53	300	12C
-	45	267	10B
1	49	257	101
2	50	379	17B
-	45	267	10B
2	50	379	17B
0	48	74	4A
1	49	257	101
9	57	398	18E
A	65	234	EA
.	46	240	F0
1	49	257	101
2	50	379	17B
/	47	70	46
L	76	236	EC
B	66	326	146
C	67	248	F8
-	45	267	10B
M	77	116	74
E	69	121	79
D	68	68	44
A	65	234	EA
N	78	39	27
/	47	70	46
X	88	88	58
I	73	44	2C
I	73	44	2C
/	47	70	46
2	50	379	17B
0	48	74	4A
1	49	257	101
9	57	398	18E
8	56	56	38

4. IMPLEMENTASI

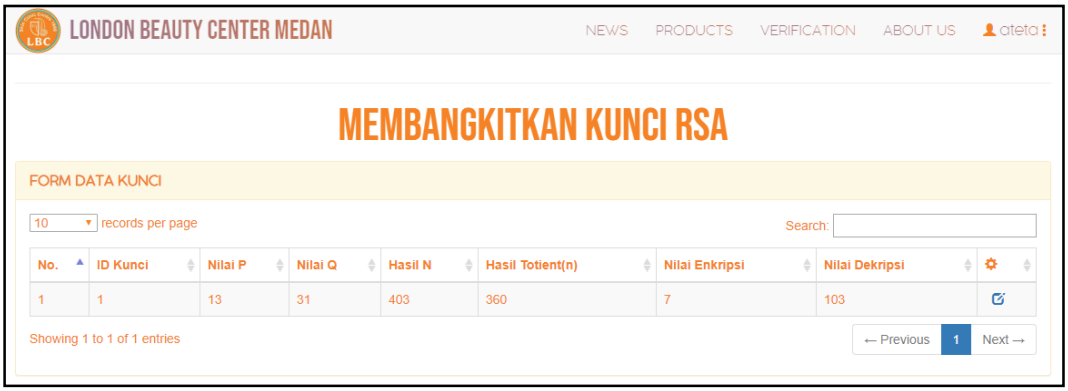
Berikut ini merupakan langkah yang digunakan untuk mengoperasikan sistem yang akan dibangun.



Gambar 4.1 Halaman *Login*

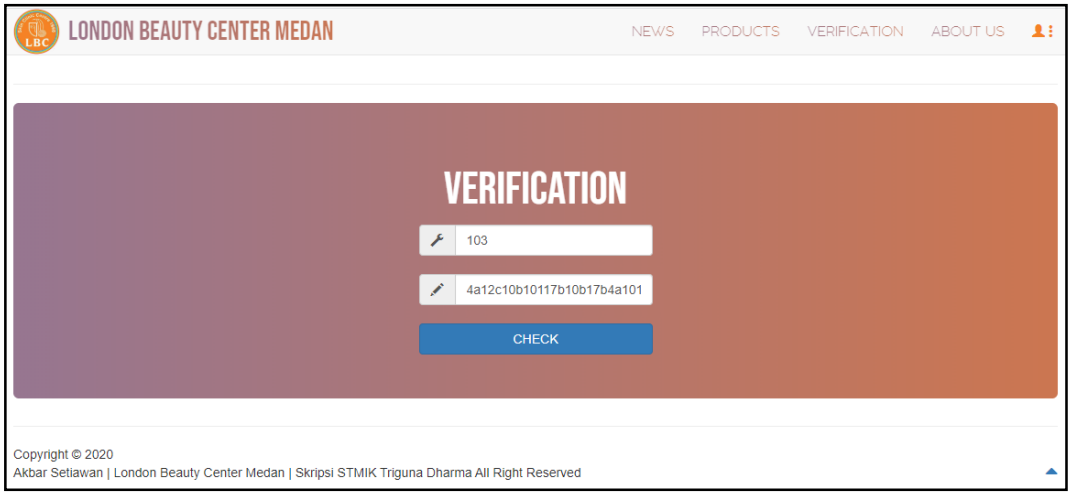


Gambar 4.2 Halaman *User*

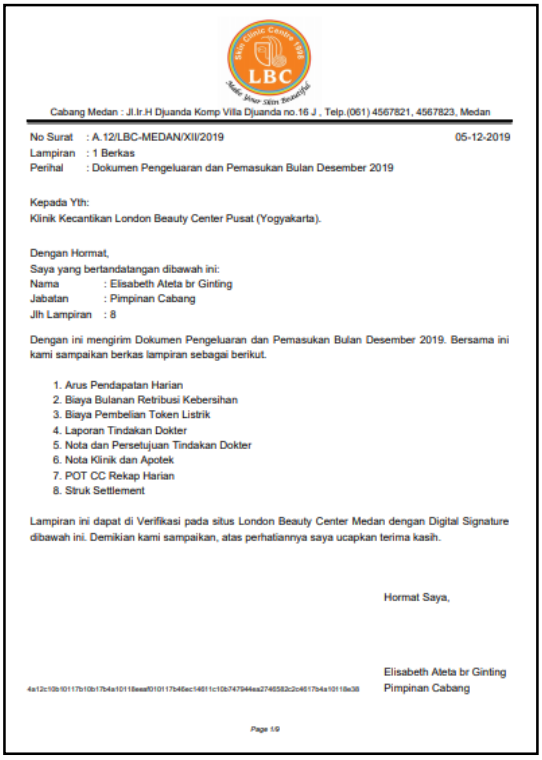


Gambar 4.3 Halaman Kunci

Gambar 4.4 Halaman *Upload* Dokumen



Gambar 4.5 Halaman Verifikasi



Cabang Medan : Jl.Ir.H Djuanda Komp Villa Djuanda no.16 J , Telp.(061) 4567821, 4567823, Medan

No Surat : A.12/LBC-MEDAN/XII/2019 05-12-2019
Lampiran : 1 Berkas
Perihal : Dokumen Pengeluaran dan Pemasukan Bulan Desember 2019

Kepada Yth:
Klinik Kecantikan London Beauty Center Pusat (Yogyakarta).

Dengan Hormat,
Saya yang bertandatangan dibawah ini:
Nama : Elisabeth Aleta br Ginting
Jabatan : Pimpinan Cabang
Jlh Lampiran : 8

Dengan ini mengirim Dokumen Pengeluaran dan Pemasukan Bulan Desember 2019. Bersama ini kami sampaikan berkas lampiran sebagai berikut.

1. Arus Pendapatan Harian
2. Biaya Bulanan Retribusi Kebersihan
3. Biaya Pembelian Token Listrik
4. Laporan Tindakan Dokter
5. Nota dan Persetujuan Tindakan Dokter
6. Nota Klinik dan Apotek
7. POT CC Rekap Harian
8. Struk Settlement

Lampiran ini dapat di Verifikasi pada situs London Beauty Center Medan dengan Digital Signature dibawah ini. Demikian kami sampaikan, atas perhatiannya saya ucapkan terima kasih.

Hormat Saya,

Elisabeth Aleta br Ginting
Pimpinan Cabang

4a12c10b10117b10b17b4a10118eeaf010117b46ec14811c10b747944ea2746582c2c46174a10118e38

Page 1/9

Gambar 4.6 Lampiran Kelengkapan Dokumen Pengeluaran

5. KESIMPULAN

Berdasarakan perumusan dan pembahasan bab-bab sebelumnya dapat diambil beberapa kesimpulan dan beberapa saran.

1. Dalam mengatasi masalah yang terjadi di klinik kecantikan *London beauty center* Medan terkait memverifikasi keaslian lampiran kelengkapan dokumen pengeluaran maka dengan begitu pentingya lampiran kelengkapan dokumen pengeluaran ini harus dijaga keasliannya dengan menggunakan algoritma Rivest Shamir Adleman.
2. Algoritma yang digunakan dapat di kombinasikan dengan algoritma yang memiliki fungsi *hash* seperti MD5 (*Message Digest*).

UCAPAN TERIMA KASIH

Pada kesempatan ini penulis mengucapkan banyak terimakasih kepada Kedua Orang Tua yang telah banyak memberikan dukungan moril dan materil, tidak terkecuali doa yang senantiasa dipanjatkan sehingga penulis dapat menyelesaikan penelitian ini.

Penyusunan skripsi ini juga tidak terlepas dari bantuan berbagai pihak. Oleh karena itu dengan segala kerendahan hati, diucapkan terimakasih yang sebesar-besarnya kepada; Bapak Azanuddin, S.Kom., M.Kom selaku Dosen Pembimbing I dan kepada Bapak Trinanda Syahputra, S.Kom., M.Kom selaku Dosen Pembimbing II yang telah banyak membantu dalam memberikan arahan dan bimbingan.

REFERENSI

[1] A. K. Muchsin, "Makalah Computer Security," 2015.

[2] R. Kurniawan, "Rancang Bangun Aplikasi Pengaman Isi File Dokumen Dengan Algoritma Rsa," Vol. 6341, No. November, Pp. 46–52, 2017.

[3] E. C. Prabowo And I. Afrianto, "Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital," Vol. 6, No. 2, 2017.

[4] J. B. Sanger, "Desain Dan Implementasi Mekanisme Tanda Tangan Dijital Dalam Pertukaran Data Dengan Hash Md5 Dan Enkripsi / Dekripsi Menggunakan Algoritma Rsa," Vol. 12, No. 2, 2015.

BIBLIOGRAFI PENULIS

	**Akbar Setiawan**, Pria kelahiran Medan, 20 Mei 1997, anak keempat dari empat bersaudara ini merupakan seorang mahasiswa STMIK Triguna Dharma yang sedang dalam proses menyelesaikan skripsi.
	**Azanuddin, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.
	**Trinanda Syahputra, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.