Sains dan Komputer (SAINTIKOM)
Vol., No., Maret 2020, pp.
ISSN: ❒

E- *Security* di dalam *Digital Signature* Berbasis Algoritma AES (*Advanced Encryption Standard*) 128 *Bit* pada Slip Gaji Pegawai di Kantor Walikota Medan

Ainun Haviza Nasution **,Jaka Prayudha,S,kom., M.Kom Ardianto Prananta,S,kom., M.Kom.**
[*]Program Studi Sistem Informasi, STMIK Triguna Dharma
[**]Program Studi Sistem Informasi Dosen Pembimbing, STMIK Triguna Dharma

Article Info
Article history:
-

Keyword:
Slip Gaji, Kriptografi, Advanced Encryption Standard 128 bit, Digital Signature.

ABSTRACT (10 pt)
Gaji adalah kompensasi yang diberikan oleh perusahaan kepada pegawainya sebagai balas jasa atas kontribusiyang diberikan pegawai kepada pegawai. Slip gaji merupakan catatan ringkas yang terdapat hak yang semestinya diterima oleh pegawai dalam jangka waktu tertentu yang diserahkan bukan hanya sebagai bukti formalitas dan catatan total gaji yang diberikan. Slip gaji dapat berfungsi untuk pinjaman ataupun pengajuan kartu kredit atas dasar permohonan pegawai. Slip gaji sering sekali dipalsukan dan disalahgunakan. Kantor walikota medan merupakan instansi pemerintahan yang harus memiliki sistem penggajian yang aman, salah satunya pada slip gaji agar terhindar dari ancaman modifikasi, interupsi, dan gangguan dari pihak yang tidak bersangkutan terhadap data pegawai.
Dengan ini diperlukan sebuah sistem yang bisa menambahkan keamanan pada slip gaji. Kemanan ini dilakukan dengan cara menambahkan sebuah algoritma kriptografi yaitu algoritma Advanced Encryption Standard 128 bit untuk mengenkripsi dan hasil enkripsi dijadikan Digital Signature untuk ditambahkan kedalam slip gaji.
Hasil pengujian menunjukkan bahwa sistem bisa menambah keamanan pada slip gaji dengan sangat baik dan menghindari terjadinya penyalahgunaan atau manipulasi oleh pihak yang tidak bersangkutan

First Author:
Nama : Ainun Haviza Nasution
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : havizanasution99@gmail.com

1. PENDAHULUAN

Keamanan (*Security*) adalah hal yang sangat penting dalam perkembangan teknologi informasi terutama dalam perkembangan industri 4.0. Dengan perkembangannya yang sangat pesat ancaman kepada keamanan computer dan data juga semakin besar. Karena hal itu hampir seluruh perusahaan besar di dunia mengandalkan *cyber security* untuk mengamankan data–data penting perusahaan mereka dari *cyber attack*[1], contohnya berupa ancaman modifikasi, interupsi, dan gangguan dari pihak yang tidak bersangkutan. Keamanan data juga sangatlah diperlukan di instansi pemerintahan seperti di kantor walikota Medan. Sebab data dan dokumen yang ada dipemerintahan merupakan data yang sangat penting dan memerlukan keamanan yang optimal agar tidak di salah gunakan oleh pihak yang tidak berkepentingan maupun pegawai instansi tersebut.

Slip gaji merupakan bukti faktual bahwa pegawai tersebut menerima gaji dari suatu instansi tempat dia bekerja[2]. Slip gaji berfungsi sebagai bukti resmi jika instansi tersebut telah melaksanakan kewajibannya memberikan gaji kepada pegawainya. Sedangkan bagi pegawai slip gaji sering digunakan untuk pinjaman atau kreditas dasar permohonan pegawai sebagai bukti sah. Namun slip gaji pegawai sering sekali disalah gunakan dan dipalsukan oleh orang yang tidak bertanggung jawab ataupun oleh pegawai itu sendiri. Pemalsuan dokumen sangatlah mudah dilakukan, hanya dengan memanipulasi isi dokumen dengan membuat yang baru dengan tampilan yang sama dengan yang asli, maka dokumen palsu sudah bisa digunakan.

Digital signature merupakan metode otentikasi yang memungkinkan pembuat pesan bias menyertakan sebuah kode yang berperan sebagai tandatangan[3]. Digital signature merupakan suatu cara yang dapat diterapkan untuk menjadikan dokumen tersebut legal secara hukum dengan menggantikan tandatangan manual pada kertas. Digital signature digunakan untuk melakukan validasi atau melihat keaslian suatu dokumen dan dari mana dokumen

tersebut berasal, dengan ditambahkannya digital signature pada slip gaji diharapkan dapat menyelesaikan masalah otentikasi dan anti penyangkalan. Digital signature dapat dilakukan dengan dua cara yaitu dengan mengenkripsi pesan atau dengan menggunakan fungsi hash.

AES merupakan algoritma yang menggunakan kunci simetris dimana proses enkripsi dan dekripsi pesan menggunakan kunci yang sama, dan termasuk dalam block cipher yang beroperasi dengan membagi plaintext dalam blok – blok bit[4]. Algoitma AES menggunakan kunci kriptografi 128, 192, dan 256 bits, yang mana panjang kunci akan menentukan jumlah putaran total kunci. AES – 128 bit menggunakan panjang kunci Nk = 4 word (kata) dimana setiap kata terdiri dari 32 bit sehingga menghasilkan total kunci 128 bit, ukuran blok teks asli 128 bit dan memiliki 10 putaran. Algoritma AES juga telah dirancang untuk memiliki ketahanan terhadap berbagai macam serangan.

2. KAJIAN PUSTAKA

2.1 Gaji

Gaji adalah kompensasi yang diberikan oleh perusahaan kepada pegawainya sebagai balas jasa atas kontribusi yang diberikan pegawai kepada perusahaan. Karena keuntungan yang didapat perusahaan tidak lepas dari bantuan pegawai perusahaan tersebut[2].

Slip gaji merupakan catatan ringkas yang terdapat hak yang semestinya diterima oleh pegawai dalam jangka waktu tertentu. Instansi pemerintahan ataupun perusahaan yang menjadi tempat bekerja harus mengeluarkan bukti gaji dan pengangkatan bahwa telah diberikannya gaji kepada pegawai. Slip gaji diserahkan bukan hanya sebagai bukti formalitas dan catatan total gaji yang diberikan[5]. Slip gaji terdapat beberapa bagian didalamnya antara lain yaitu :

a) Nama Perusahaan
b) KerahasiaanGaji
c) Tanggal Pembayaran, Sub Departemen dan Sub Bagian dan Data Karyawan.
d) Jumlah Penghasilan dan Potongan

2.2 Kriptografi

Kriptografi berasal dari bahasa yunani, kryptos dan graphein. Kryptos berarti secret (tersembunyi, rahasia) dan graphein berarti writing (tulisan). Menurut istilah, kriptografi merupakan ilmu dan seni untuk membentengi keamanan pada pesan saat pesan dikirimkan dari suatu tempat ke tempat lainnya Kriptografi dapat didefinisikan sebagai ilmu seni yang menjaga kerahasiaan pesan dengan cara menyandikan kedalam bentuk yang tidak bisa dimengerti (Random)[6]. Kriptografi bisa juga didefinisikan sebagai ilmu yang mempelajari bagaimana cara melindungi data atau informasi agar terjaga keamanannya, tanpa terjadinya gangguan dari pihak lain yang tidak berkepentingan.

2.3 *Advanced Enryption Standart* (AES)

AES merupakan sistem penyandian blok yang bersifat non fiestel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES dapat memiliki panjang kunci bit 128, 192, dan 256 bit. AES termasuk kedalam kriptografi simetris, karena menggunakan kunci yang sama untuk kedua proses enkripsi dan dekripsi. Simetris sendiri jauh lebih efektif dan lebih cepat dari pada asimetris. AES juga termasuk dalam jenis kriptografi yang sifatnya block cipher. Dengan demikian algoritma ini mendapatkan keluaran berupa blok dengan jumlah bit tertentu.

AES-128 bit menggunakan panjang kunci Nk = 4 word (kata) yang mana setiap kata terdiri dari 32 bit sehingga menghasilkan total kunci 128 bit, ukuran blok teks asli 128 bit dan memiliki 10 putaran. Untuk putaran kunci terdiri dari Ki = 4 kata dan total putaran kunci 128 bit dan memiliki ukuran kunci yang diperluas 44 kata dan 176 byte. Dalam beberapa kasus, blok ini juga dianggap sebagai *array* satu dimensi dari vektor 4-*byte*, di mana setiap vektor terdiri dari kolom yang sesuai dalam representasi *array* dua dimensi. Array ini memiliki panjang masing-masing 4, 6, atau 8, dan indeks dalam rentang 0..3, 0..5, atau 0..7. Vektor 4-*byte* ini disebut dengan *word.* 128 bit blok data dikelompokkan menjadi 16 byte dan dipetakan dalam sebuah array berukuran 4 X 4 disebut sebagai state. Semua operasi internal dilakukan di salam state[7].

Tabel 2.1 parameter AES

	AES 128	**AES 192**	**AES 256**
Key size	4 word (16 byte)	6 word (24 byte)	8 word (16 byte)
Plaintext box size	4 word (16 byte)	4 word (16 byte)	4 word (16 byte)
Number of round	10	12	14
Round key size	4 word (16 byte)	4 word (16 byte)	4 word (16 byte)
Expanded key size	44 word (176 byte)	52 word (208 byte)	60 word (240 byte)

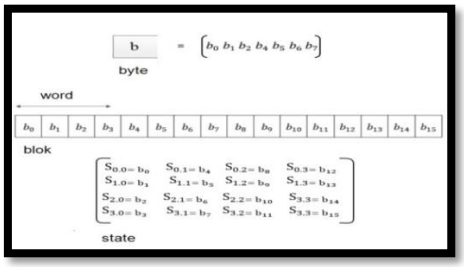
2.3.1 Sejarah *Advanced Encryption Standars* (AES)

Pada tahun 90-an, setelah beberapa tahun standar penyandian simetris DES dianggap tidak lagi aman, lembaga standar Amerika serikat NIST (*National Institute of Standards and Technology*) membuat sayembara untuk menggantika DES dengan sebuah sistem penyandian yang disebut dengan Advanced Encryption Standard pada tanggal 12 september 1997. NIST memberikan spesifikasi AES, yaitu harus memiliki panjang blok 128 bit dan mampu mendukung panjang kunci 128,192,dan 256. Setelah beberapa seleksi, NIST memilih sistem penyandian *Rijndael* yang dikembangkan oleh *joan daemen* dan *vincent rijment* sebagai sistem penyandian AES pada tahun 2000.

2.3.2 Unit Data AES

AES menggunakan 5 unit ukuran data: *bit*, *byte*, *word*, *blok* dan *state*. Yaitu:

1. *Bit* merupakan satuan data terkecil, yaitu nilai dari digit sistem terkecil.
2. *Byte* merupakan satuan dari 8 *bit*.
3. *Word* merupakan satuan dari 4 *byte* (32 *bit*), dan *Blok* berukuran 16 *byte*.
   State adalah blok yang ditata sebagai matriks *byte* berukuran 4x4.



Gambar 2.1 Unit Data AES

2.3.3 Transformasi – Transformasi AES

Algoritma eonkripsi AES menggunakan 4 jenis tranformasi:

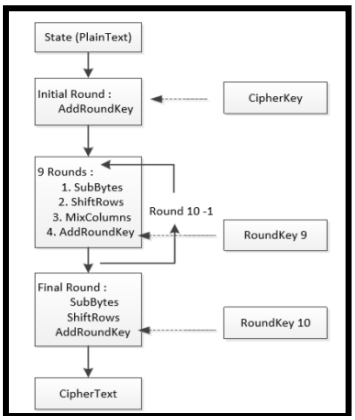
1. Substitusi yang disebut dengan *SubBytes*, merupakan perubahan byte yang mana setiap bagian pada state akan dipetakan dengan menggunakan sebuah tabel substitusi (*S-Box*).
2. Permutasi yang disebut dengan *ShiftRows*, perubahan*Shiftrows*yang pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit).
3. Percampuran yang disebut dengan *MixColumns*, *MixColumns* mengoperasikan setiap elemen yang berada dalam satu kolom pada state.

Penambahan kunci yang disebut dengan *AddRoundKe*, melakukan XOR antara state sekarang dengan round key.

2.3.4 Struktur Enkripsi AES

Proses di dalam aes merupakan perubahan terhadap *state*. Sebuah teks asli dalam bentuk blok (128 bit) terlebih dulu diorganisir sebagai *state*. Enkripsi AES adalah perubahan terhadap *state* secara berulang dalam beberapa ronde. *State* yang menjadi keluaran ronde k menjadi masukan untu ronde ke-k+1.

Pada awalnya teks asli direorganisasi sebagai sebuah *state*. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut *Addroundkey*). Setelah itu, ronde ke-1 sampai dengan ronde ke- (Nr-1) dengan Nr adalah jumlah ronde menggunakan 4 jenis transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundkey*. Pada ronde terakhir, yaitu ronde ke- Nr dilakukan transformasi serupa dengan ronde lain namun tanpa transformasi *mixcolumns*.



Gambar 2.2 Diagram Alur Proses Enkripsi AES

Adapun penjelasan dari setiap transformasi yaitu :

1. *AddRoundKey*

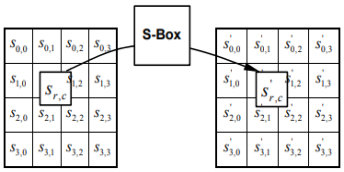
Pada proses enkripsi dan dekripsi AES proses *AddRoundKey* sama, sebuah *round key* ditambahkan pada *state* dengan operasi *XOR*. Setiap *round key* terdiri dari Nb *word* dimana tiap *word* tersebut akan dijumlahkan dengan *word* atau kolom yang bersesuaian dari *state.*

2. Transformasi *SubBytes* adalah perubahan *byte* yang mana setiap bagian pada *state* akan dipetakan dengan menggunakan sebuah tabel substitusi (*S-Box*).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

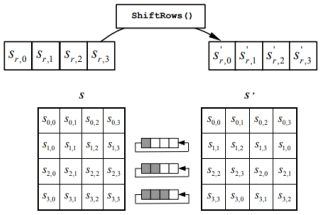
Tabel 2.3Tabel *S-Box*

Untuk setiap *byte* pada *array state*, misalkan S[r, c] = xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r, c], maka nilai substitusinya, dinyatakan dengan S'[r, c], adalah elemen di dalam tabel subtitusi yang merupakan perpotongan baris x dengan kolom y. Ilustrasikan pengaruh pemetaan *byte* pada setiap *byte* dalam *state* dapat.



Gambar 2.4 Pengaruh Pemetaan pada Setiap *Byte* dalam*State*

3. Transformasi *Shift Rows* pada dasarnya adalah proses pergeseran bit dimana bit palingkiri akan dipindahkan menjadi bit paling kanan (rotasi bit).



Gambar 2.5 Proses Transformasi *Shiftrows*

Transformasi *mixcolumns* merupakan operasi yang beroperasi terhadap setiap kolom pada state.*Mixcolumn* merupakan perkalian matriks pada sebuah kolom.Perkalian tersebut merupakan perkalian pada Persamaan 3. Transformasi MixColoums dapatdilihat pada perkalian matriks berikut:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Gambar 2.8 Perkalian Matriks *Mix Columns*

Contoh: Misalkan *state* seperti berikut, dan akan dilakukan transformasi*MixColumns*,

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

·

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

=

04	E0	48	28
66	CB	F8	06
81	19	D3	26
E5	9A	7A	4C

Gambar 2.9Transformasi *Mix Columns*

2.4 Digital Signature

Digital signature merupakan suatu metode untuk menggantikan tanda tangan secara manual pada dokumen kertas. Tanda tangan pesan dapat dilakukan dengan dua cara yaitu:

1. Enkripsi pesan mengenkripsi pesan dengan sendirinya serta menyediakan ukuran asli, pesan yang terenkripsi sudah menyatakan pesan tersebut telah ditandatangani.
2. Tanda tangan digital dengan fungsi *hash* (*hash function*).

Pada dasarnya, tanda tangan berfungsi untuk mengidentifikasi kesahan seseorang pada dokumen yang ditandatanganinya. Selain itu juga, tanda tangan bisaberfungsi untuk memverifikasi bahwa penandatangan telah mengetahui dan menbenarkan isi dari dokumen yang telah ditandatanganinya tersebut. Atribut yang harus dimiliki oleh sebuah tandatangan adalah:

1. Autentikasi penandatangan adalah tanda tangan dapat secara unik dikenali oleh pembuat dokumen tanpa bisa ditiru oleh orang lain.
2. Autentikasi dokumen adalah tanda tangan dapat dipakai untuk memferifikasi keaslian dokumen, maka bisa diketahui jika dokumen asli telah diubah.

Digital signature yang dicantumkan dalam suatu dokumen digital dapat memverifikasi darimana asalnya data tersebut. Sebuah tanda tangan digital bisa dipakai untuk memastikan apakah data tersebut benar bersumber dari pengirim, hingga perlu untuk divalidasi.

3. ANALISA DAN HASIL

3.1 Algoritma Sistem

Adapun algoritma dalam metode *Advanced Encryption Standard* yang akan digunakan untuk menyelesaikan permasalahan adalah melakukan proses ekspansi kunci, enkripsi, dan digital signature.

3.2 Ekspansi Kunci

Proses ekspansi kunci dibutuhkan untuk proses *AddRoundKey*. Jumlah kunci dari proses enkripsi kunci yang dibutuhkan algoritma AES 128 Bit adalah 10 kunci. Kunci yang akan digunakan pada kasus ini adalah "SEKDA.KOTA.MEDAN". berikut ini adalah proses ekspansi kunci *Advance Encryption Standard* :

1. Urutkan *plaintext* kunci ke dalam blok berukuran 128 Bit (16 Kode ASCII), setelah itu kunci akan diubah ke dalam bentuk *Hexadecimal*.

S	E	K	D	A	K	O	T	.	1	0	7	1	5	9	0
53	45	4B	44	41	4B	4F	54	2E	31	30	37	31	35	39	30

2. Setelah itu susun kunci yang telah diubah ke dalam *state* berukuran 4 x 4 seperti berikut :

53	45	4B	44
41	4B	4F	54
2E	31	30	37
31	35	39	30

⟶ Kunci Ronde ke-0

3. Setelah itu langkah pertama untuk menghasilkan kunci ke-1 adalah melakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom ke 4 ke atas 1 kali dari kunci ronke ke-0.

44				54	
54	→			37	
37				30	
30				44	

4. Lalu substitusikan hasik dari *RotWord* dengan nilai pada tabel *S-Box* (*SubBytes*).

→	54			20	
→	37	→		9A	
→	30			04	
→	44			1B	

Hasil substitusi *RotWord* dengan nilai pada tabel *X-Box*

5. Tahap akhir untuk mendapatkan kolom pertama kunci ronde ke-1 adalah proses XOR antara kolom pertama dari kunci ronde ke-0 dan hasil dari *SubBytes* lalu di XOR-kan dengan *RCon*.

3.2 Tabel *R Con*

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

20		53		01		72		
9A	⊕	41	⊕	00	=	DB	→	Kolom pertama kunci ronde ke -1 (wi)
04		2E		00		2A		
1B		31		00		2A		

6. Lalu untuk mendapatkan kolom kedua dilakukan XOR antara kolompertama (wi) dengan kolom kedua dari kunci rond ke-0, setelah itu dilakukan proses seperti kolom kedua untuk mendapatkan kolom berikutnya.

72		45		37		
DB	⊕	4B	=	90	→	Kolom Kedua
2A		31		1B		
2A		35		1F		

37		4B		7C		
90	⊕	4F	=	DF	→	Kolom Ketiga
1B		30		2B		
1F		30		26		

7C		44		38		
DF	⊕	54	=	8B	→	Kolom Keempat
2B		37		1C		
26		30		16		

7. Dengan demikian, dari seluruh proses di atas maka dihasilkan kunci untuk ronde ke-1, yaitu :

72	37	7C	38
DB	90	DF	8B
2A	1B	2B	1C
2A	1F	26	16

Proses diatas akan diulang sebanyak 10 kali untuk mendapatkan kunci ronde ke-2 sampai kunci ronde ke-10. Kunci dari setiap rondenya akan digunakan untuk proses enkripsi dan deskripsi, berikut ini adalah hasil seluruh ekspansi *key* :

72	37	7C	38
DB	90	DF	8B
2A	1B	2B	1C
2A	1F	26	16

4D	7A	06	3E
47	D7	08	83
6D	76	5D	41
2D	32	14	02

E2	D3	7E	3A
B4	1B	70	DF
FA	60	0D	4A
73	3A	6C	03

Kunci Ronde Ke – 1 Kunci Ronde Ke – 2 ... Kunci Ronde Ke – 10

3.3 Proses Enkripsi

Pada proses ini dilakukan penyandian terhadap slip gaji Kantor walikota medan. *Plaintext* yang akan dienkripsi adalah " UMUM/21/11/19/IIIC", dimana *plaintext* diambil dari data slip gaji, UMUM diambil dari bagian dan pengambilan, 21/11/19/IIIC diambil dari tanggal pengambilan gaji dan golongan pegawai, dan berikut ini adalah proses enkripsinya :

1. Urutkan *plaintext* ke dalam blok lalu ubah ke bentuk bilangan *hexadecimal*.

U	M	U	M	.	I	V	/	a	.	S	B	U	0	0	1
55	4D	55	4D	2E	49	56	2F	61	2E	53	42	55	30	30	31

2. Susun 16 byte pertama dari *plaintext* yang sudah diubah ke bentuk bilangan *hexadecimal* ke dalam *state* 4 x 4.

55	4D	55	4D
2E	49	56	2F
61	2E	53	42
55	30	30	31

3. Lalu masuk ke proses *AddRoundKey*, pada proses ini XOR-kan *plaintext* di atas dengan kunci ronde ke-0

53	45	4B	44	⊕	55	4D	55	4D	=	06	08	1E	09
41	4B	4F	54		2E	49	56	2F		6F	02	19	7B
2E	31	30	37		61	2E	53	42		4F	1F	63	75
31	35	39	30		55	30	30	31		64	05	09	01

4. Setelah itu hasil dari *AddRoundKey* di atas akan menjadi ronde ke-1 yang akan diproses lagi dengan 4 transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*.

Ronde 1

1. Transformasi pertama yaitu *SubBytes*, pada proses ini setiap *byte*akan ditukar dengan nilai pada tabel *S-Box*.

06	08	1E	09
6F	02	19	7B
4F	1F	63	75
64	05	09	01

SubBytes →

6F	30	72	01
A8	77	D4	21
84	D0	FB	9D
43	6B	01	7C

2. Setelah itu dilakukan proses *ShiftRows*, dengan cara menggeser setiap baris kecuali baris pertama pada *state*, baris kedua digeser 1 *byte* ke kiri, baris ketiga digeser 2 *byte* ke kiri, dan baris keempat digeser 3 *byte* ke kiri, untuk lebih jelasnya seperti di bawah ini :

		6F	30	72	01
	A8	77	D4	21
84	D0	FB	9D
43	6B	01	7C

=

6F	30	72	01
77	D4	21	A8
FB	9D	84	D0
7C	43	6B	01

3. Proses Selanjutnya adalah *MixColumns*, pada proses ini dilakukan proses perkalian antar *polinominal* tetap dengan *state* hasil *ShiftRows.*

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

X

6F	30	72	01
77	D4	21	A8
FB	9D	84	D0
7C	43	6B	01

Proses perhitungan untuk mencari baris pertama menggunakan operator polinominal, dengan aturan jika dikali 01 maka hasilnya tetap, jika dikali 02 maka *bitshift* 1x ke kiri jika MSB = 0 dan *bitshift* 1x ke kiri diikuti operasi XOR dengan 1B (0001 1011) jika MSB = 1, dan jika dikali 03 maka dilakukan operasi dikali 02 dan XOR dengan bilangan *hexadecimal* hasil *ShiftRows* itu sendiri. Dibawah ini adalah uraian perkalian *MixColumns* :

Byte baris 1 kolom 1 ($S^1_{0,0}$)
= ({02}x{6F})⊕ ({03}x{77}) ⊕ ({01}x{FB}) ⊕ ({01}x{7C})
= 11011110 ⊕ 10011001 ⊕ 11111011 ⊕ 01111100
= 11000000
= CA

Byte baris 2 kolom 1 ($S^1_{1,0}$
= ({01}x{6F})⊕ ({02}x{77}) ⊕ ({03}x{FB}) ⊕ ({01}x{7C})
= 01101111 ⊕ 01110111 ⊕ 11101101 ⊕ 01100010
= 01001100 = 4C

Byte baris 4 kolom 4 ($S^1_{3,3}$)
= ({01}x{6F})⊕ ({01}x{77}) ⊕ ({02}x{FB}) ⊕ ({03}x{7C})

= 00000011 ⊕ 00010011 ⊕ 01010001 ⊕ 01100000
= 00100001 = 21

4. Langkah terakhir dari ronde ke-1 adalah *AddRoundKey*, proses ini sama denganyang sebelumnya tetapi *state* hasil proses *MixColumns* di-XOR-kan dengan kuncironde ke-1, berikut ini adalah prosesnya :

D6	93	D8	9C	⊕	CA	15	BD	D9	=	1C	86	65	45
A2	8C	C7	88		4C	BF	73	C3		EE	33	B4	4B
7B	3A	14	59		69	FA	BB	E0		12	C0	AF	B9
5E	1A	5B	15		E7	BA	F5	21		B9	A0	AE	34

Proses di atas akan diulangi untuk ronde ke-2 sampai ronde ke-10, dan pada ronde ke 10 transformasi *MixColumns*tidak dilakukan. Untuk hasil transformasi proses enkripsi ronde ke-1 sampai ronde ke-10 bisa dilihat di bawah ini

Table 3.3 Proses Enkripsi AES 128 bit

	SubBytes				ShiftRows				MixColumns				AddRoundKey			
R0													6	8	1E	9
													6E	1C	7A	60
													65	70	1	7C
													7C	6B	8	D
R1	6F	30	72	1	6F	30	72	1	CA	15	BD	D9	1C	86	65	45
	9F	9C	DA	D0	9C	DA	D0	9F	4C	BF	73	C3	EE	33	B4	4B
	4D	51	7C	10	7C	10	4D	51	69	FA	BB	E0	12	C0	AF	B9
	10	7F	30	D7	D7	10	7F	30	E7	BA	F5	21	B9	A0	AE	34
R2	9C	44	4D	6E	9C	44	4D	6E	1C	90	7D	49	C	13	26	8E
	28	C3	8	B3	C3	8	B3	18	59	F8	90	6F	30	1D	B2	C5
	C9	BA	79	56	79	56	C9	BA	85	35	8C	36	A7	2D	80	63
	56	E0	E4	18	18	56	E0	E4	35	3E	76	C3	B5	A4	B7	17
R3	FE	7D	F7	19	FE	7D	F7	19	2D	B5	1D	4F	95	8E	7D	E8
	4	A4	37	A6	A4	37	A6	4	11	D0	D	CB	84	A0	5F	33
	5C	D8	CD	FB	CD	FB	5C	D8	D0	43	32	56	BA	31	4C	7D
	D5	49	A9	F0	F0	D5	49	A9	8B	F0	68	BE	CD	2C	75	77
R4	2A	19	FF	9B	2A	19	FF	9B	B3	3A	C	96	42	F0	A6	9B
	5F	E0	CF	24	E0	CF	24	5F	4	86	C1	EA	60	92	87	54
	F4	C7	29	FF	29	FF	F4	C7	9C	EF	BB	78	2B	2A	0	E8
	BD	71	9D	F5	F5	BD	71	9D	46	7A	28	F	5C	BC	F3	1D

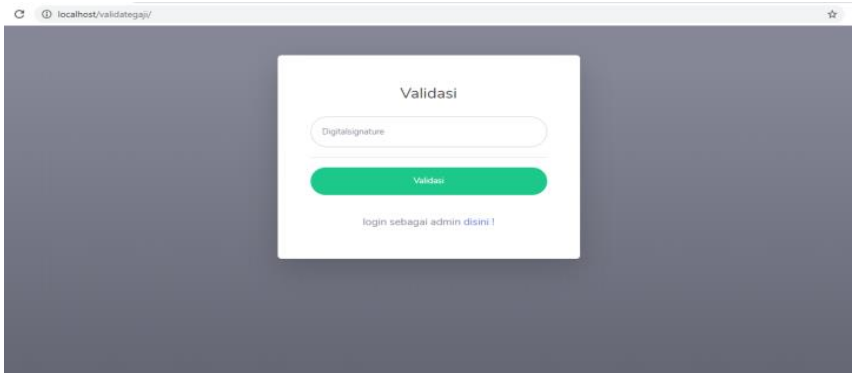
R5	2C	8C	24	14	2C	8C	24	14	2D	EB	DC	AB	62	6E	F3	89
	D0	4F	17	20	4F	17	20	D0	B3	73	39	96	B7	63	6F	7E
	F1	E5	63	9B	63	9B	F1	E5	52	4D	62	2	2C	F6	62	92
	4A	65	0D	A4	A4	4A	65	0D	B	C	27	13	C6	7	F7	D1
R6	AA	9F	0D	A7	AA	9F	0D	A7	CD	3D	93	AC	39	4C	CD	D0
	A9	FB	A8	F3	FB	A8	F3	A9	9C	B1	F3	15	F8	C5	D1	DF
	71	42	AA	4F	AA	4F	42	71	5C	A9	7A	54	7	49	9A	24
	B4	C5	68	3E	3E	B4	C5	68	C8	E9	37	FA	96	BC	B2	BD
R7	12	29	BD	70	12	29	BD	70	17	B6	78	2F	D7	7	97	BC
	41	A6	3E	9E	A6	3E	9E	41	EC	47	A8	8B	D9	6	CB	22
	C5	3B	B8	36	B8	36	C5	3B	51	8C	1D	1E	AA	97	E6	95
	90	65	37	7A	7A	90	65	37	DC	38	4D	84	92	23	D3	5D
R8	0E	C5	88	65	0E	C5	88	65	A8	D5	2D	7B	3B	F7	E0	25
	35	6F	1F	93	6F	1F	93	35	FB	8A	7C	E9	F3	C3	56	6A
	AC	88	8E	2A	8E	2A	AC	88	5C	5F	32	F1	92	8A	1C	54
	4F	26	66	4C	4C	4F	26	66	42	FC	F0	DE	D0	75	E7	10
R9	E2	68	E1	3F	E2	68	E1	3F	FB	59	5	EA	9F	1F	8E	3F
	0D	2E	B1	2	2E	B1	2	0D	CB	1	B1	33	C5	46	DC	DD
	4F	7E	9C	20	9C	20	47	7E	A4	9	D1	69	E1	99	6F	72
	70	9D	94	CA	CA	70	9D	94	10	C9	5C	1	DA	8A	8	9B
R10	DB	C0	19	75	DB	C0	19	75					A1	FC	AE	17
	A6	5A	86	C1	5A	86	C1	A6					FB	60	4A	C3
	F8	EE	A8	40	A8	40	F8	EE					6D	15	13	1E
	57	7E	30	14	14	57	7E	30					DD	DD	A0	74

Setelah proses ekripsi selesai *AddRoundkey* pada ronde ke-10 akan di jadikan sebagai *Digital Signature* yang akan ditampilkan pada slip gaji dan akan digunakan untuk menvalidasi slip gaji. Digital signature dihasilkan dari random string yang di enkripsi menggunakan AES 128 bit. Pada saat validasi digital signature dipanggil lagi dari tabel karyawan.

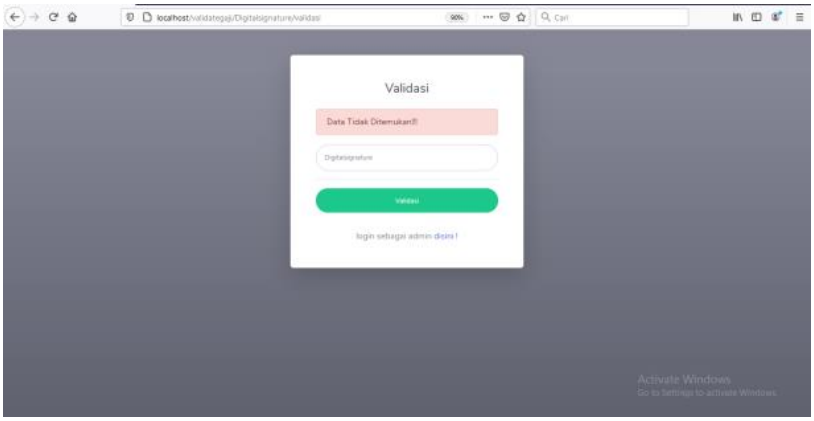
4. PENGUJIAN DAN IMPLEMENTASI

4.1. Halaman Validasi Slip Gaji

Berikut ini tampilan halaman validasi sebelum akses login yang berfungsi menyediakan menu validasi hasil digital signature yang ada pada slip gaji yaitu :

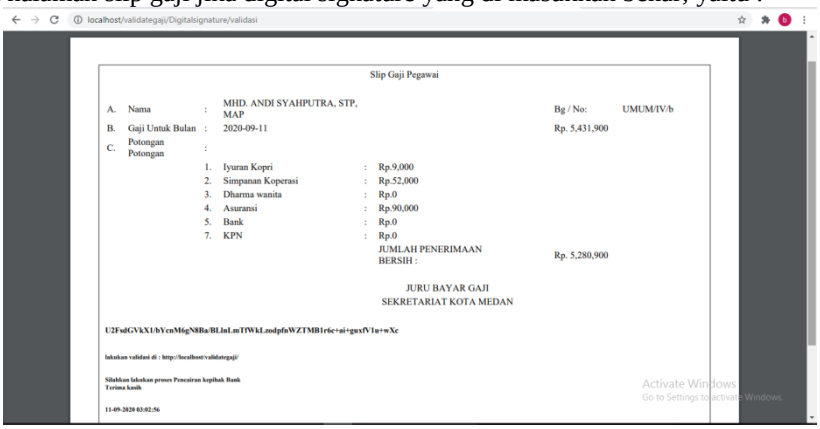


Gambar 4.1 Halaman Validasi Slip Gaji



Gambar 4.1 Halaman Validasi Slip Gaji Jika Digital Signature Salah

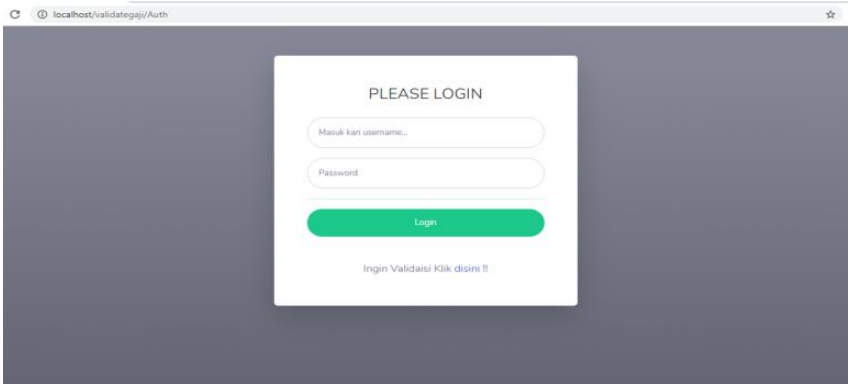
Berikut ini tampilan halaman slip gaji jika digital signature yang di masukkan benar, yaitu :



Gambar 4.3 Halaman Hasil Slip Gaji

4.2. Halaman Akses Login

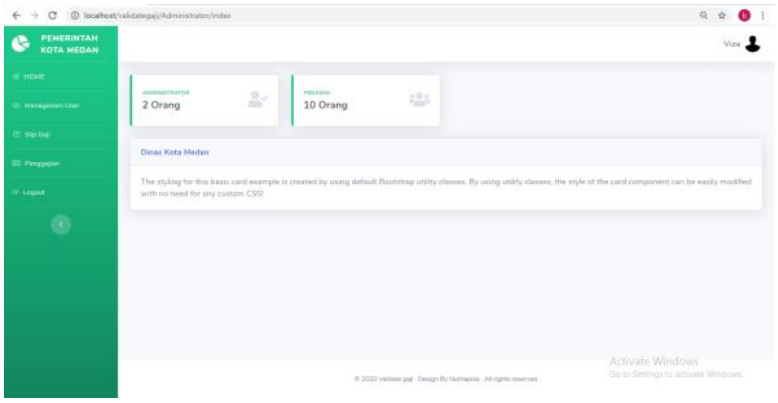
Berikut ini tampilan halaman akses login yang berfungsi untuk bagian keuangan agar bisa mengatur data di dalam program, yaitu :



Gambar 4.4 Halaman Akses Login

4.3. Halaman Utama Setelah Login

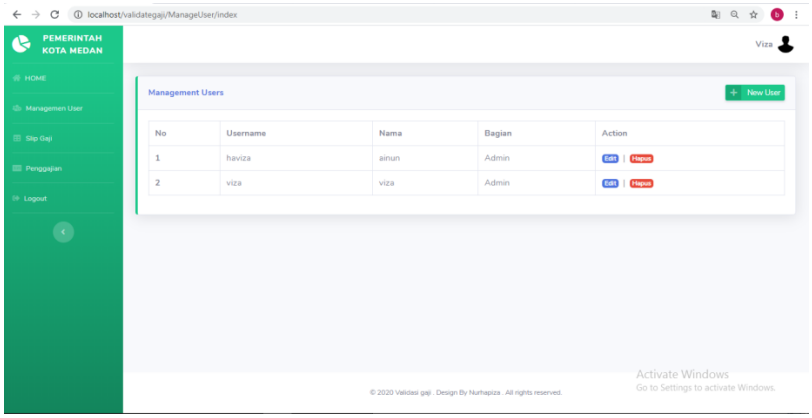
Berikut ini tampilan halaman utama setelah proses login , yaitu:



Gambar 4.5 Halaman Utama Setelah Login

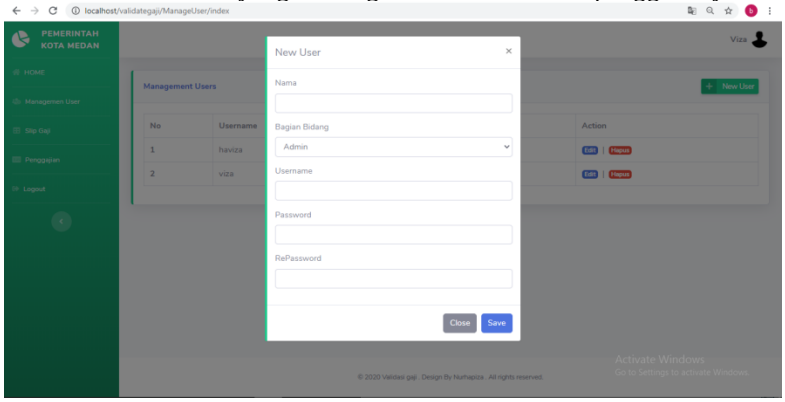
4.4. Halaman Managemen User

Berikut ini tampilan halaman managemen user untuk menambah pengguna yang bisa mengakses data, yaitu:



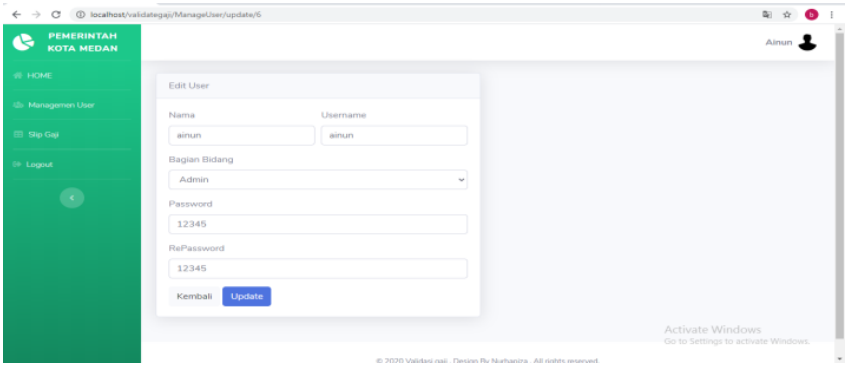
Gambar4.6 Halaman Managemen User

Berikut ini tampilan halaman new user yang berfungsi untuk menambah pengguna, yaitu :



Gambar 4.7 Halaman New User

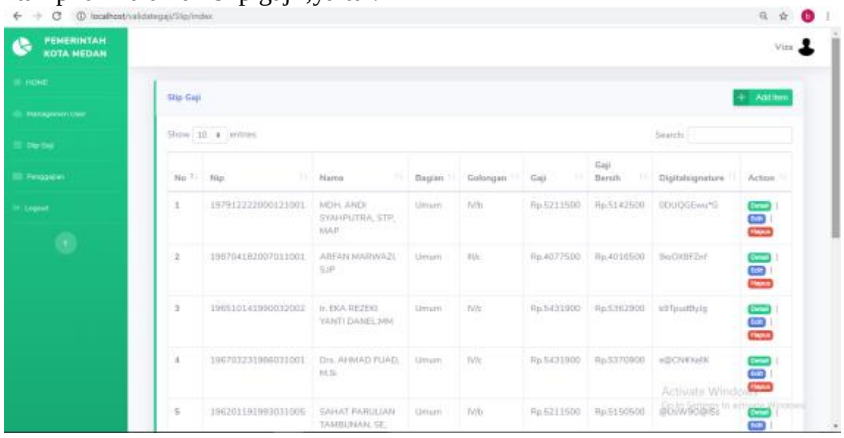
Berikut ini tampilan halaman edit user yang berfungsi untuk mengubah atau memperbarui data pengguna, yaitu :



Gambar 4.8 Halaman Edit User

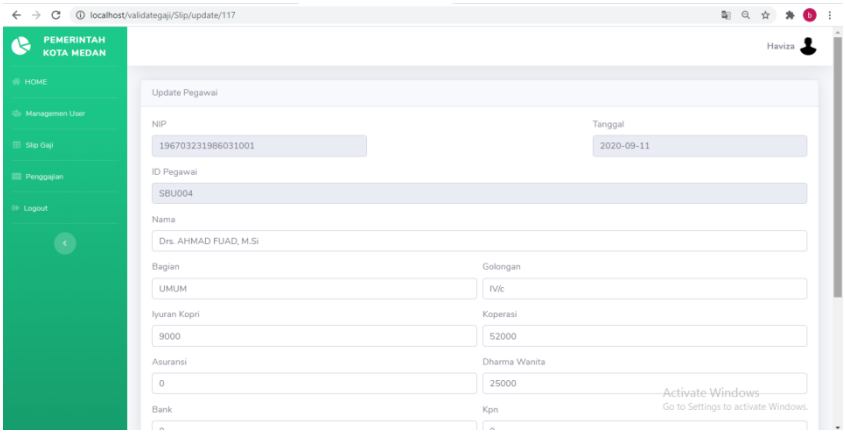
4.5. Halaman Slip Gaji

Berikut ini tampilan halaman slip gaji ,yaitu :



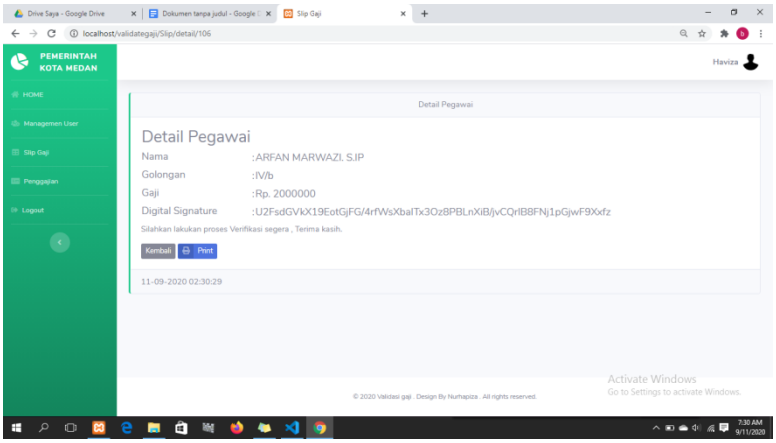
Gambar 4.9 Halaman Slip Gaji

Berikut ini tampilan halaman edit slip yang berfungsi untuk mengubah atau memperbarui data pada slip gaji, yaitu:



Gambar 4.10 Halaman Edit Slip Gaji

Berikut ini tampilan halaman detail pegawai yang berfungsi untuk melihat detail data pada slip gaji, yaitu:



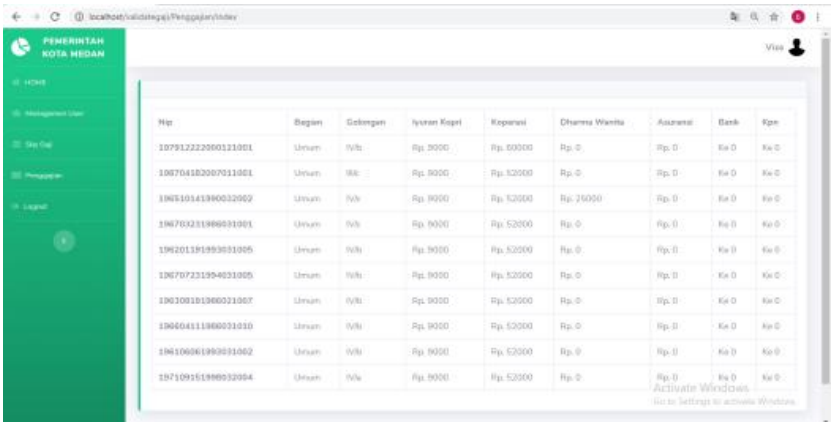
Gambar 4.11 Halaman Detail Slip Gaji

Berikut ini tampilan halaman print detail pegawai yang berfungsi untuk mengeluarkan digital signature, yaitu:

Gambar 4.12 Halaman Print Slip Gaji

4.6 Halaman Penggajian

Berikut ini tampilan halaman Penggajian ,yaitu :



Gambar 4.13 Halaman Penggajian

5. KESIMPULAN

Adapun simpulan akhir dari penelitian ini yaitu sebagai berikut :

1. Kantor walikota medan merupakan salah satu instansi yang harus memiliki keamanan data yang baik.
2. Berdasarkan penelitian, metode *Advanced Encryption Standard* (AES) dan *Digital Signature* dapat diterapkan sebagai penambah keamanan pada slip gaji agar slip gaji lebih terverifikasi.

3. Berdasarkan penelitian, dalam upaya memodelkan sistem validasi yang dirancang dapat dilakukan yang diawali dengan analisis masalah kebutuhan kemudian dilakukan pemodelan.
   Sistem yang telah dirancang selanjutnya diuji dan diimplementasikan dengan memasukkan data-data sampel sesuai dengan yang ada pada bab-bab sebelumnya, jika hasil outputnya sesuai dengan data perhitungan manual maka dalam pengujian ini sistem berjalan dengan baik, baik dalam hal menambahkan data ke *database*, perintah update untuk merubah data di *database*, dan perintah delete untuk menghapus data di *database* adalah sarana yang digunakan untuk pengkodean dan pengujian sistem

UCAPAN TERIMA KASIH

Puji syukur saya ucapkan kepada Allah Subhanahu Wata'ala yang telah melimpahkanrahmat, kesehatan, serta karunia-Nya, hingga dapat menyelesaikan Skripsi yang berjudul E- *Security* di dalam *Digital Signature* Berbasis Algoritma AES (*Advanced Encryption Standard*) 128 *Bit* pada Slip Gaji Pegawai di Kantor Walikota Medan tepat pada waktunya. Penulisan skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan pendidikan Strata 1 program studi Sistem Informasi di STMIK Triguna Dharma. Teruntuk Ibunda Hadjirah dan Ayahanda Alm. Iwan Achyar Nasution serta keluarga yang tercinta terima kasih atas segala do'a, kasih sayang, perhatian, dukungan, semangat yang tiada henti tercurah.Dalam penulisan skripsi ini dapat banyak bantuan bimbingan dan dukungan dari berbagai pihak, baik berupa masukan, arahan, motivasi, dukungan, maupun saran-saran yang telah diberikan. Untuk itu pada kesempatan ini ingin mengucapkan terima kasih kepada Bapak Rudi Gunawan, SE, M.SI selaku Ketua STMIK Triguna Dharma,Bapak Zulfian Azmi ST, M.Kom selaku Wakil Ketua I Bidang Akademi STMIK Triguna Dharma.Bapak Marsono, S.Kom, M.Kom Selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma,Bapak Jaka Prayudha, S.Kom., M.Kom Selaku Dosen Pembimbing I yang telah banyak membimbing dalam memberikan arahan, masukan sehingga terselesaikannya skipsi ini, Ardianto Prananta,S,kom., M.**Kom** Selaku Dosen Pembimbing II yang telah banyak membantu dalam memberikan bimbingan tentang sistematika penulisan dengan benar.Seluruh Dosen, Staff dan Pegawai di STMIK Triguna Dharma Medan.

REFERENSI

[1] P. Group, "Pentingnya Cyber Security," 2019. [Online]. Available: http://www.phintraco.com/pentingnya-cyber-security/.
[2] R. Jermias, "Analisa Sistem Informasi Akuntansi Gaji Dan Upah Pada PT. BANK SINARMAS Tbk. MANADO," *J. Ris. Ekon. Manajemen, Bisnis dan Akunt.*, vol. 4, no. 2, pp. 814–828, 2016.
[3] H. Agung, "Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature."
[4] H. Haryanto, R. Wiryadinata, and M. Afif, "Implementasi Kombinasi Algoritma Enkripsi Aes 128 Dan Algoritma Kompresi Shannon-Fano," vol. 3, no. 1, 2014.
[5] M. I. Fitrianda, "Digital Digital Repository Repository Universitas Universitas Jember Jember Digital Digital Repository Repository Universitas Universitas Jember," 2013.
[6] A. Arif, P. Mandarani, and M. Tenik Informatika, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (Aes) 128 Bit Pada Sistem Keamanan Short Message Service (Sms) Berbasis Android," vol. 4, no. 1, 2016.
[7] R. Sadikin, *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*, I. ANDI Yogyakarta, 2018.

BIOGRAFI PENULIS

	**Ainun Haviza Nasution,** Perempuan kelahiran Medan, 21 Maret 1999, anak kelima dari lima bersaudara ini merupakan mahasiswa STMIK Triguna Dharma yang sedang dalam proses menyelesaikan skripsi.

	**Jaka Prayudha, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Komputer.
	**Ardianto Prananta,S,kom., M.Kom.** Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Komputer.