Penerapan *Advanced Encryption Standard* pada Aplikasi *Payment Gateway* untuk Keamanan Data Transaksi Penjualan

Implementation of Advanced Encryption Standard in Payment Gateway Application for Sales Transaction Data Security

Aryanto Winata[1], Kasmawi[2*]
[1,2]Jurusan Teknik Informatika, Politeknik Negeri Bengkalis
E-mail: [1]aryantowinata77@gmail.com, [2*]kasmawi@polbeng.ac.id
Corresponding author

Abstrak

Keamanan data transaksi penjualan *membership* menjadi aspek yang sangat penting untuk melindungi privasi pelanggan dan meningkatkan kepercayaan terhadap sistem, terutama di era digital yang semakin kompleks. Penelitian ini bertujuan untuk mengembangkan aplikasi penjualan *membership* di UMKM Gym di bengkalis dengan menerapkan algoritma *Advanced Encryption Standard (AES) CBC 128-bit* dan integrasi *payment gateway*. Pengembangan aplikasi menggunakan metode *Waterfall*, mencakup identifikasi masalah, analisis sistem, desain sistem, implementasi, dan pengujian. Penerapan algoritma *AES CBC 128-bit* dilakukan untuk mengenkripsi data sensitif, seperti *payment_va_name* dan *payment_va_number*, yang tersimpan dalam basis data, memastikan keamanan dari akses tidak sah. Keamanan *AES CBC 128-bit* diuji dengan simulasi serangan *bruteforce key* menggunakan *Cryptool*. Hasil pengujian menunjukkan bahwa algoritma *AES CBC 128-bit* dapat memberikan keamanan yang kuat terhadap ancaman keamanan data transaksi penjualan *membership*, sementara *payment gateway Midtrans* memungkinkan transaksi *online* yang efisien dan aman. Penelitian ini menghasilkan aplikasi yang aman, efisien, dan terintegrasi dengan *payment gateway*, memberikan solusi yang signifikan untuk perlindungan data transaksi penjualan *membership*. Sistem ini mampu meningkatkan kepercayaan pelanggan terhadap layanan *online* yang ditawarkan oleh UMKM Gym di bengkalis.

Kata kunci: Keamanan Data Transaksi Penjualan *Membership*; Algoritma *AES*; Aplikasi Penjualan *Membership*; *Payment Gateway*; *Bruteforce Key*

Abstract

The security of membership sales transaction data is a crucial aspect to protect customer privacy and enhance trust in the system, especially in an increasingly complex digital era. This research aims to develop a membership sales application at UMKM Gym in bengkalis by implementing the Advanced Encryption Standard (AES) CBC 128-bit algorithm and integrating a payment gateway. The application development uses the Waterfall method, which includes problem identification, system analysis, system design, implementation, and testing. The AES CBC 128-bit algorithm is applied to encrypt sensitive data, such as payment_va_name and payment_va_number, stored in the database, ensuring protection from unauthorized access. The security of AES CBC 128-bit is tested through brute force key attack simulations using Cryptool. The test results show that the AES CBC 128-bit algorithm provides strong security against threats to membership sales transaction data, while the Midtrans payment gateway enables efficient and secure online transactions. This research produces an application that is secure, efficient, and integrated with a payment gateway, offering a significant solution for the protection of membership sales transaction data. This system is capable of enhancing customer trust in the online services offered by UMKM Gym in bengkalis

Keywords: Data Security in Membership Sales Transactions, AES Algorithm, Membership Sales Application, Payment Gateway, Bruteforce Key

1. PENDAHULUAN

Keamanan data transaksi penjualan menjadi salah satu hal yang sangat penting untuk dijaga dari ancaman keamanan seperti serangan *cybercrime* [1]. Perlindungan data transaksi penjualan menjadi fokus utama untuk memastikan keberlangsungan bisnis yang stabil dan kepercayaan pelanggan yang tinggi. Oleh karena itu dibutuhkan sebuah keamanan dalam melakukan proses transaksi (*payment gateway*) [2]. *Payment gateway* adalah sebuah sistem atau layanan yang memberikan otorisasi dan mengelola proses pembayaran dalam bisnis daring dan penjualan secara *online* dengan teknik pengamanan data yaitu Kriptografi [3]. Kriptografi merupakan suatu ilmu yang bertujuan untuk menciptakan suatu komunikasi yang aman sehingga tidak dapat dimengerti atau diterjemahkan oleh setiap orang kecuali orang tertentu yang dimaksud [4]. Cara kerja kriptografi adalah dengan mengubah data yang dikirim oleh pengguna, yang disebut plaintext, menjadi data terenkripsi atau ciphertext yang tidak dapat dibaca oleh pihak lain, Data tersebut hanya dapat dikembalikan ke bentuk aslinya dengan menggunakan kunci yang sesuai [5]. Dengan demikian, pengguna yang tidak memiliki hak akses tidak akan dapat mengetahui atau membaca data asli, sehingga mencegah potensi penyalahgunaan data [6]. Salah satu teknik enkripsi dalam kriptografi adalah *Advanced Encryption Standard (AES). AES* merupakan algoritma chiper yang digunakan untuk menjaga keamanan data atau informasi yang bersifat rahasia [7].

UMKM Gym yang sedang berkembang banyak menghadapi tantangan dalam mengelola transaksi penjualan *membership* secara aman. Saat ini, sistem pendataan dan transaksi pembayaran masih dilakukan secara konvensional tanpa penerapan keamanan yang memadai. Hal ini menyebabkan berbagai kendala, termasuk kebocoran dan manipulasi data transaksi penjualan *membership*, yang dapat menurunkan kepercayaan pelanggan dan mempengaruhi keberlangsungan bisnis. Keamanan data transaksi penjualan membership, terutama saat transaksi *online*, sangat penting untuk melindungi data tersebut dari kebocoran dan penyalahgunaan. Selain itu, penerapan sistem transaksi *online* diperlukan untuk meningkatkan efisiensi dan kenyamanan pelanggan. Data nomor virtual akun pengguna dan nomor rekening pemilik gym yang tercatat didalam data transaksi dapat disalahgunakan jika bocor, seperti untuk penipuan atau transaksi ilegal, yang dapat merugikan pelanggan dan bisnis UMKM Gym. Oleh karena itu, dibutuhkan sebuah teknik untuk mengamankan data penjualan membership dan sebuah teknik untuk mempermudahkan proses transaksi *online*.

Beberapa penelitian menunjukkan peningkatan keamanan data transaksi dengan Teknik kriptografi. [8] berhasil menggunakan algoritma *AES* untuk menghasilkan sebuah aplikasi bank sampah yang mampu memberikan alternatif untuk mengelola data transaksi bank sampah dengan baik karena adanya integritas data transaksi antara bank sampah dengan nasabah. [5] menghasilkan sebuah aplikasi pengamanan data dengan *AES* yang dapat membantu dalam mengamankan data penjualan. [4] berhasil menghasilkan sistem *e-marketplace* yang terhubung dengan layanan *payment gateway* yang menawarkan beragam metode pembayaran, serta menjamin keamanan data transaksi melalui penggunaan algoritma kriptografi *AES*. [9] menghasilkan sebuah aplikasi keamanan data yang mengamankan informasi data transaksi deposito dari pihak yang tidak berwenang dengan metode *RC-5*. [10] berhasil memanfaatkan algortima *AES 128 bit* untuk mengenkripsi data keuangan dengan rata-rata waktu enkripsi 1,2687 detik. [11] menggunakan *AES Mode CBC* untuk mengenkripsi dan otentikasi transmisi pesan di *ZeroMQ*. [12] berhasil menggunakan algoritma *AES 128 bit* untuk membangun sistem yang mampu mengenkripsi data penjualan dari perusahaan sehingga dapat mengamankan data dengan maksimal dan baik. [13] menghasilkan sebuah aplikasi yang menggunakan *AES* untuk mengenkripsi file dengan berbagai ekstensi.

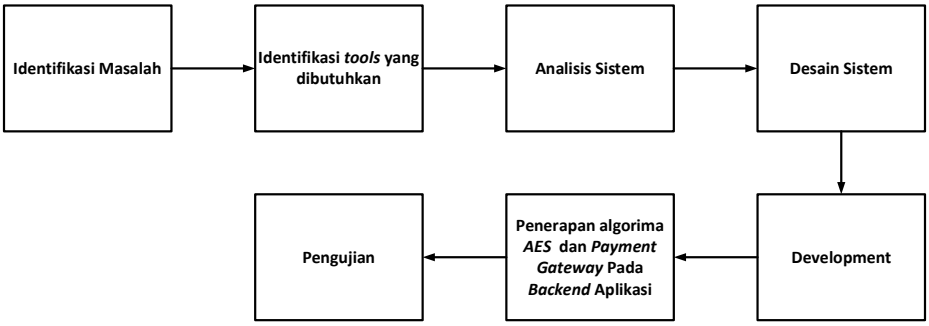
Berdasarkan latar belakang dan beberapa penelitian terkait sebelumnya sebagai acuan, penelitian ini mengembangkan aplikasi penjualan membership dengan mengimplementasikan algoritma kriptografi *AES CBC 128-bit* untuk meningkatkan keamanan data transaksi penjualan membership serta menggunakan *payment gateway* guna mempermudah proses transaksi *online*.

Perbedaan utama dalam penelitian ini adalah penerapan *AES CBC 128-bit* pada backend aplikasi dengan *IV (Initialization Vector)* yang berbeda, sehingga dapat memberikan keseimbangan optimal antara tingkat keamanan dan efisiensi performa serta mengintegrasikan *payment gateway* untuk mendukung transaksi *online*. Penerapan *IV* yang dihasilkan secara acak memastikan setiap enkripsi bersifat unik, sehingga sulit untuk dieksploitasi dan meningkatkan perlindungan terhadap serangan yang berusaha menebak pola enkripsi. Selain itu, *AES CBC 128-bit* ini memiliki kecepatan tinggi dalam proses enkripsi dan dekripsi karena membutuhkan lebih sedikit operasi matematis, menjadikannya lebih efisien dalam aplikasi yang memerlukan kecepatan transaksi. Selain itu, algoritma ini lebih hemat sumber daya, sehingga cocok untuk diterapkan pada sistem dengan keterbatasan komputasi tanpa mengorbankan keamanan data.

2. METODE PENELITIAN

2.1 Metode Penelitian

Metode penelitian yang digunakan adalah metode *Waterfall* yang bertujuan untuk mengembangkan aplikasi penjualan membership. Metode untuk mencapai tujuan penelitian dijabarkan pada Diagram blok berikut.



Gambar 1 Metode *Waterfall* Pencapaian Tujuan Penelitian

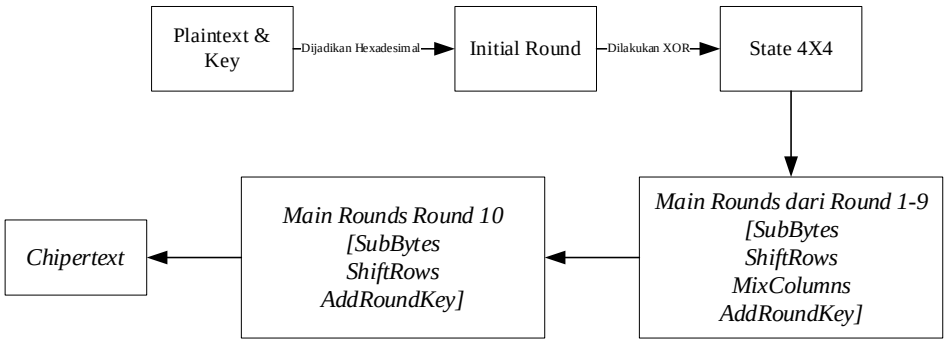
Gambar 1 merupakan prosedur penelitian untuk melakukan pengembangan aplikasi penjualan membership untuk mencapai tujuan penelitian. Berikut ini adalah prosedur penelitian yang meliputi:

1. Identifikasi Masalah: Melakukan identifikasi masalah dan referensi terhadap sistem penjualan *membership* UMKM Gym.
2. Identifikasi *tools* yang dibutuhkan: Melakukan penyiapan tools yang dibutuhkan.
3. Analisis Sistem: Melakukan analisa terhadap sistem penjualan *membership* UMKM Gym dan akan dibangun sistem berdasarkan kebutuhan dari UMKM Gym.
4. Desain Sistem: Melakukan perancangan aplikasi *membership* yang dimulai dari pembuatan usulan sistem penjualan *membership*, rancangan *user interface*, rancangan database dan penerapan keamanan data transaksi penjualan.
5. Pengembangan: Melakukan pengembangan aplikasi yang dimulai dari pengkodean yang sesuai dengan desain sistem menggunakan *Framework Flutter*.
6. Penerapan *AES* dan *Payment Gateway*: Melakukan penerapan algoritma *Advanced Encryption Standard CBC 128-bit* dan *Payment Gateway* pada *backend* aplikasi penjualan *membership* untuk keamanan data transaksi penjualan *membership* dan proses transaksi *online* UMKM Gym.
7. Pengujian: Melakukan pengujian untuk mengetahui apakah penerapan *AES CBC 128-bit* dan *Payment Gateway* pada aplikasi penjualan *membership* dapat berjalan dengan lancar dan apakah data transaksi penjualan *membership* aman dari simulasi serangan *bruteforce*.

2.2 *Advanced Encryption Standard (AES)*

Advanced Encryption Standard (AES) merupakan algoritma enkripsi yang dirancang untuk menjaga keamanan data atau informasi yang bersifat sensitif. *AES* mendukung beberapa ukuran kunci, yaitu *128 bit, 192 bit*, dan *256 bit*. Variasi dalam ukuran kunci ini akan memengaruhi jumlah putaran yang diterapkan selama proses enkripsi dan dekripsi data. Berikut ini adalah langkah-langkah untuk menerapkan enkripsi *AES*:

1. Melakukan Ekspansi Kunci yaitu mengubah *plaintext* dan *key* menjadi heksadesimal.
2. Melakukan *Initial Round Key* yaitu melakukan *XOR* antara *state 4x4 plaintext* dan *state 4x4 key*.
3. Melakukan *Main Round* dari *Round* 1 sampai 9 yang terdiri dari:
   - *SubBytes* yaitu melakukan substitusi *byte* dengan tabel substitusi (*S-Box*).
   - *ShiftRows* yaitu melakukan permutasi *byte-byte* dari kolom yang berbeda.
   - *MixColumns* yaitu mengacak data di masing-masing kolom.
   - *AddRoundKey* yaitu melakukan *XOR* data dengan *key*.
4. Melakukan *Final Round* yaitu proses putaran terakhir tanpa *MixColumns* [13].



Gambar 2 Alur Enkripsi AES

Tabel 1 Ukuran Kunci AES

Tipe	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.3 *Payment Gateway*

Payment gateway adalah sistem pembayaran digital yang berperan dalam memproses dan memvalidasi informasi transaksi sesuai dengan ketentuan yang ditetapkan oleh penyedia layanan [2]. Penggunaan payment gateway dalam aplikasi memberikan berbagai jaminan dari penyedia layanan, termasuk kecepatan dan kepraktisan dalam sistem pembayarannya. Transaksi elektronik yang di lakukan akan menjadi lebih aman, dan efisiensi aliran kas meningkat dengan pencatatan yang lebih baik, biaya transaksi lebih ekonomis, dan informasi pelanggan terlindungi dengan baik [4].

2.4 Aplikasi *Mobile*

Aplikasi *mobile*, atau yang sering disebut *Mobile Apps*, adalah perangkat lunak yang dirancang khusus untuk berfungsi di perangkat mobile dan dapat berjalan secara mandiri pada sistem operasi yang sesuai. Aplikasi ini umumnya memungkinkan pengguna untuk mengakses layanan internet yang sebelumnya hanya dapat diakses melalui *PC* atau *notebook*. Oleh karena itu, aplikasi *mobile* mempermudah pengguna dalam mengakses layanan internet dari jarak jauh menggunakan perangkat pribadi mereka [9].

3. HASIL DAN PEMBAHASAN

3.1 Hasil Penerapan *AES* dan *Payment Gateway*

Pada tahapan ini, dilakukan penerapan algoritma *AES CBC 128-bit* dengan memanfaatkan *IV (Initialization Vector*) yang dihasilkan secara acak untuk memastikan setiap enkripsi unik dan meningkatkan keamanan data transaksi penjualan membership dan *payment gateway* pada *backend* aplikasi penjualan *membership* untuk meningkatkan keamanan data transaksi penjualan. Berikut ini adalah langkah-langkah untuk melakukan enkripsi *AES 128-bit* :

1. Mengubah *plaintext* dan *key* ke dalam *hexadecimal*

Mengubah *plaintext* dan *key* ke dalam *hexadesimal* berdasarkan tabel *ASCII*.

Tabel 2 Pengubahan *Plaintext* dan *Key* ke Hexadesimal

Plaintext															
6	9	5	7	7	6	9	8	3	1	7	4	1	8	2	7
36	39	35	37	37	36	39	38	33	31	37	34	31	38	32	37
Key															
K	R	I	P	T	O	G	R	A	F	I		A	E	S	S
4B	52	49	50	54	4F	47	52	41	46	49	20	41	45	53	53

1*6 byte* dari *plaintext* dan *key* yang telah diubah ke *hexadecimal* disusun menjadi *state 4x4*.

Tabel 3 *State 4x4 Plaintext* dan *Key*

Plaintext			
36	37	33	31
39	36	31	38
35	39	37	32
37	38	34	37
Key			
4B	54	41	41
52	4F	46	45
49	47	49	53
50	52	20	53

2. Melakukan *Initial Round*.

Melakukan *XOR* antara *State 4x4 Plaintext* dan *State 4x4 Key*.

Tabel 4 Intial Round

State 4x4 Plaintext			
36	37	33	31
39	36	31	38
35	39	37	32
37	38	34	37
State 4x4 Key			
4B	54	41	41

52	4F	46	45
49	47	49	53
50	52	20	53
Initial Round			
7D	63	72	70
6B	79	77	7D
7C	7E	7E	61
67	6A	14	64

2. Melakukan pembangkitan kunci atau proses *Add Round Key*.

Tabel 5 *Add Round Key*

Round	WI-4	WI-3	WI-2	WI-1
0	4B	54	41	41
	52	4F	46	45
	49	47	49	53
	50	52	20	53
1	24	70	31	70
	BF	F0	B6	F3
	A4	E3	AA	F9
	D3	81	A1	F2
2	2B	5B	6A	1A
	26	D6	60	93
	2D	CE	64	9D
	82	03	A2	50
3	F3	A8	C2	D8
	78	AE	CE	5D
	7E	B0	D4	49
	20	23	81	D1
4	B7	1F	DD	05
	43	ED	23	7E
	40	F0	24	6D
	41	62	E3	32
5	54	4B	96	93
	7F	92	B1	CF
	63	93	B7	DA
	2A	48	AB	99
6	FE	B5	23	B0
	28	BA	0B	C4
	8D	1E	A9	73
	F6	BE	15	8C
7	A2	17	34	84
	A7	1D	16	D2
	E9	F7	5E	2D
	11	AF	BA	36
8	97	80	B4	30
	7F	62	74	A6
	EC	1B	45	68
	4E	E1	5B	6D
9	A8	28	9C	AC
	3A	58	2C	8A
	D0	CB	8E	E6
	4A	AB	F0	9D
10	E0	C8	54	F8
	B4	EC	C0	4A
	8E	45	CB	2D
	DB	70	80	1D

3. Melakukan Enkripsi.

Melakukan enkripsi pada semua *round* yaitu melakukan *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey* pada semua *Round*.

Tabel 6 Proses Enkripsi

Round	WI-4	WI-3	WI-2	WI-1
1	49	46	F5	64
	7F	30	28	01
	54	31	24	5D
	01	0C	55	D2
2	49	46	F5	64
	7F	30	28	01
	54	31	24	5D
	01	0C	55	D2
3	46	ED	5A	CC
	90	1A	74	3D
	05	0E	09	3A
	52	6A	54	D0
4	1A	B7	0C	D1
	73	1D	E7	01
	30	24	4A	B7
	D3	0B	33	D0
5	1A	B7	0C	D1
	73	1D	E7	01
	30	24	4A	B7
	D3	0B	33	D0
6	1A	01	D3	64
	90	D0	D4	01
	05	24	64	B7
	D3	0B	33	D0
7	0D	A1	C4	48
	4F	D0	D4	6D
	D0	D4	6D	B6
	D4	6D	B6	D0
8	3A	36	6C	D4
	39	D0	D4	6D
	D0	D4	6D	B6
	D4	6D	B6	D0
9	3A	36	6C	D4
	39	D0	D4	6D
	D0	D4	6D	B6
	D4	6D	B6	D0
10	24	04	29	4D
	1F	2D	05	1A
	79	6D	4D	0C
	4D	6D	B6	D0

4. Hasil Enkripsi.

Melakukan pengubahan Hexadesimal Hasil *Round 10* ke *Chipertext* berdasarkan tabel *ASCII*.

Tabel 7 Hasil Enkripsi Akhir

$	.	)	M
.	-	.	.
y	m	M	.
M	m	.	.

Berikut ini adalah hasil penerapan *AES CBC 128-bit* pada *database* sistem penjualan *membership*, khususnya dibagian tabel *Order* kolom *payment_va_name* dan *payment_va_number*.

payment_va_name	payment_va_number
SCtpZ3dpM1V5bG5Tdjc4TXRaaGxNQT09OjrO8fBAb0IYwiqWG3Ns7v6h	Si95Q1RuTWI4eEdnRDMvMjBDQmU2ZWRPZkVETHIyMENwYmErMHZVVmox…
c1NpM5tEb0ZRVTNIL0ZEOTV3MnBDUT09Ojq1H5SoO8wQeri/GUx7rqQX	dmtmOX1reGg4cmY3cTBoTmUxQW1KWmpXckdmT08yY1Bvd8RNVYzhIWlJ4…
ZE9LUCtuZjFOS1crV1dDRkVTVWtwUT09OjpZXnR34hLx2dnOIwyXO+EQ	YU15STN3b1ViQktCajNEUnlDSHZrZEpVTGMvbUsyS1ZIam1jZjdKSEhG…
VkpnckdjcmJMcWZ1eDd2c2lFSHNGdz09OjpqmIlyzxMqAueAD2u7Lt6K	dk9KOGNmNHNoWGpCSkQrcTFwelV6OCtTWlJPam53am94dmhVRzAvVFpR…
amhLarRIa0RtanFjV3A3OGpyVWJHZz09OjpEeUqPzakUgDqmGSinhEJP	NWh5K2c1Y1dyYms4Rmt3YWdzVkw2dlpMemZyUmtidlhvQUk1RCtk001X…
cjBsQ1luaG8zMWNITzZyaDZKckVjdz09OjqSoU7haMap1KFUP1ZG6de7	aFA3YVR6VzFPZk1uUEwvb2xKcE3IQkxVY2VMT1RLZnQ4aTWCQnJaSjZy…

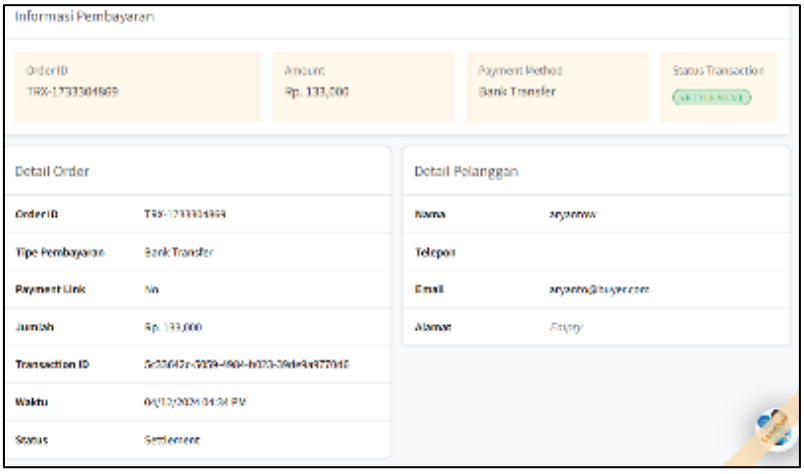
Gambar 3 Hasil Enkripsi *AES CBC 128-bit*

Selanjutnya adalah melakukan penerapan *payment gateway* pada *backend* aplikasi penjualan *membership*. Berikut ini adalah *source code* untuk menerapkan *payment gateway*.

```
<?php
namespace App\Services\Midtrans;
use Midtrans\CoreApi;
class CreateVaService extends Midtrans
{
    protected $order;
    public function __construct($order)
    {
        parent::__construct();
        $this->order = $order;
    }
    public function getVA()
    {
        $itemDetails = [];
        foreach ($this->order->orderItems as $orderItem) {
            $itemDetails[] = [
                'id' => $orderItem->product_id,
                //price string double to integer
                'price' => intval($orderItem->price),
                'quantity' => $orderItem->quantity,
                'name' => $orderItem->product->name,
            ];
        }
        $itemDetails[] = [
            'id' => 'SHIPPING_COST',
            'price' => $this->order->shipping_price,
            'quantity' => 1,
            'name' => 'SHIPPING_COST',
```

```
        ];
        $params = [
            'payment_type' => 'bank_transfer',
            'transaction_details' => [
                'order_id' => $this->order->transaction_number,
                'gross_amount' => $this->order->grand_total,
            ],
            'item_details' => $itemDetails,
            'customer_details' => [
                'first_name' => $this->order->user->name,
                'email' => $this->order->user->email
            ],
            'bank_transfer' => [
                'bank' => $this->order->payment_va_name,
            ],
        ];
        $response = CoreApi::charge($params);
        return $response;
    }
}
```

Berdasarkan *source code* diatas , dapat dijelaskan bahwa Kelas ini menerima objek order yang mengandung rincian produk, kuantitas, dan data pelanggan. Metode *getVA()* berfungsi mencocokkan informasi item pesanan, termasuk harga satuan, jumlah item, serta biaya pengiriman, lalu merangkumnya dalam struktur data yang sesuai dengan spesifikasi *API Midtrans*. Struktur data ini, yang meliputi ID transaksi unik, total tagihan, dan profil pembeli, kemudian dikirimkan ke *API Midtrans* melalui metode *CoreApi::charge()* untuk menghasilkan *virtual account (VA)*. Respons dari *API Midtrans*, yang berisi status transaksi dan informasi *VA*, akan dikembalikan. Penerapan fungsi ini memungkinkan aplikasi penjualan *membership* dapat melakukan pembayaran secara *online* dengan menggunakan beberapa metode yang disediakan di *Payment Gateway Midtrans.*



Gambar 4 Hasil Penerapan *Payment Gateway*

3.2 Hasil Pengujian Keamanan *AES CBC 128-bit*

Pada pengujian yang dilakukan dengan menggunakan 21 data transaksi penjualan *membership* dari kolom *payment_va_name* dan *payment_va_number* untuk menguji kekuatan hasil enkripsi *AES CBC 128-bit* terhadap simulasi serangan *Bruteforce Key* dengan menggunakan

tool Cryptool. Hasil dari pengujian ini adalah tidak ada satu pun data transaksi penjualan *membership* yang berhasil didekripsi.

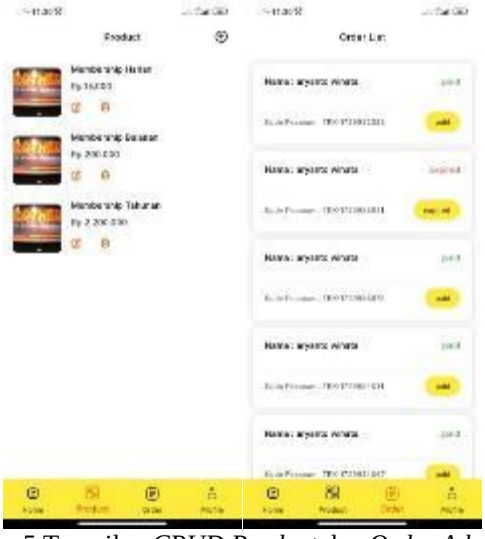
Tabel 8 Hasil Pengujian Keamanan *AES CBC 128-bit*

No	Payment_va_name	Payment_va_number	Hasil Pengujian
1	VnN4dkVXd1RFQ1J4UXJGM	ZHJpK0IrWWVaWW1PZXZKWW9Y	**Tidak Berhasil**
2	NUlOT0JwRkJldlkrRUFyY0t	TkdON0tOQVlKbTlKdjB4Vi9xTitLRX	**Tidak Berhasil**
3	NVhNcEx1ZnlCaDI0TXJYdG	MnBnYVNnWkxnREpyNHU4QkFSdCt	**Tidak Berhasil**
4	REJvTkZrQTR2dDI0bUp4Zl	QkNtN0dvUlRHSFJFck10MmwyelBLd	**Tidak Berhasil**
5	SmtSR3ZDQkx5cUM1bUZmQ	aUtiVk8rYm9ibSt6QXhYMkw2R3l	**Tidak Berhasil**
6	Rk5BRFNiZDU4NjhhamVxblk	NmM3dEpVOHUzTHVaUlR3NkFFRH	**Tidak Berhasil**
7	NlZJWGpxR0Evano3S0JvMX	TjlFTXdmQnlnQS9wNzF1UlBlY3poaU	**Tidak Berhasil**
8	ZXR1UlB4WWhDMnBBZktv	ZjFoaXVYR3EzV092elFHaE1BN09xL0	**Tidak Berhasil**
9	RmE1dUcxU1FnOHVQNS9JT	N0tjZzRRREdhTFE5Z3l6d3NjNWdHb	**Tidak Berhasil**
10	eTBrcllTU3d5T29RZGEwNmo	SCtzSVpzRmlHemxUQUpSLzNzcGZK	**Tidak Berhasil**
11	bTFOMVBCVWdYbHFON	eXhheWxzZXdNQUFjeDdVZXd4cWM	**Tidak Berhasil**
12	T2o4UDdZTnlnenZDSTlQeGZ	K0p1MTFqYjR3VW9XS3BZMTJ5W	**Tidak Berhasil**
13	eWtLZGhhQUtEVGpnaE13cV	TnNXQWNwTDRjdHVhZFg0KzhkU	**Tidak Berhasil**
14	R0xZKysxUUhZNU1XcU9xVj	TDlCVXBXZDVxZzNCb1FZVklYY2R	**Tidak Berhasil**
15	Z0NBa1NDa3BjK1plOG9sa3l	L0NJbDFwL2VWdnFwNEllM0NlUk	**Tidak Berhasil**
16	MmZPaWRNRjZnV045K05Sc	RzVNb1FYVm8wbDJIV1pxTUN0TT	**Tidak Berhasil**
17	aVpxeDJpakJWaW44UmpjM	ckZPbWtZWm1uWjZ0MS9oUXdpOU	**Tidak Berhasil**
18	cjlQaG1xOFRaMzJmU0xjWX	a2F3N2NNRWVHamFrdlhFM0I4aUJ	**Tidak Berhasil**
19	bUljcFVlZU5yZGtlNVRvMjI	WGYrWU03RUR4UlRzRnY2MklBZW	**Tidak Berhasil**
20	QUVKdjl0MkhuUjF0NXUyN	YWhFclJCWEZZZzMwMWo2WC91S2N	**Tidak Berhasil**
21	SlhxTURsUGZCdwdd	dzdxN1B2TWJZdndKY0xwblc3RCt3	**Tidak Berhasil**

3.3 Hasil Perancangan *User Interface*

1. Hasil Perancangan *UI Admin.*

Perancangan *UI Admin* ini bertujuan untuk mempermudahkan *admin* untuk melakukan pengolahan data ,penambahan produk, dan perhitungan jumlah order. Berikut ini adalah hasil rancangan *UI admin.*

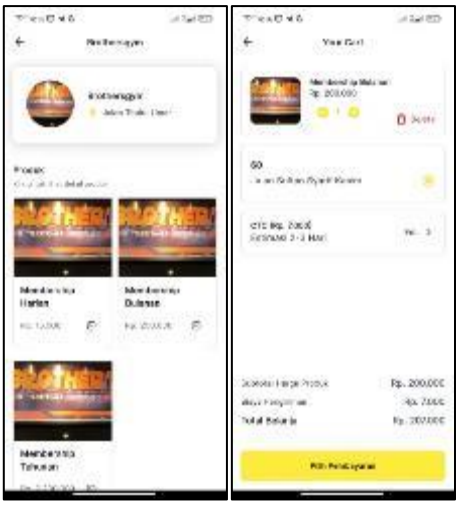


Gambar 5 Tampilan *CRUD Product* dan *Order Admin*

Gambar 4 merupakan hasil perancangan *CRUD Product* dan *Order Admin*, dimana admin dapat melakukan penambahan produk baru dan melihat order yang masuk beserta dengan jumlah ordernya.

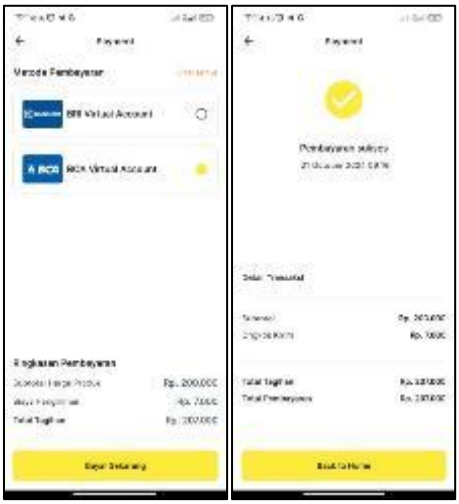
2. Hasil Perancangan *UI User.*

Pada aplikasi penjualan *membership, user* dapat melakukan pembelian produk, memilih metode pembayaran, melakukan pembayaran dan mendapatkan kuitansi. Berikut ini adalah hasil perancangan *UI User*.



Gambar 6 Tampilan *UI* Menu Produk dan Menu Pembayaran

Gambar 5 menunjukkan bahwa tampilan menu produk dan menu pembayaran, sehingga *user* bisa melakukan pemilihan produk dan melihat total harga dari produk yang dibeli serta melakukan pembayaran.



Gambar 7 Tampilan *UI* Menu Metode Pembayaran dan Kuitansi

Gambar 6 menunjukkan bahwa tampilan menu metode pembayaran dan kuitansi, sehingga *user* bisa melakukan pemilihan metode pembayaran dan mendapatkan kuitansi setelah selesai melakukan pembayaran.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan, dapat disimpulkan bahwa algoritma *AES CBC 128-bit* dan *payment gateway* dapat diterapkan pada bagian *backend* aplikasi penjualan *membership*, memungkinkan pengguna melakukan pembayaran *online* dengan mudah dan aman. Enkripsi *AES CBC 128-bit* memastikan data transaksi dienkripsi sebelum disimpan ke dalam *database*, dan pengujian dengan simulasi serangan *bruteforce key* menunjukkan tingkat keamanan yang tinggi. Aplikasi ini dikembangkan menggunakan metode *waterfall* yang terstruktur. Untuk pengembangan lebih lanjut, disarankan agar enkripsi data tidak hanya diterapkan pada tabel *order*, tetapi juga pada tabel-tabel lain di database untuk meningkatkan keamanan keseluruhan.

Selain itu, penambahan fitur seperti pencarian atau laporan otomatis dapat mempermudah akses dan pengelolaan data bagi pengguna dan admin. Metode enkripsi juga dapat ditingkatkan dengan menggunakan algoritma *AES 256-bit* atau algoritma lainnya untuk meningkatkan keamanan data.

DAFTAR PUSTAKA

[1] R. Ayyadurai, "Transaction Security in E-Commerce : Big Data Analysis in Cloud Environments".

[2] A. Fian, P. Sokibi, and L. Magdalena, "Penerapan Payment Gateway pada Aplikasi Marketplace Waroeng Mahasiswa Menggunakan Midtrans," *J. Inform. Univ. Pamulang*, vol. 5, no. 3, p. 387, 2020, doi: 10.32493/informatika.v5i3.6719.

[3] S. K, Ankur singh, Gulshan Kumar, Vrindwan Kumar, and Mahesh T R, "Online Service Booking Platform with Payment Integration," *Int. J. Inf. Technol. Res. Appl.*, vol. 2, no. 2, pp. 41–46, 2023, doi: 10.59461/ijitra.v2i2.54.

[4] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *J. Comput. Syst. Informatics*, vol. 4, no. 1, pp. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.

[5] A. Putra Ramadani Tarigan, P. S. Ramadhan, and K. Ibnutama, "Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard)," *J. Cyber Tech*, vol. 5, no. 1, p. 26, 2023, doi: 10.53513/jct.v5i1.7851.

[6] M. A. Hidayah, N. Budi Nugoho, and M. Iswan Perangin-Angin, "Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan P ada PT.Mestika Sakti," *J. CyberTech*, vol. x. No.x, no. x, 2020.

[7] Y. Jiang, G. Sun, and T. Feng, "Research on Data Transaction Security Based on Blockchain," *Inf.*, vol. 13, no. 11, pp. 1–17, 2022, doi: 10.3390/info13110532.

[8] A. P. Nugroho and H. B. Suseno, "Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES," *"QUERY J. Sist. Inf. Keamanan Data Transaksi Nasabah Pada Apl. Bank Sampah Berbas. Web Menggunakan Algoritm. AES.,"* vol. 04, no. April, pp. 9–17, 2020, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/query/article/view/8007/3720

[9] A. Utama and R. F. Siahaan, "Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada Easy Tronik dengan Metode RC-5," *J. Ilmu Komput. dan Sist. Inf.*, vol. 3, no. 3, pp. 29–39, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/86

[10] A. Ramadan and Painem, "Pengamanan Data Keuangan Menggunakan Algoritma Advanced Encryption Standard 128 Pada Pt. Charise Deo Indonesia," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 49–57, 2022.

[11] I Made Sukarsa, I Made Rama Pradana, and Putu Wira Buana, "Implementasi Enkripsi dan Otentikasi Transmisi Data ZeroMQ Menggunakan Advanced Encryption Standard," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, pp. 1149–1156, 2020, doi: 10.29207/resti.v4i6.2581.

[12] F. A. Sitorus, N. B. Nugroho, and U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," *J. CyberTech*, no. x, pp. 1–15, 2020, [Online]. Available: https://ojs.trigunadharma.ac.id/

[13] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 182, 2020, doi: 10.30865/jurikom.v7i1.1960.