

## **Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace**

**Muhammad Rian Andriyanto, Pristi Sukmasetya\***

Fakultas Teknik, Teknik Informatika, Universitas Muhammadiyah Magelang, Magelang, Indonesia

Email: <sup>1</sup>hiddenfoxe01@gmail.com, <sup>2</sup>pristi.sukmasetya@ummggl.ac.id

Email Penulis Korespondensi: <sup>2</sup>pristi.sukmasetya@ummggl.ac.id

Submitted: 31/10/2022; Accepted: 30/11/2022; Published: 30/11/2022

**Abstrak**—Desa Sriwedari dikenal sebagai penghasil bibit tanaman dan buah-buahan yang unggul di wilayah Kecamatan Salaman. Toko Bibit Sriwedari adalah salah satu bentuk usaha dari pemerintah desa yang menjual berbagai macam bibit tanaman dan buah-buahan hasil dari pembibitan oleh masyarakat setempat. Namun, dalam penerapannya sistem penjualan dan transaksinya masih menggunakan cara yang terbilang konvensional. Dengan membuka toko secara *offline* dan pemasaran produk melalui jejaring sosial media membuat Toko Bibit Sriwedari kurang memiliki pelanggan tetap. Belum lagi resiko penipuan dari pelanggan yang memesan bibit melalui sosial media menjadi kekhawatiran tersendiri bagi penjual. Oleh karena itu, penelitian ini dilakukan dengan maksud untuk menjawab permasalahan yang ada di atas dengan membuat sebuah sistem *e-marketplace* berupa toko *online* yang akan terintegrasi dengan *payment gateway* yang memiliki berbagai metode pembayaran online. Di samping itu juga akan diterapkan keamanan data pada sistem pembayaran menggunakan algoritma kriptografi *Advanced Encryption Standard (AES)* yang berfungsi untuk mengenkripsi data transaksi pembayaran agar rekaman data yang tersimpan di dalam *database* tidak mudah dibaca dan menghindari penyalahgunaan data oleh pihak yang tidak memiliki hak akses. Metode yang digunakan dalam mengembangkan sistem ini adalah *Rapid Application Development (RAD)*. Metode ini sangat cocok diterapkan dalam pengembangan perangkat lunak dengan sumber daya yang minim sehingga dapat mempercepat proses iterasi setiap tahapan pengembangan dan tetap memperhatikan masukan dari calon pengguna sistem. Hasil dari penelitian ini berupa sistem *e-marketplace* terintegrasi dengan layanan *payment gateway* yang memiliki berbagai macam metode pembayaran dengan keamanan data transaksi menggunakan algoritma kriptografi AES.

**Kata Kunci:** Pasar Elektronik; Gerbang Pembayaran; Enkripsi; Kriptografi; Algoritma AES-256

**Abstract**—Sriwedari Village known as a producer of superior plant seeds and fruits in the Salaman District area. The Sriwedari Seed Shop is a form of business from the village government that sells various kinds of plant seeds and fruits from nurseries by the local community. However, in its application the sales and transaction system still uses a fairly conventional method. By opening an offline store and marketing products through social media networks, the Sriwedari Seed Shop has less regular customers. Not to mention the risk of fraud from customers who order seeds through social media is a concern for sellers. Therefore, this research was conducted with the intention of answering the problems above by creating an e-marketplace system in the form of an online store that will be integrated with a payment gateway that has various online payment methods. In addition, data security will also be applied to the payment system using the Advanced Encryption Standard (AES) cryptographic algorithm which functions to encrypt payment transaction data so that data records stored in the database are not easy to read and prevent misuse of data by parties who do not have access rights. The method used in developing this system is Rapid Application Development (RAD). This method is very suitable to be applied in software development with minimal resources so that it can speed up the iteration process at each stage of development while still paying attention to input from potential system users. The results of this research are an integrated e-marketplace system with payment gateway services that have various payment methods with transaction data security using the AES cryptographic algorithm.

**Keywords:** E-Marketplace; Payment Gateway; Encrypt; Cryptography; AES-256 Algorithm

## **1. PENDAHULUAN**

Desa Sriwedari adalah bagian dari wilayah Kecamatan Salaman yang didominasi oleh sektor pembibitan tanaman dan buah-buahan. Dengan keragaman pembibitan tanaman dan buah-buahan menjadikan Desa Sriwedari dikenal sebagai tempat penghasil bibit unggulan. Toko Bibit Sriwedari adalah salah satu bentuk usaha dari pemerintah desa yang menjual berbagai bibit tanaman dan buah-buahan hasil dari pembibitan oleh masyarakat setempat. Akan tetapi dengan banyaknya pebisnis yang mulai menjual bibit tanaman mengakibatkan persaingan bisnis jual beli tanaman menjadi sangat ketat [1].

Sistem penjualan Toko Bibit Sriwedari sendiri masih dilakukan secara manual yaitu mengunggah katalog produk melalui media sosial *facebook* dan transaksi dilakukan dengan cara transfer bank kemudian konfirmasi bukti pembayaran kepada admin melalui *whatsapp*. Hal ini menyebabkan lingkup penjualan bibit masih kecil dan kurang adanya pelanggan tetap [2]. Untuk itu maka perlu dibangun sebuah sistem yang dapat menangani proses jual beli secara otomatis dan transaksi pembayaran yang aman.

Belanja secara *online* menjadi solusi banyak orang untuk melakukan transaksi jual beli [3]. *E-marketplace* merupakan sebuah peluang besar untuk mengatasi terbatasnya akses teknologi informasi dikarenakan modal yang kurang dan tenaga ahli yang tidak memadai [4]. Dalam penggunaannya *e-marketplace* erat kaitannya dengan metode pembayaran *online* dengan memanfaatkan *payment gateway* untuk mempermudah dalam bertransaksi [5]. Dalam penerapannya, *e-marketplace* sangat diperlukan pengamanan data mengingat banyak *cyber crime* yang mengincar *website* dengan lalu lintas pengguna yang tinggi [6].

*Cyber crime* adalah kejahatan dengan memanfaatkan teknologi komputer khususnya internet sebagai alat utama dalam menjalankan aksinya [7]. Data yang bersifat sensitif perlu diamankan salah satunya adalah data transaksi pengguna. Data transaksi berupa informasi pembayaran yang sifatnya rahasia dan perlu diamankan untuk menghindari penyalahgunaan data. Untuk itu diperlukan sebuah algoritma yang dapat menyandikan data yang bersifat sensitif agar pengguna yang tidak memiliki hak akses tidak dapat mengetahui isi dari data tersebut [8].

*Advanced Encryption Standard* (AES) adalah salah satu algoritma kriptografi yang berfungsi untuk melakukan proses mengubah data asli menjadi data tersandi (*encrypt*) dan begitu juga sebaliknya (*decrypt*) dari sebuah informasi atau data [9],[7],[10]. Dibutuhkan sebuah kunci yang menjamin data tersebut terlindungi dalam kedua proses diatas. Kunci tersebut berfungsi untuk mengamankan tiap proses perubahan data [10]. Algoritma AES menggunakan kunci simetrik yaitu kunci yang sama setiap melakukan proses enkripsi maupun deskripsi.

Angger Wibowo telah melakukan penelitian tentang pembangunan aplikasi *e-commerce* pemasaran batik pada Toko Batik Rifqi menggunakan PHP dan MySQL dengan metode pengembangan SDLC (*System Development Life Cycle*) untuk memudahkan pembeli dalam membeli batik di Toko Batik Rifqi melalui media *internet*. Dengan adanya *website* ini dapat mempermudah pemasaran produk sehingga jangkauan konsumen menjadi lebih luas [11]. Selanjutnya I G P Fajar Pranadi Sudhana telah melakukan penelitian tentang pengembangan sistem pembayaran untuk Desa Wisata Tri Eka Buana dengan *online payment*. Mengintegrasikan *website* Desa Wisata Tri Eka Buana dengan salah satu layanan *payment gateway* dapat mempermudah pelanggan dalam melakukan pembayaran [12].

Salma Dola Silalahi telah melakukan penelitian tentang penerapan algoritma kriptografi Word Auto Key Encryption untuk pengamanan soal ujian berbasis komputer menyimpulkan bahwa setelah diterapkan algoritma WAKE pada soal ujian berbasis computer, data tersebut dapat terenkripsi dengan baik sehingga dapat meminimalisir kebocoran soal [13]. Selanjutnya Muhammad Arif Hidayah telah melakukan penelitian tentang penerapan kriptografi menggunakan algoritma AES untuk keamanan data penjualan pada PT. Mestika Sakti Medan menyimpulkan bahwa setelah diterapkan algoritma AES pada data penjualan yang cukup banyak di PT. Mestika Sakti Medan, data tersebut dapat terenkripsi menjadi *chipertext* sehingga dapat mengurangi resiko penyalahgunaan data [14].

Aditya Puji Nugroho telah melakukan penelitian tentang keamanan data transaksi nasabah pada aplikasi bank sampah berbasis web menggunakan algoritma AES menyimpulkan bahwa algoritma AES dapat mengamankan data transaksi nasabah dengan efektif dikarenakan sulit untuk ditembus dengan serangan *brute force* dan memerlukan waktu yang sangat lama untuk menemukan kunci yang benar sehingga dapat memberikan alternatif untuk mengelola data bank sampah dengan baik karena adanya integritas data antara bank sampah dengan nasabah [15].

Berdasarkan penelitian sebelumnya, dalam penelitian ini penulis akan berfokus pada bagaimana membangun sistem *e-marketplace* bbit sriwedari dan mengimplementasikan algoritma kriptografi *Advanced Encryption Standard* (AES) dengan ukuran kunci 256 bit untuk keamanan data transaksi pengguna. Sehingga dengan adanya penelitian ini bertujuan menciptakan sebuah sistem *e-marketplace* untuk menangani proses transaksi jual beli bibit buah dan tanaman di Desa Sriwedari agar lebih efektif dan efisien. Di samping itu juga tetap memperhatikan sisi keamanan data pengguna agar tetap terlindungi dari penyalahgunaan data oleh pihak yang tidak memiliki hak akses. Hasil dari penelitian ini nantinya adalah data transaksi pembayaran yang tersimpan di dalam *database* berupa data tersandi (*chipertext*) yaitu hasil dari proses enkripsi data asli yang telah di input oleh pengguna (*plaintext*).

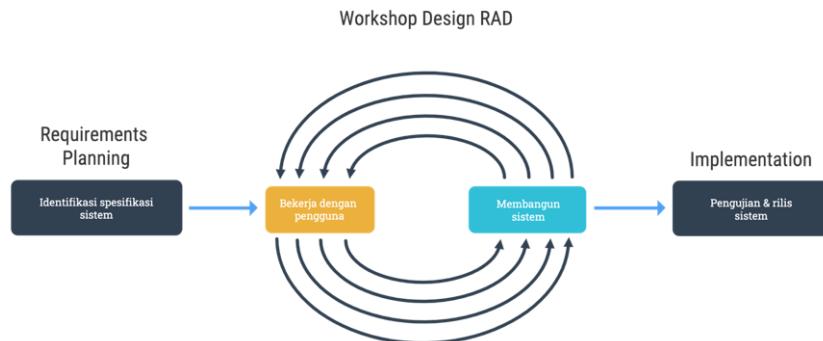
## 2. METODOLOGI PENELITIAN

### 2.1 Tahapan Penelitian

Pada penelitian ini penulis menggunakan metode pengumpulan data dan metode pengembangan sistem. Tiga tahapan dalam metode pengumpulan data yaitu, observasi, wawancara dan studi pustaka. Observasi dalam penelitian ini dilakukan dengan mengamati secara langsung proses bisnis pada Toko Bibit Sriwedari untuk mengetahui pemasalahan yang ada sehingga menjadi acuan dalam mengembangkan sistem *e-marketplace* bbit sriwedari.

Wawancara pada penelitian ini dilakukan dengan tanya jawab secara langsung dengan pemilik sentra pembibitan, karyawan, maupun pembeli guna mendapatkan masukan dari berbagai peran. Studi literatur dalam penelitian ini akan dijadikan sebagai pendukung dan referensi. Jurnal dan artikel yang terkait dengan topik penelitian digunakan sebagai perbandingan dengan penelitian yang dilakukan.

Metode selanjutnya yaitu metode pengembangan sistem. Pada penelitian ini penulis menggunakan metode pengembangan sistem *Rapid Application Development* (RAD), model proses pengembangan perangkat lunak dengan teknik incremental yang mengutamakan penggerjaan yang cepat [16].



**Gambar 1.** Tahapan *Rapid Application Development* (RAD)

Dapat dilihat pada gambar 1 bahwa metode *Rapid Application Development* (RAD) memiliki tiga tahapan. Pada tahap *Requirements Planning* melibatkan pengguna untuk membahas analisis kebutuhan sistem agar dapat mengidentifikasi secara jelas spesifikasi sistem yang dibutuhkan. Selanjutnya pada tahap *Workshop Design RAD* akan dibuat rancangan pemodelan sistem. Pada tahap akhir yaitu *Implementation* sistem akan mulai dibangun sampai hasil rancangan sesuai dengan spesifikasi sistem (*looping*). Selanjutnya akan dilakukan pengujian untuk memastikan sistem dapat bekerja dengan baik secara fungsional. Pengujian sistem ini akan menerapkan *black box testing* pada *server lokal*.

## 2.2 Kriptografi

Kriptografi merupakan ilmu yang mempelajari tentang penyandian menggunakan perhitungan matematika [17]. Cara kerja dari kriptografi yaitu mengubah data yang dikirim oleh pengguna (*plaintext*) menjadi data yang tersandi (*chiphertext*), lalu data tersebut hanya dapat dikembalikan ke bentuk semula dengan kunci. Dengan begitu pengguna yang tidak memiliki hak akses tidak dapat mengetahui bentuk data yang sebenarnya sehingga dapat menghindari penyalahgunaan data. Terdapat dua macam dalam algoritma kriptografi yaitu algoritma simetrik yang menggunakan satu kunci untuk proses enkripsi dan deskripsi data. Sedangkan algoritma asimetrik menggunakan kunci yang berbeda dalam kedua proses tersebut.



**Gambar 2.** Ilustrasi penerapan algoritma kriptografi pada sistem

Dapat dilihat pada gambar 2 diatas penerapan algoritma kriptografi terletak pada data pesanan yang dienkripsi sesaat setelah pengguna melakukan pembayaran kemudian data yang tersimpan ke *database* berupa data yang sudah tersandi (*chiphertext*).

## 2.3 Advanced Encryption Standard (AES)

*Advanced Encryption Standard* (AES) adalah salah satu algoritma *chiper* yang digunakan untuk melindungi data atau informasi yang sifatnya rahasia. Sejak 2001, AES telah menggantikan algoritma *Data Encryption Standard* (DES) yang dianggap sudah kuno dan mudah dibobol. AES didukung oleh berbagai ukuran kunci, diantaranya yaitu 128 bit, 192 bit, 256 bit. Perbedaan ini yang nantinya akan mempengaruhi jumlah putaran yang dipakai saat proses enkripsi maupun deskripsi data [18]. Perbedaan tiap ukuran kunci pada algoritma AES dapat dilihat pada tabel 1 berikut.

**Tabel 1.** Perbedaan ukuran kunci algoritma AES

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

## 2.4 Payment Gateway Midtrans

Dengan perkembangan teknologi yang begitu pesat maka muncul beragam cara dalam melakukan transaksi. Pembayaran digital merupakan salah satu cara dalam melakukan transaksi menggunakan uang elektronik yang kini mulai banyak diminati oleh masyarakat karena kemudahan, kepraktisan, dan kecepatannya dalam melakukan transaksi pembayaran [12]. Midtrans adalah salah satu layanan *payment gateway* yang cukup terkenal di Indonesia. Midtrans memberikan kemudahan untuk para pemilik industry untuk meningkatkan penjualannya [3]. Disamping

itu juga Midtrans memberikan kemudahan kepada pengembang (*developer*) dalam melakukan pengujian sistem pembayaran [19].

### 3. HASIL DAN PEMBAHASAN

Pada penelitian ini penulis akan menjelaskan mengenai bagaimana proses bisnis sistem *e-marketplace* berasal dari berjalan. Pokok bahasan mencakup tentang hasil dari tiap tahapan dalam pengembangan sistem yaitu *Requirements Planning*, *Workshop Design* yang meliputi usulan rancangan sistem berupa *use case diagram* dan *activity diagram* dengan menerapkan algoritma kriptografi AES-256 untuk mengamankan data transaksi pengguna.

#### 3.1 Requirements Planning

Pada tahap ini menghasilkan sebuah rancangan sistem dengan melibatkan calon pengguna sistem. Kebutuhan sistem dapat teridentifikasi seperti yang ditunjukkan pada tabel 2.

**Tabel 2.** Analisis kebutuhan sistem

User	Admin
Melihat beranda	Melihat dashboard
Melihat produk	Mengelola user
Melihat keranjang	Mengelola kategori produk
Memesan produk	Mengelola produk
Membayar pesanan	Mengelola transaksi pesanan
Melihat status pesanan	Melihat status pesanan
	Menginput resi

#### 3.2 Workshop Design RAD

Pada tahap ini akan menggambarkan bisnis model dari sistem *e-marketplace* berasal dari *use case diagram* dan *activity diagram*.

##### 3.2.1 Use Case Diagram

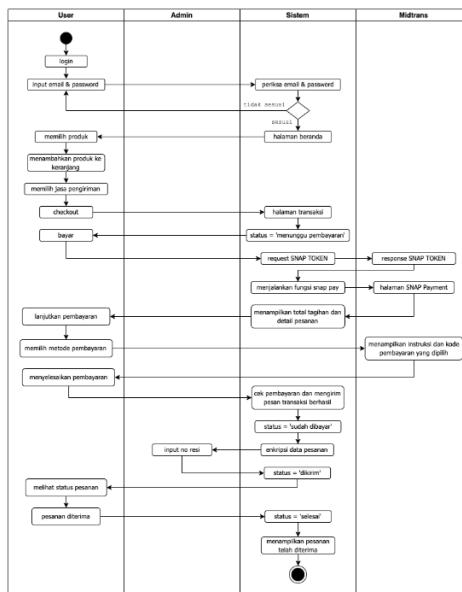
*Use case diagram* dalam penelitian ini menggambarkan interaksi aktor dengan sistem guna melihat fungsi utama yang ada kaitannya secara langsung dengan aktor dari sistem *e-marketplace* berasal dari sriwedari. Dalam sistem ini terdapat dua aktor yang berhubungan dengan sistem. Interaksi aktor dengan sistem digambarkan dalam model *use case diagram* pada gambar 3.



**Gambar 3.** Use case diagram *e-marketplace* berasal

##### 3.2.2 Activity Diagram

Aktivitas yang dilakukan oleh sistem pada penelitian ini digambarkan dalam sebuah model *activity diagram*. Sebelumnya dalam *use case diagram* telah digambarkan bagaimana aktor melakukan aktivitas menggunakan sistem, sedangkan dalam *activity diagram* akan lebih berfokus pada proses yang berjalan pada sistem. Proses penjualan pada sistem *e-marketplace* berasal dari pengguna memilih produk, melakukan pesanan dan sistem akan berkomunikasi dengan layanan *payment gateway* midtrans kemudian pengguna akan melakukan pembayaran dan admin menginput resi sampai barang diterima oleh pengguna akan ditampilkan pada gambar 3 berikut.



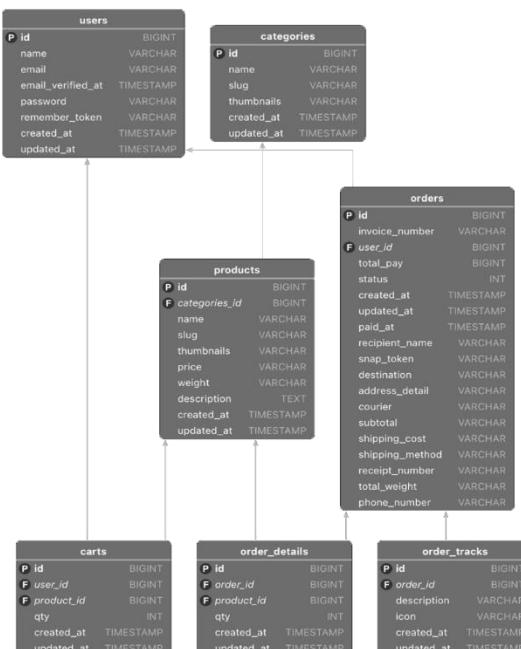
**Gambar 3.** Activity diagram e-marketplace bbit sriwedari

### 3.3 Implementation

Pada tahap ini penulis akan menjabarkan hasil implementasi dari metode penelitian dan algoritma AES-256 pada sistem *e-marketplace* bbit sriwedari. Hasil implementasi berupa *database* sistem dan implementasi sistem berupa pengujian sistem menggunakan *black box testing* yaitu memasukkan data dan melihat *output* apakah sesuai atau tidak. Pengujian akan berfokus pada transaksi pengguna.

#### 3.3.1 Implementasi Database

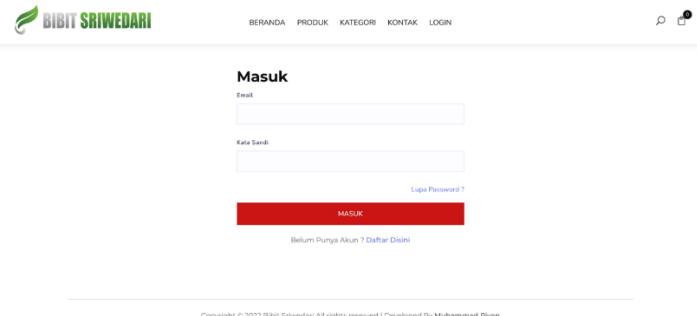
*Database* digunakan untuk menyimpan data dari sebuah sistem. Dengan adanya *database* dapat memudahkan dalam melakukan akses, simpan, pembaruan, dan penghapusan data. Disamping itu juga data pengguna dari sistem dapat terjaga dengan aman. Sistem *e-marketplace* bbit sriwedari memiliki tiga tabel utama yaitu tabel users yang digunakan untuk menyimpan data *login* dari pengguna, tabel categories yang digunakan untuk menyimpan data kategori dari produk, tabel products yang berisi detail data produk dan tabel orders yang berisi tentang data transaksi dari pengguna. Selanjutnya terdapat tabel carts yang berisi data produk yang dipilih oleh pengguna, tabel ini memiliki relasi dengan tabel users dan tabel products. Tabel orders memiliki relasi dengan tabel order\_details yang berisi detail order dari pengguna dan tabel order\_tracks yang berisi tentang status pesanan produk pengguna. Rancangan *database* dapat dilihat pada gambar 4 berikut.



**Gambar 4.** Database sistem e-marketplace bbit sriwedari

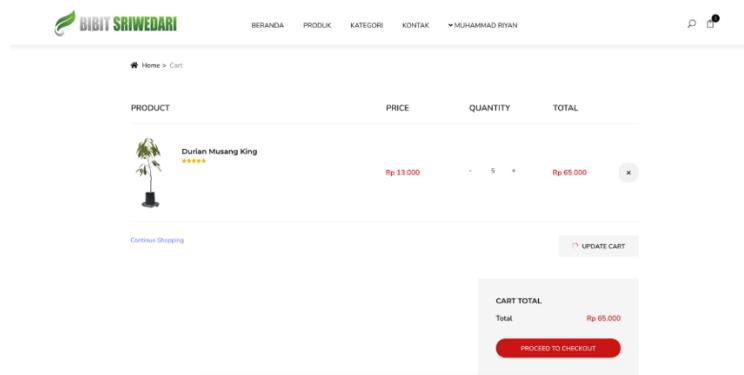
### 3.3.2 Implementasi Sistem

Pada tahap ini akan dijabarkan bagaimana hasil implementasi dari bisnis model dari sistem *e-marketplace* bibit sriwedari. Berikut hasil pengujian dari transaksi pengguna.



**Gambar 5.** Halaman *login*

Pada gambar 5 diatas pengguna melakukan login terlebih dahulu untuk melakukan transaksi pada sistem *e-marketplace* bibit sriwedari.



**Gambar 6.** Halaman keranjang

Pada gambar 6 terlihat bahwa pengguna telah memilih produk dan memproses pesanan dengan menekan tombol *checkout* untuk melanjutkan pemesanan.

A screenshot of the Bibit Sriwedari website's order details page. It is divided into two main sections: 'BILLING DETAIL' on the left and 'YOUR ORDER' on the right. The 'BILLING DETAIL' section contains fields for Recipient Name (Muhammad Rian), Phone Number (08882117413), Province (DI Yogyakarta), City (Kabupaten Sleman), Address Detail (Jl. Wono No. 33, Ngaglik, Sleman), Courier (JNE), and Shipment Method (Rp 65.000 - Rp 100.000 Estimasi 1-2 hari). The 'YOUR ORDER' section shows a summary of the purchase: Product (1. Durian Musang King x 5), Total (Rp 65.000), Total Weight (0.5 Kg), Subtotal (Rp 65.000), Shipping Cost (Rp 11.000), and Total (Rp 76.000). A 'PLACE ORDER' button is located at the bottom of this section.

**Gambar 7.** Halaman detail pesanan

Pada gambar 7 diatas pengguna diminta untuk melengkapi data pesanan dan memilih jasa pengiriman barang, kemudian pesanan akan dikonfirmasi.

A screenshot of the Bibit Sriwedari website's transaction history page. The table lists three transactions: 1. Transaction ID 3SHAV4, Product Durian Musang King, Status 'Menunggu Pengiriman' (Pending Shipment), Created At 2022-10-28 20:15:19, with a 'Detail' button. 2. Transaction ID DE20DS, Product Durian Musang King, Status 'Sedang' (In Progress), Created At 2022-10-27 10:45:10, with a 'Detail' button. 3. Transaction ID DZE4MC, Product Durian Musang King, Status 'Selesai' (Completed), Created At 2022-10-25 16:55:31, with a 'Detail' button.

**Gambar 8.** Halaman transaksi

# Journal of Computer System and Informatics (JoSYC)

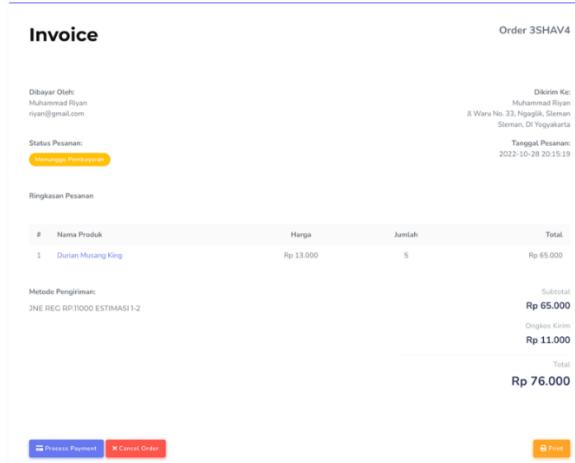
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)

Volume 4, No. 1, November 2022, Page 179–187

<https://ejurnal.seminar-id.com/index.php/josyc>

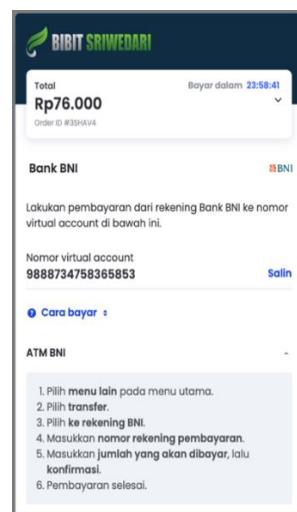
DOI 10.47065/josyc.v4i1.2451

Pada gambar 8 terlihat pada halaman transaksi pengguna bahwa status pesanan masih menunggu pembayaran.



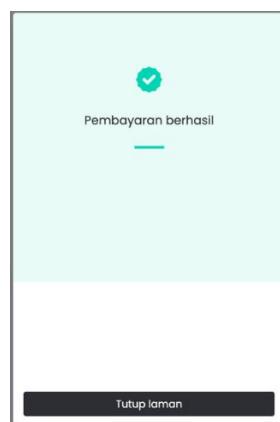
**Gambar 9.** Halaman *invoice*

Pada gambar 9 dapat dilihat detail pesanan produk dari pengguna, kemudian pengguna akan memproses pembayaran.



**Gambar 10.** Halaman pembayaran

Pada gambar 10 terlihat bahwa pengguna melakukan pembayaran dengan metode pembayaran bank transfer dari BNI.



**Gambar 11.** Pembayaran berhasil

Pada gambar 11 diatas terlihat transaksi pembayaran pengguna telah berhasil. Kemudian admin akan mendapatkan notifikasi pesanan di halaman dashboard.

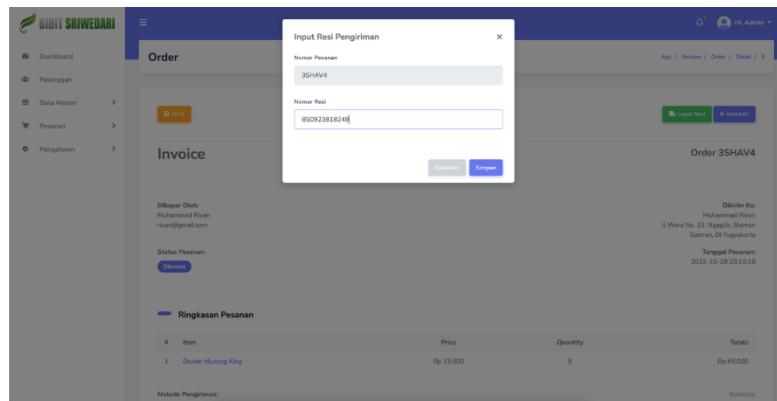
# Journal of Computer System and Informatics (JoSYC)

ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)

Volume 4, No. 1, November 2022, Page 179–187

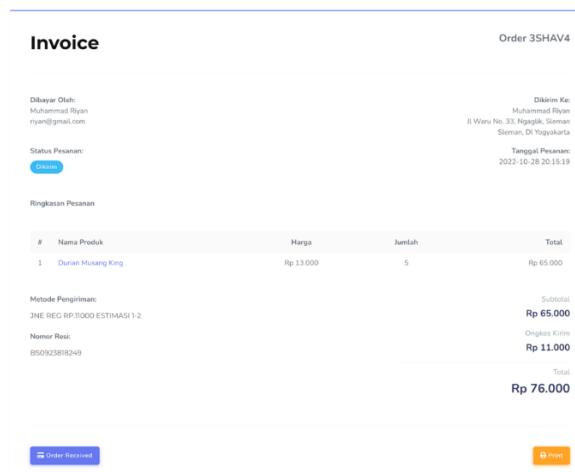
<https://ejurnal.seminar-id.com/index.php/josyc>

DOI 10.47065/josyc.v4i1.2451



Gambar 12. Admin menginput no resi

Pada gambar 12 diatas terlihat admin menginput no resi pesanan. Pada tahap ini status pesanan akan berubah menjadi dikirim.



Gambar 13. Pengguna mengecek status pesanan

Pada gambar 13 diatas pengguna mengecek status pesanan, setelah pesanan sudah diterima pengguna akan mengkonfirmasi bahwa pesanan telah diterima.

ID	Invoice_number	User_ID	Total_Pay	Status	Created_at	Updated_at	Paid_at	Recipient_name	Shap_token	Destination	Address_detail
1	TCoSwxPTISXg0tOSf5FB0==	2	127000	2022-10-26	2022-10-26 16:55:31	2022-10-26 17:00:51	2022-10-26 17:05:20	P5muFu0S2z-WT8tpIgH==> s0Rj2B/NHY0uex35GObc08AEHuUszVW/CGeV=+NFznefA... qfKeyQm/PxJUDV02V+RP4IPMBW9u/1V2yfet=> f+ZeePZTQ0exIU2DyD73==>			
2	Z0vW8b4PfQJQ3xaXkElP0q==	2	55000	2022-10-27	2022-10-27 10:45:10	2022-10-27 11:45:14	2022-10-27 00:00:00	86+eqJ35qfP9sWm0j2CA==> J0fbV1raOPbzHfFJDN2QfRWhdF+vdwNwQfGQyaesD8E... RIUFMOL0nIHqJLmkQ3h7VduhNfjxJmtnLDb+> WallWePNKUJ1EYyfFalg=>			
3	NIBhRQCz/Mnkmaek21BQcg==	2	76000	2022-10-28	2022-10-28 20:15:19	2022-10-28 20:21:52	2022-10-28 20:31:16	86+eqJ35qfP9sWm0j2CA==> pKerKD4qR+j7QtmMGcC32pk32zy2s0zV/mzYhaRku5zR... E6582yGIker9B4e+XpAbXeNj96vO3dpQjPa=> zTWP+tpHrMmMetlgDhmyCrwgcBL6038VFnWJctuX0+			

Gambar 14. Hasil pengujian data transaksi yang sudah terenkripsi dengan AES

Pada gambar 14 diatas dapat dilihat bahwa data transaksi pembayaran pengguna berhasil tersimpan di database dan data terenkripsi menjadi *chipertext*.

[bibitsriwedari.test/transaction/NI6hRQCz/Mnkmaek21BQcg==](http://bibitsriwedari.test/transaction/NI6hRQCz/Mnkmaek21BQcg==)

Gambar 15. Url detail transaksi yang sudah terenkripsi dengan AES

Pada gambar 15 diatas dapat dilihat juga *uniform resource locator* (url) sudah terenkripsi ketika pengguna mengakses data detail transaksi pembayaran.

## 4. KESIMPULAN

Kesimpulan yang didapat penulis setelah melakukan penelitian ini yaitu berdasarkan hasil dari pengujian dan analisis dari penerapan algoritma kriptografi AES-256 terhadap sistem *E-Marketplace* Bibit Sriwedari bahwa algoritma tersebut dapat berjalan dengan baik dalam melakukan enkripsi data transaksi pembayaran dari pengguna dan waktu yang relatif cepat. Algoritma AES-256 juga cukup aman dalam pemrosesan enkripsi data dikarenakan memiliki kunci yang panjang dan banyak proses putaran. Dengan begitu sistem *E-Marketplace* Bibit Sriwedari mampu memberikan alternatif kepada penjual bibit tanaman dan buah-buahan dalam mengelola penjualan bibit

serta untuk pembeli dalam membeli bibit tanaman dan buah-buahan yang disukai karena adanya integritas data antara penjual bibit dan pembeli.

## REFERENCES

- [1] Paryanta, H. Basuki, and A. Widhiyatmoko, “Sistem Informasi Penjualan Bibit Tanaman di Toko Higar Agro Berbasis Android,” *Go Infotech: Jurnal Ilmiah STMIK AUB*, vol. 27, no. 2, pp. 159–166, Dec. 2021, doi: 10.36309/goi.v27i2.158.
- [2] D. A. Afriansyah, D. Setiawati, and A. R. Bahtiar, “Rancang Bangun Website E-commerce di Toko Sean Shoes Menggunakan Metode Rapid Application Development,” *JITU : Journal Informatik Technology And Communication*, vol. 6, no. 1, pp. 1–8, 2022, doi: 10.36596/jitu.v6i1.634.
- [3] Alfian, P. Sokibi, and L. Magdalena, “Penerapan Payment Gateway pada Aplikasi Marketplace Waroeng Mahasiswa Menggunakan Midtrans,” *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 3, pp. 387–393, Sep. 2020, doi: 10.32493/informatika.v5i3.6719.
- [4] N. W. Kusbin, D. R. Kaparang, and J. R. Batmetan, “Perancangan dan Implementasi Sistem Transaksi Jual Beli Produk Berbasis Web,” *Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 1, pp. 44–53, 2021, [Online]. Available: <https://ejurnal.unima.ac.id/index.php/ismartedu>
- [5] C. D. Asti, W. H. N. Putra, and W. Purnomo, “Pengembangan Website E-Commerce dengan Pemanfaatan Sistem Payment Gateway Midtrans (Studi Kasus: Butik Rizza Collection),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 12, pp. 5213–5220, 2021, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [6] L. Mustika, “Implementasi Algoritma AES untuk Pengamanan Login dan Data Customer pada E-Commerce Berbasis Web,” *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, pp. 148–155, Feb. 2020, doi: 10.30865/jurikom.v7i1.1943.
- [7] Y. Putra, Y. Yunus, and Sumijan, “Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Serangan Cross Site Scripting,” *Jurnal Sistim Informati dan Teknologi (Jsisfotek)*, vol. 3, no. 2, pp. 56–63, Jun. 2021, doi: 10.37034/jsisfotek.v3i2.44.
- [8] 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,” *Jurnal CyberTech*, pp. 1–15, 2020, [Online]. Available: <https://ojs.trigunadharma.ac.id/>
- [9] D. Novianto and Y. Setiawan, “Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES),” *Jurnal Ilmiah Informatika Global*, vol. 9, no. 2, pp. 83–89, 2018.
- [10] A. Prameshwari and N. P. Sastra, “Implementasi Algoritma Advanced Encryption Standard (AES) 128 untuk Enkripsi dan Dekripsi File Dokumen,” *Jurnal Eksplora Informatika*, vol. 8, no. 2, pp. 52–58, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.
- [11] A. Wibowo, A. S. Hidayat, and E. Rahmawati, “Pembangunan Aplikasi E-Commerce Pemasaran Batik pada Toko Batik Rifqi,” *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, pp. 46–53, 2020.
- [12] I. G. P. F. P. Sudhana, I. G. A. J. Sadguna, I. G. N. S. Waisnawa, A. D. Yulianti, and A. A. A. N. Harmini, “Pengembangan Sistem Pembayaran untuk Desa Wisata Tri Eka Buana dengan Online Payment,” *Bhakti Persada Jurnal Aplikasi IPTEKS*, vol. 7, no. 1, pp. 17–23, May 2021, doi: 10.31940/bp.v7i1.2171.
- [13] S. D. Silalahi and G. L. Ginting, “Penerapan Algoritma Kriptografi Word Auto Key Encryption dalam untuk Pengamanan Soal Ujian Berbasis Komputer,” *Journal of Computer System and Informatics (JoSYC)*, vol. 2, no. 1, pp. 91–106, 2020.
- [14] M. A. Hidayah, N. B. Nugoho, and Moch. I. Perangin-Angin, “Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan Pada PT. Mestika Sakti,” *Jurnal CyberTech*, 2020.
- [15] A. P. Nugroho, Arini, and H. B. Suseno, “Keamanan Data Transaksi Nasabah pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES,” *QUERY : Jurnal Sistem Informati*, vol. 4, no. 1, pp. 9–17, 2020.
- [16] Gushelmi, “Penerapan Metode Rapid Application Development dalam Membangun Website E-Commerce,” *Jurnal Sains Dan Teknologi (JSIT)*, vol. 2, no. 1, pp. 37–45, 2022, doi: 10.47233/jsit.v2i1.84.
- [17] K. A. Seputra and G. A. J. Saskara, “Kriptografi Simetris RC4 pada Transaksi Online Booking Engine System,” *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 17, no. 2, pp. 286–295, 2020.
- [18] A. Fathurrozi and Selviyani, “Penerapan Algoritma Advanced Encryption Standard (AES-256) dengan Mode CBC dan Secure Hash Algorithm (SHA-256) untuk Pengamanan Data File,” *Journal of Information and Information Security (JIFORTY)*, vol. 2, no. 2, pp. 227–238, 2021, [Online]. Available: <http://ejurnal.ubharajaya.ac.id/index.php/jiforty>
- [19] E. Febriyanto, U. Rahardja, and N. Alnabawi, “Penerapan Midtrans sebagai Sistem Verifikasi Pembayaran pada Website iPanda,” *JURNAL INFORMATIKA UPGRISS*, vol. 4, no. 2, pp. 246–254, 2018.