Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Implementasi Algoritma AES Pada Qr-Code Untuk Validasi Keaslian Surat Kontrak Kerja Di Pt. Citra Alfa Sasmita

Vira Dwi Puspita Anggraini[1], Khairi Ibnutama[2], Zaimah Panjaitan[3]

[1,2,3] Sistem Infromasi, STMIK Triguna Dharma
Email: [1]virapuspitaanggraini@gmail.com, [2]mr.ibnutama@gmail.com, [3]zaimahp09@gmail.com
Email Penulis Korespondensi: virapuspitaanggraini@gmail.com

Article History:
Received Jul 25th, 2025
Revised Aug 14th, 2025
Accepted Aug 30th, 2025

Abstrak

Penelitian ini bertujuan untuk meningkatkan keamanan surat kontrak kerjasama di PT. Cita Alfa Sasmita dengan mengimplementasikan algoritma kriptografi AES 128-bit. Proses enkripsi menghasilkan *ciphertext* yang kemudian dikonversi menjadi QR-Code sebagai identitas unik dokumen. QR-Code ini digunakan untuk memverifikasi keaslian surat dan mencegah pemalsuan. Sistem dibangun menggunakan Laravel dan diuji pada perangkat dengan spesifikasi minimal RAM 4GB dan prosesor Core i3. Hasil implementasi menunjukkan bahwa metode ini mampu menjaga keamanan dan mempercepat proses validasi dokumen. Meskipun sistem cukup efektif, terdapat kelemahan dalam pembacaan QR-Code pada perangkat rendah spesifikasi dan keterbatasan responsivitas tampilan. Secara keseluruhan, integrasi AES 128-bit dengan QR-Code terbukti efisien dalam melindungi dokumen digital secara praktis

Kata Kunci : AES 128-bit, QR-Code, Kriptografi, Surat Kontrak, Keamanan Data

Abstract

This study aims to improve the security of cooperation contract letters at PT. Cita Alfa Sasmita by implementing the AES 128-bit cryptographic algorithm. The encryption process produces ciphertext which is then converted into a QR-Code as a unique document identity. This QR-Code is used to verify the authenticity of the letter and prevent forgery. The system is built using Laravel and tested on devices with minimum specifications of 4GB RAM and a Core i3 processor. The implementation results show that this method is able to maintain security and accelerate the document validation process. Although the system is quite effective, there are weaknesses in reading QR-Code on low-spec devices and limited display responsiveness. Overall, the integration of AES 128-bit with QR-Code has proven to be efficient in protecting digital documents practically.

Keyword : *AES 128-bit, QR-Code, Cryptography, Contract Letter, Data Security*

1. PENDAHULUAN

Berbagai tindak kejahatan yang semakin modern dan variatif[1], perlu menekankan peningkatan keamanan salah satunya dari manipulasi data, pemalsuan dan penyalahgunaan informasi sehingga dapat minimalisasi kerugian[2]. PT. Cita Alfa Sasmita merupakan agen resmi yang memiliki izin mendistribusikan LPG ke pangkalan yang terikat dalam hubungan perjanjian atau kontrak untuk menyalurkan LPG langsung ke tangan konsumen. Dalam menjalankan aktivitasnya, perusahaan menghadapi tantangan dalam hal keamanan dan validasi dokumen kontrak kerjasama. Di era digital saat ini, pemalsuan dokumen kontrak merupakan ancaman nyata yang dapat menyebabkan kerugian finansial dan operasional[3].

Selama ini surat kontrak kerjasama LPG pada PT. Cita Alfa Sasmita masih belum terdigitalisasi, melainkan dalam bentuk dokumen fisik. Kontrak kerjasama antara agen dan pangkalan disusun dalam bentuk dokumen tertulis resmi yang ditandatangani oleh kedua belah pihak[4]. Salinan kontrak fisik ini disimpan oleh masing-masing pihak sebagai dokumen

legal[5]. Dokumen fisik memiliki beberapa risiko terkait keamanan, hal ini dapat berpotensi menimbulkan kecurangan. Seperti memodifikasi isi dokumen yaitu dengan membuat dokumen baru menggunakan desain dan tampilan yang serupa dengan aslinya[6].

Seperti, merubah harga jual LPG diatas HET (Harga Eceran Tertinggi) yang telah ditetapkan pemerintah[7]. Pemalsuan juga dapat terjadi pada tanda tangan[8] menggambarkan dengan palsu seolah-olah datangnya dari orang yang namanya tercantum dibagian bawah surat perjanjian tersebut[9]. Selain itu, pemalsuan identitas dan penyalahgunaan indentitas dapat mengakibatkan kerugian terhadap pemilik asli data pribadi tersebut[10], misalnya pangkalan sudah berpindah kepemilikan dan pemilik yang baru belum melakukan perubahan identitas pemilik pangkalan dan melakukan pelanggaran yang tidak sesuai dengan ketentuan[11], misalnya pengoplosan gas LPG[12]. Oleh karena itu, menjaga keaslian dan keamanan surat kontrak Kerjasama menjadi prioritas utama untuk menghindari risiko pemalsuan, manipulasi data, dan penyalahgunaan informasi yang dapat merugikan perusahaan dan pemilik data[13].

Berdasarkan penelitian sebelumnya, penggunaan algoritma kriptografi AES dalam QR-Code terbukti efektif untuk validasi keaslian dan keamanan data. Nahar Mardiyantoro menyatakan algoritma AES mampu mengenkripsi dan menjaga informasi dalam KTA dengan baik [14]. Adiat Pariddudin mengemukakan algoritma AES pada QR-Code efektif dalam mengamankan tiket dari manipulasi dan penjualan ulang [15]. La Surimi menyatakan penggunaan QR-Code dan algoritma AES dapat memvalidasi surat dengan mengindentifikasi surat asli atau surat palsu[16]. Yosua Situmeang menambahkan algoritma AES pada QR-Code dapat menghindari kebocoran dan manipulasi data penerima bantuan sosial[17].

Dengan penelitian ini, diharapkan dapat memberikan solusi efektif dalam meningkatkan keamanan dan validasi dokumen kontrak kerjasama di PT. Cita Alfa Sasmita, sekaligus meminimalisasi risiko kecurangan dan penyalahgunaan informasi.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi adalah pengetahuan pada suatu bidang ilmu yang mempelajari tentang kaidah-kaidah matematika yang berkaitan tentang bagaimana mengonversi pesan asli ke kebentuk yang lain sehingga maksud dari isi pesan tidak mudah dipahami[18]. Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *Cryptos* dan *graphein*[19], *Cryptos* yang artinya tersembunyi dan *graphein* yang artinya tulisan[20]. Kriptografi dapat diartikan sebagai suatu ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi[21] seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data.

2.2 Advanced Encryption Standard

Advanced Encryption Standard (AES) merupakan teknik atau algoritma kriptografi penyandian pesan yang menggunakan teknik blok simetris[22]. Cara kerja algoritma AES menggunakan substitusi dan permutasi dalam orientasi *byte* yang diulang-ulang sehingga hasil enkripsi lebih aman. Algoritma ini mempunyai kunci internal yang berbeda-beda di setiap putarannya[14]. Algoritma AES memiliki ukuran *block* yang tetap yaitu sepanjang 128 bit dengan panjang kunci 128bit, 192bit, dan 256-bit dan setiap blok dienkripsi dalam sejumlah putaran tertentu[23]. AES-128 menggunakan 10 *round*, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 *round*[24]. Untuk Kunci AES-128 menggunakan proses perulangan yang disebut sebagai *round* yaitu sebanyak 10 kali putaran dengan pola matriks 4 x 4 dimana setiap pola matriks terdiri atas 1 *byte* atau 8 bit untuk melakukan enkripsi dan dekripsi[25].

Tabel 1. Perbandingan Jumlah *Round* dan *Key* pada Tipe AES[41]

Tipe	Panjang Kunci (Nk words)	Ukuran Blok (Nb words)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.2.1 Proses Ekspansi Kunci

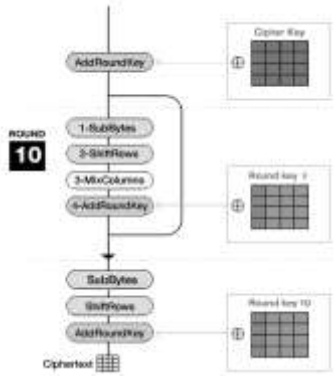
Proses ekspansi kunci dalam algoritma AES yang akan dipakai pada tiap tahap diperlukan dalam proses enkripsi. Untuk melakukan pengembangan jumlah kunci yang akan dipakai dari kunci utama maka dilakukan *key schedule*. Proses ini terdiri dari beberapa, yaitu:

1. *Rotate*, yaitu proses perputaran 8 bit pada 32 bit dari kunci.
2. *SubBytes*, yaitu 8 bit dari *subkey* disubstitusikan dengan nilai dari *S-Box*.
3. *Rcon*, proses ini akan diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari *user*.
4. XOR, dengan wi[-Nk] yaitu *word* yang berada pada Nk sebelumnya.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

2.2.2 Struktur Enkripsi AES

Enkripsi adalah aktivitas mengubah bentuk data yang awalnya mudah dipahami menjadi kode yang sulit dipahami. Caranya, dengan mengacak data sensitif agar berbeda dengan aslinya[26]. Proses enkripsi algoritma AES-128 terdiri dari 4 jenis transformasi *byte*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*[25]. Pada awal proses enkripsi, *state* akan mengalami transformasi *byte AddRoundKey*. Kemudian *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey* sebanyak Nr. Proses dalam algoritma AES ini disebut *round function*. *Round* terakhir sedikit berbeda dengan *round* sebelumnya, dimana pada *round* terakhir tidak mengalami transformasi *MixColumns*[27].



Gambar 1. Skema Proses Enkripsi AES

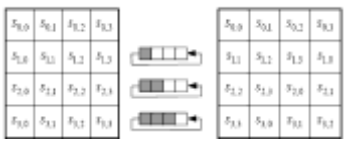
Secara garis besar, algoritma AES yang bekerja pada blok data 128-bit dengan kunci 128-bit (tanpa menyertakan proses pembangkitan *round key*) terdiri atas tahapan-tahapan berikut[28]:

1. *Plaintext* diubah menjadi kedalam bentuk *ASCI*
2. *AddroundKey*, tahapan ini melakukan operasi XOR antara data awal *(plaintext)* dengan *cipherkey*. Proses ini disebut juga sebagai *initial round*.
3. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes*, Transformasi ini memetakan setiap *byte* dari *array state* dengan menggunakan tabel substiusi *S-Box*.

x \ y	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

Gambar 2. Tabel *S-Box*

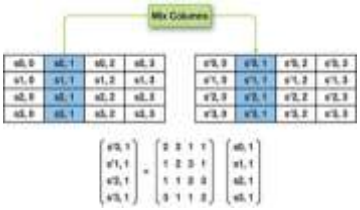
   b. *ShiftRows*, seperti namanya adalah sebuah proses yang melakukan *shift* atau pergeseran pada setiap elemen blok / tabel yang dilakukan per barisnya[15]. Jumlah pergeseran bergantung pada nilai baris (r). Baris r = 1 digeser sejauh 1 *byte*, baris r = 2 digeser sejauh 2 *byte*, dan baris r = 3 digeser sejauh 3 *byte*, Baris r = 0 tidak digeser.



Gambar 3. Proses *ShiftRows*

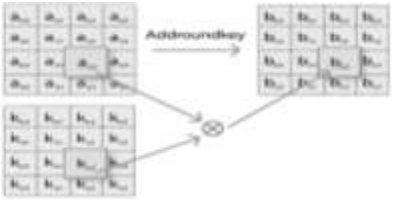
   c. *MixColumns*, mengalikan tiap elemen dari *blok chiper* dengan matriks. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan *dot product* lalu perkalian keduanya dimasukkan ke dalam sebuah *blok chiper* baru[15]. Mengalikan setiap kolom dari *array state* dengan *polinom* a(x) mod (x4 + 1). Setiap kolom diperlakukan sebagai polinom 4-suku pada GF(28). a(x) yang ditetapkan adalah a(x) = {03}x3 + {01}x2 + {01}x + {02}[42].

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index



Gambar 4. Proses *MixColumns*

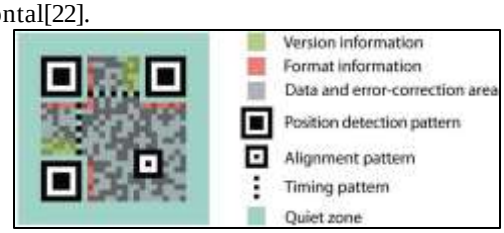
d. *AddRoundKey*, Melakukan operasi XOR terhadap sebuah *round key* dengan *array state*, dan hasilnya disimpan di *array state*[28].



Gambar 5. Proses *AddRoundKey*

2.3 QR-Code (Quick Response)

Qr-Code merupakan teknik yang mengubah data tertulis menjadi kode-kode 2 dimensi yang tercetak kedalam suatu media yang lebih ringkas[29]. QR-Code dirancang untuk memungkinkan proses pembacaan dan penyampaian informasi secara cepat dan efisien[17]. QR-Code memiliki kemampuan untuk menyimpan data di dalamnya. QR-Code merupakan pengembangan dari kode batang (barcode). Karena QR-Code merupakan matriks dua dimensi, maka penyimpanan data dilakukan secara vertikal dan horisontal[22].



Gambar 6. Struktur QR-Code

3. HASIL DAN PEMBAHASAN

3.1 Algoritma Sistem

Adapun algoritma yang akan digunakan dalam metode *Advanced Encryption Standard* adalah melakukan proses ekspansi kunci dan proses enkripsi.

3.1.1 Proses Ekspansi Kunci

AES dengan panjang kunci 128 bit (16 *byte*) memerlukan 10 buah kunci *ronde (RoundKey)* yang dihasilkan melalui proses ekspansi dari kunci utama[30]. Pada penelitian ini, kunci yang akan digunakan yaitu "31DES202401TRIVI". Berikut adalah proses ekspansi kunci dengan metode AES 128 bit.

a. Urutkan *plaintext* kunci kedalam blok berukuran 128 bit (16 Kode ASCII), kemudian kunci diubah kedalam bentuk *hexadecimal*

3	1	D	E	S	2	0	2	4	0	1	T	R	I	V	I
33	31	44	45	53	32	30	32	34	30	31	54	52	49	56	49

b. Susun kunci yang telah diubah kedalam bentuk *hexadecimal* dalam *state* berukuran 4 x 4

33	53	34	52
31	32	30	49
44	30	31	56
45	32	54	49

c. Untuk membentuk kolom pertama dari sub-kunci pada setiap *ronde*, langkah awal yang dilakukan adalah menerapkan fungsi *RotWord*, yaitu dengan melakukan pergeseran *rotasi* terhadap kolom ke 4 ke atas 1 kali menggunakan *RoundKey* ke-0 untuk menghasilkan *RoundKey* ke-1.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

52	→	49	
49		56	
56		49	
49		52	

d. Hasil dari fungsi *RotWord* akan melalui proses substitusi *byte* dengan menggunakan nilai yang terdapat pada tabel *S-Box*, disebut proses *SubBytes*.

49	→	3B
56	→	B1
49	→	3B
52	→	00

e. Untuk memperoleh kolom pertama dari *RoundKey* ke-1 adalah dengan melakukan operasi XOR antara kolom pertama dari *RoundKey* ke-0 dengan hasil dari *SubBytes* yang telah dikombinasikan melalui XOR dengan *Rcon*.

33	⊕	3B	⊕	01	=	09
31		B1		00		80
44		3B		00		7F
45		00		00		45

f. Untuk menghasilkan kolom-kolom berikutnya, dilakukan operasi XOR antara kolom pertama (Wi) dengan kolom kedua dari *RoundKey* ke-0. Proses ini diulang untuk setiap kolom selanjutnya hingga seluruh kolom dalam *RoundKey* terbentuk.

09	⊕	53	=	5A	5A	⊕	34	=	6E	6E	⊕	52	=	3C
80		32		B2	B2		30		82	82		49		CB
7F		30		4F	4F		31		7E	7E		56		28
45		32		77	77		54		23	23		49		6A

g. Berdasarkan seluruh proses yang telah dijelaskan sebelumnya, maka *RoundKey* ke-1 berhasil diperoleh, yaitu:

09	5A	6E	3C
80	B2	82	CB
7F	4F	7E	28
45	77	23	6A

Untuk menghasilkan *RoundKey* ke-2 hingga *RoundKey* ke-10, proses diatas tersebut diulangi sebanyak 10 kali. Di bawah ini ditampilkan hasil ekspansi kunci dari *RoundKey* ke-2 hingga *RoundKey* ke-10

RoundKey ke-2			
14	4E	20	1C
B4	06	84	4F
7D	32	4C	64
AE	D9	FA	90

RoundKey ke-3			
94	DA	FA	E6
F7	F1	75	3A
1D	2F	63	07
32	EB	11	81

….

RoundKey ke-10			
15	A5	DB	48
F0	3F	CF	20
05	31	10	06
24	FF	76	1E

3.1.2 Proses Enkripsi AES

Proses enkripsi berupa surat kontrak kerjasama PT. Cita Alfa Sasmita. *Plaintext* yang akan dienkripsi adalah “RISKA YUNIKA GAS" dengan proses enkripsi seperti berikut ini:

a. *Plaintext* disusun ke dalam blok dan dikonversi ke dalam bentuk *hexadecimal*.

R	I	S	K	A		Y	U	N	I	K	A		G	A	S
52	49	53	4B	41	20	59	55	4E	49	4B	41	20	47	41	53

b. *Blok plaintext* dalam bentuk *hexadecimal* tersebut kemudian diatur ke dalam *state* berukuran 4 x 4 *byte*.

52	41	4E	20
49	20	49	47
53	59	4B	41
4B	55	41	53

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

c. Tahap berikutnya adalah proses *AddRoundKey*, yaitu melakukan operasi XOR antara *plaintext* dengan *cipherkey* (*RoundKey* ke-0).

52	41	4E	20
49	20	49	47
53	59	4B	41
52	41	4E	20

⊕

33	53	34	52
31	32	30	49
44	30	31	56
45	32	54	49

=

61	12	7A	72
78	12	79	0E
17	69	7A	17
0E	67	15	1A

d. Hasil dari *AddRoundKey* akan menjadi input untuk *Round* ke-1, yang terdiri dari 4 transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*.

Hasil *AddRoundKey*			
61	12	7A	72
78	12	79	E
17	69	7A	17
E	67	15	1A

SubBytes			
EF	C9	DA	40
BC	C9	B6	AB
F0	F9	DA	F0
AB	85	59	A2

ShiftRows			
EF	C9	DA	40
C9	B6	AB	BC
DA	F0	F0	F9
A2	AB	85	59

MixColumns			
FD	13	3C	FF
B1	1E	19	6A
74	62	1E	FE
66	4B	3F	37

RoundKey Ke-1			
9	5A	6E	3C
80	B2	82	CB
7F	4F	7E	28
45	77	23	6A

AddRoundKey			
F4	49	52	C3
31	AC	9B	A1
B	2D	60	D6
23	3C	1C	5D

Proses tersebut dilakukan pada seluruh kolom *state* dan diulang untuk setiap *round* dari *round* ke-2 hingga *round* ke-10. Namun, perlu dicatat bahwa pada *round* ke-10, transformasi *MixColumns* tidak lagi dilakukan. Berikut adalah hasil transformasi proses enkripsi *round* ke-2 sampai dengan *round* ke-10:

Round ke-2			
45	D4	B6	56
15	32	76	1B
3C	80	0E	99
AD	3A	2E	DE

Round ke-3			
9B	79	E7	88
24	75	D8	44
3A	3C	D4	3D
32	D4	9C	BF

Round ke-4			
C8	16	EA	26
D7	FD	C7	DC
10	C2	11	1C
45	96	EA	EA

Round ke-5			
5A	83	4C	0D
D6	4E	BC	76
E6	F9	91	CF
0B	F3	1F	01

Round ke-6			
3E	B6	70	4C
A0	63	CF	37
FC	E2	AC	10
36	93	28	54

Round ke-7			
C8	BD	F9	E6
69	54	2E	55
C5	88	AE	9C
6C	16	0B	D8

Round ke-8			
09	65	19	15
D3	49	F3	4
00	68	EE	AE
88	E2	36	03

Round ke-9			
E0	1D	3B	CB
C3	6B	E6	B0
A7	F0	72	AC
1E	76	54	AA

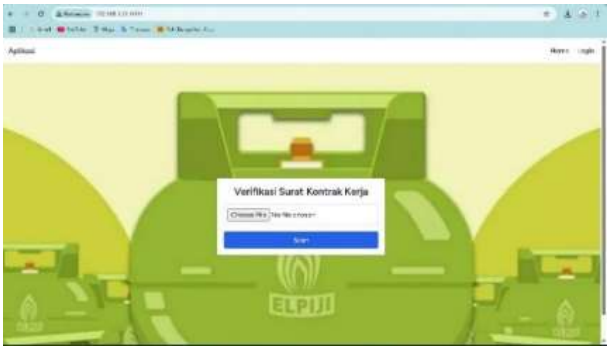
Round ke-10			
F4	01	39	57
8F	B1	28	0E
45	A0	4C	8A
88	8D	4E	3E

Hasil dari proses *AddRoundKey* pada *round* ke-10 merupakan *ciphertext* akhir, yaitu hasil akhir dari seluruh tahapan enkripsi yaitu menghasilkan *ciphertext* dalam bentuk *Hexadesimal* F48F4588 01B1A08D 39284C4E 570E8A3E. *Ciphertext* ini nantinya akan dipakai sebagai kode unik atau *primary key* dalam database, yang memiliki peran penting dalam pengidentifikasian dan pengamanan data. Dengan demikian, hasil enkripsi ini memastikan bahwa data yang tersimpan dalam sistem tetap aman dan hanya dapat diakses dengan kunci yang tepat.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

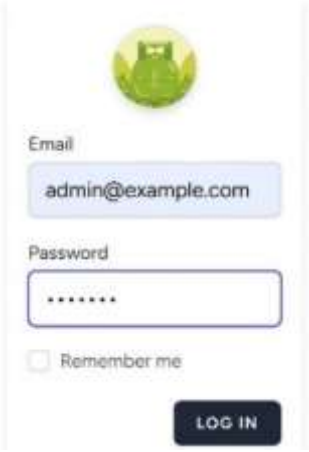
3.2 Implementasi Sistem

1. Tampilan *Menu Home*



Gambar 7. Tampilan *Menu Home*

2. Tampilan *Form Login*



Gambar 8. Tampilan *Form Login*

3. Tampilan *Form* Profile Ganti *Password*

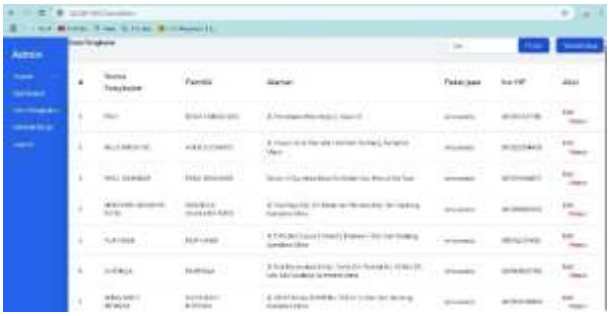
Gambar 9. Tampilan *Form* Profile Ganti *Password*

4. Tampilan *Form* Dashboard

Gambar 10. Tampilan *Form* Dashboard

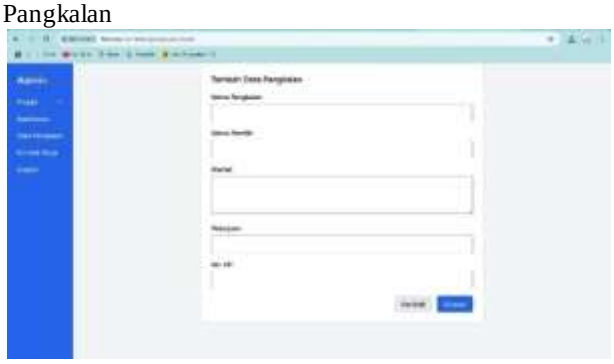
Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

5. Tampilan *Form* Data Pangkalan



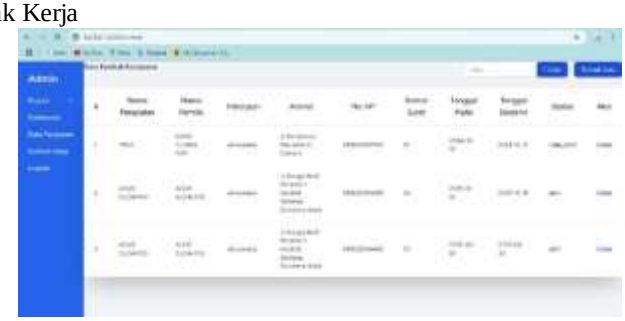
Gambar 11. Tampilan *Form* Data Pangkalan

6. Tampilan Tambah Data Pangkalan



Gambar 12. Tampilan Tambah Data Pangkalan

7. Tampilan *Form* Kontrak Kerja



Gambar 13. Tampil *Form* Kontrak Kerja

8. Tampilan Tambah Kontrak

Gambar 14. Tampil Tambah Kontrak

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 24 ; Nomor 2 ; Agustus 2025 ; Page 252-261
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

9. Tampilan Hasil Validasi

Gambar 15. Tampil Hasil Validasi

4. KESIMPULAN

Berdasarkan hasil pembahasan mengenai Implementasi Algoritma AES Pada QR-Code Untuk Validasi Keaslian Surat Kontrak Kerjasama Di PT. Cita Alfa Sasmita. Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa penerapan algoritma AES 128-bit yang dikonversi menjadi QR-Code terbukti menjadi solusi yang efektif dan efisien untuk melindungi keaslian surat kontrak kerjasama. Proses enkripsi yang rumit menghasilkan QR-Code dengan *ciphertext* yang unik dan sulit dipalsukan, sehingga mencegah manipulasi dan pemalsuan dokumen surat kontrak kerjasama. Selain meningkatkan keamanan, sistem yang dibangun secara langsung mempercepat dan menyederhanakan proses verifikasi. Penggunaan QR-Code memberikan perlindungan berlapis terhadap manipulasi dan akses tidak sah, sehingga metode ini dapat diimplementasikan sebagai standar pengamanan dokumen.

UCAPAN TERIMAKASIH

Terima kasih diucapkan kepada kedua orang tua serta keluarga dan orang tersayang yang selalu memberi motivasi, doa, dan dukungan moral maupun materi dan tidak lupa terima kasih diucapkan kepada Bapak Khairi Ibnutama S.Kom., M.Kom dan Ibu Zaimah Panjaitan S.Kom., M.Kom serta pihak-pihak yang telah mendukung dalam proses pembuatan jurnal ini yang tidak dapat disebutkan satu per satu. Kiranya jurnal ini bias memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

DAFTAR PUSTAKA

[1] K. Kartono, F. A. Sugandar, and A. Azis, "PERANAN POLRES TANGERANG SELATAN DALAM UPAYA PENCEGAHAN DAN PENANGGULANGAN KEJAHATAN (Studi Kasus Pada Polres Tangerang Selatan Tahun 2015-2017)," *Pamulang Law Rev.*, vol. 1, no. 2, p. 59, 2020, doi: 10.32493/palrev.v1i2.5327.

[2] L. Megawati, C. Wiharma, and A. Hasanudin, "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia," *J. Huk. Mimb. Justitia*, vol. 9, no. 2, p. 410, 2023, doi: 10.35194/jhmj.v9i2.3856.

[3] N. N. Tricintiya and Y. Achdiani, "PENINGKATAN PROGRESIF ANCAMAN PEMALSUAN DATA," vol. 20, no. 2, pp. 194–202, 2024.

[4] F. P. P. Perjanjian, D. A. N. Akibat, and H. Pelanggaran, "ANTARA PT REZEKI KENCANA ABADI DENGAN PANGKALAN GAS LEWANTI MARBUN SKRIPSI OLEH : YUNITA MAILANI BR . TINAMBUNAN PROGRAM STUDI ILMU HUKUM FAKULTAS HUKUM UNIVERSITAS MEDAN AREA MEDAN Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Di Faku," 2023.

[5] S. Septiani, C. L. Ramadhany, and S. A. Putri, "KOHERENSI DAN KEJELASAN KALIMAT DALAM SURAT PERJANJIAN KERJASAMA : PENDEKATAN LINGUISTIK DAN LEGAL terlibat dalam suatu kesepakatan . Dalam berbagai konteks , seperti bisnis , kelembagaan , dan memastikan kesepakatan dapat dipahami dengan benar oleh pihak," vol. 5, no. 5, pp. 6162–6167, 2024.

[6] L. Amelia, "Sistem Validasi Dokumen Digital Menggunakan Fungsi Hash," 2022.

[7] K. Antara, P. Lpg, K. G. Dan, and A. Lpg, "Dasma Maduma Sinaga , 2 Wiwik Sri Widiarty , 3 Gindo L Tobing Mahasiswa Program Studi Hukum Progam Magister Program Pascasarjana Universitas Kristen Indonesia Dosen Program Studi Hukum Progam Magister Program Pascasarjana Universitas Kristen Indonesia Ema".

[8] K. Humaira R, M. Z. Rizaldi, and A. U. Hosnah, "Analisis Yuridis Terhadap Tindak Pidana Pemalsuan Dokumen," *Indones. J. Islam. Jurisprudence, Econ. Leg. Theory*, vol. 2, no. 1, pp. 339–349, 2024, doi: 10.62976/ijijel.v2i1.461.

[9] A. U. P. Lubis, "Analisis Yuridis Pertanggungjawaban Notaris terhadap Pemalsuan Tanda Tangan oleh Penghadap dalam Akta Autentik," *J. SOMASI (Sosial Hum. Komunikasi)*, vol. 1, no. 1, pp. 116–128, 2020, doi: 10.53695/js.v1i1.36.

[10] Y. S. Kartika and W. Yulianingsih, "Jurnal Rectum," pp. 1–11, 2023.

[11] E. Suriadi, Kristiawanto, and S. T. Paparang, "Efektifitas Penerapan Tilang Elektronik Terhadap Pelanggaran Lalu Lintas Di Wilayah Hukum Polda Metro Jaya," *Policy, Law, Notary Regul. Issues*, vol. 1, no. 2, pp. 15–26, 2022, doi: 10.55047/polri.v1i2.83.

[12] D. Irawan, "Peran Kepolisian Dalam Penanganan Tindak Pidana Pengoplosan Gas Lpg (Liquified Petroleum Gas) (Studi Pada Kepolisian Daerah Sumatera Utara)," 2020.

[13] G. Assidiqih and I. F. Susilowati, "Tinjauan Yuridis Sertifikat Tanah Elektronik Sebagai Alat Bukti Kepemilikan Tanah Di Indonesia," *Novum J. Huk.*, no. Salam 2020, pp. 57–72, 2021.

[14] Nahar Mardiyantoro and M. Listiani, "Implementasi Algoritma AES Pada QR-Code Sebagai Parameter Keaslian Data Dalam Pembuatan KTA," *SATESI J. Sains Teknol. dan Sist. Inf.*, vol. 1, no. 1, pp. 26–31, 2021, doi: 10.54259/satesi.v1i1.5.

[15] A. Pariddudin and F. Syauqi, "Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 2, pp. 43–52, 2020, doi: 10.36350/jbs.v10i2.87.

[16] L. Surimi, A. M. Sajiah, N. Ransi, J. Nangi, and ..., "Rancang Bangun Sistem Validasi Surat Akademik Menggunakan QR Code dan Algoritma AES pada Siakadbeta Universitas Halu Oleo," *J. Fokus ...*, vol. 08, no. 03, pp. 164–168, 2023, [Online]. Available: https://elektroda.uho.ac.id/index.php/journal/article/view/110%0Ahttps://elektroda.uho.ac.id/index.php/journal/article/download/110/46

[17] Y. Situmeang, A. Situmorang, and P. Lumbanraja, "Implementasi Algoritma AES Rijndael Pada QR Code Untuk Validasi dan Keamanan Data Penerima Bantuan Sosial di Kelurahan Padang Bulan Selayang II," *J. Ilm. Tek. Inform.*, vol. 3, no. 2, pp. 21–30, 2023, [Online]. Available: https://ejurnal.methodist.ac.id/index.php/methotika

[18] P. Studi, T. Informatika, F. Teknik, and U. P. Batam, "Implementasi Caesar Cipher Pada Algoritma," 2022.

[19] S. D. Nurcahya, "Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 4, pp. 694–697, 2022, doi: 10.32672/jnkti.v5i4.4690.

[20] N. Oper, S. Balafif, and To'o Fathonah Al-Khaliq.Z, "Modifikasi Algoritma Kriptogafi Caesar Cipher Menjadi Algoritma Kriptografi Asimetris Dengan Metode Agile," *J. Inform. Teknol. dan Sains*, vol. 4, no. 3, pp. 179–184, 2022, doi: 10.51401/jinteks.v4i3.1920.

[21] I. Pendahuluan, "I. pendahuluan 1.1," pp. 1–5, 2021.

[22] H. A. Alfatihah, I. Fitri, and A. Andrianingsih, "Sistem Presensi dan Sertifikasi Elektronik Memanfaatkan QR Code Menggunakan Algoritma AES," *Smatika J.*, vol. 11, no. 02, pp. 70–80, 2021, doi: 10.32664/smatika.v11i02.580.

[23] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. Faizal Prianggara, and M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," *Digit. Transform. Technol.*, vol. Vol.03, no. No.1, pp. 1–10, 2023, [Online]. Available: https://jurnal.itscience.org/index.php/digitech/article/view/2293

[24] A. E. Standard *et al.*, "Enkripsi Algoritma AES (Advanced Encryption Standard)," 2001.

[25] Hamid, "Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection," *J. Akad.*, vol. 17, no. 1, pp. 8–13, [Online]. Available: https://www.ejournal.lppmunidayan.ac.id/index.php/akd

[26] Indri Widya Wulandari and Hwihanus Hwihanus, "Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan," *J. Kaji. dan Penal. Ilmu Manaj.*, vol. 1, no. 1, pp. 11–25, 2023, doi: 10.59031/jkpim.v1i1.46.

[27] R. Firdaus and R. R. Santika, "Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security," *Semin. Nas. Mhs. Fak. Teknol. Inf. Univ. Budi Luhur*, no. September, pp. 111–120, 2022.

[28] A. Rosyadi, "Dan Dekripsi Email," *Transient*, vol. 1, no. 3, pp. 2–6, 2012.

[29] J. D. Irawan and E. Adriantantri, "Pemanfaatan QR-Code Sebagai Media Promosi Toko," *J. Mnemon.*, vol. 1, no. 2, p. 57, 2018.

[30] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *J. Ilmu Komput. dan Sist. Inf.*, vol. 4, no. 2, pp. 75–85, 2021, [Online]. Available: https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181