Implementasi Algoritma AES Pada Aplikasi Pembelian *Voucher Hotspot* Berbasis Android

Rony Heri Irawan[1], Umi Mahdiyah[2], Rizki Dwi Kurniawan[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri
E-mail: [1]rony@unpkediri.ac.id, [2]umimahdiyah@unpkediri.ac.id, [3]rizkidwi123@gmail.com
Coresponden Author: *rony@unpkediri.ac.id*

Diterima Redaksi: 19 Juli 2023 Revisi Akhir: 21 Oktober 2023 Diterbitkan Online: 28 Januari 2024

Abstrak – *Pada era digital yang semakin maju, kebutuhan akan akses internet yang cepat dan aman semakin meningkat. Dalam konteks ini, voucher hotspot menjadi salah satu cara yang populer untuk memperoleh akses internet yang terjangkau dan mudah digunakan. Saat ini, penggunaan voucher masih menggunakan metode cetak voucher ke kertas. Hal ini dapat menimbulkan kekurangan salah satunya yaitu menimbulkan sampah kertas bekas voucher tersebut. Dengan permasalahan tersebut, maka dibuatlah sebuah aplikasi pembelian voucher berbasis android dengan implementasi algoritma enkripsi AES. Enkripsi AES adalah algoritma enkripsi yang terkenal karena kemanannya yang sudah terjamin. Tujuan dari penelitian ini adalah membangun sebuah sistem atau aplikasi pembelian voucher hotspot berbasis android dengan enkripsi AES. Dari pengujian sistem yang telah dilakukan dengan metode blackbox, aplikasi yang dibuat telah berjalan sesuai dengan rancangan dan menjawab permasalahan penelitian.*

Kata Kunci *— AES, Enkripsi, Hotspot, Voucher*

Abstract – *In the increasingly advanced digital era, the need for fast and secure internet access is increasing. In this context, hotspot vouchers are a popular way to obtain affordable and easy-to-use internet access. Currently, the use of vouchers still uses the method of printing vouchers on paper. This can lead to deficiencies, one of which is the waste of used paper vouchers. With these problems, an Android-based voucher purchase application was created with the implementation of the AES encryption algorithm. AES encryption is a well-known encryption algorithm because of its guaranteed security. The purpose of this research is to build a system or application for buying Android-based hotspot vouchers with AES encryption. From the system testing that has been carried out using the blackbox testing method, the applications that have been made have been running according to the design and have answered research problems.*

Keywords *— AES, Encryption, Hotspot, Voucher*

1. PENDAHULUAN

Seiring dengan kemajuan waktu, internet saat ini telah menjadi kebutuhan utama bagi sebagian besar masyarakat. Dengan tuntutan mobilitas yang tinggi seperti saat ini, untuk meningkatkan produktivitas maka terciptalah teknologi WLAN (*Wireless Local Area Network*) [1]. WLAN merupakan sebuah teknologi yang media transiminya tanpa menggunakan kabel, namun menggunakan gelombang radio [2].

Pembangunan *hotspot* saat inni merupakan trend dalam perkembangan teknologi. *Hotspot* ini mirip dengan konsep Warung Internet (Warnet) tetapi dengan cakupan yang lebih luas (Syahputra & WIjaya, 2022).Pemanfaatan voucher hotspot untuk mengakses internet telah menjadi umum di berbagai tempat, seperti restoran, hotel, dan tempat umum lainnya. Pada implementasi saat ini, *hotspot voucher* terbagi menjadi dua jenis yaitu, berbayar dan gratis [3].

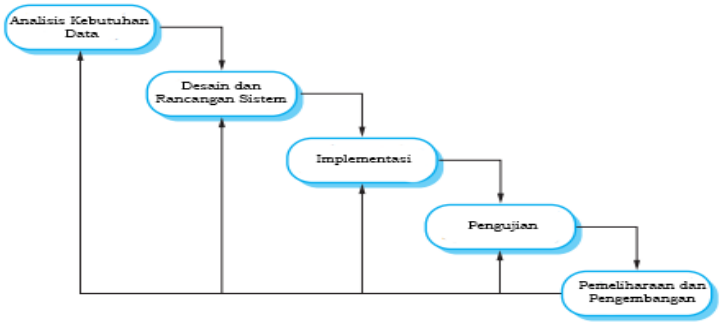
Berdasarkan pengamatan yang dilakukan oleh peneliti, penggunaan *voucher* masih dalam bentuk cetakan dengan kode *voucher*. *Voucher* yang berbentuk kertas tersebut memiliki beberapa kekurangan seperti menambah sampah kertas, kurang amannya kode *voucher*, dan bisa terjadi keterlambatan *voucher*.

Dari permasalahan yang terjadi maka dibuat sebuah aplikasi yang dapat memudahkan pembelian *voucher* tanpa cetak ke kertas. Aplikasi yang dibangun berbasis android yang menggunakan framework *Flutter* dan bahasa pemrograman *Dart* dengan enkripsi AES256 untuk keamanan kode *voucher* melalui mikrotik API.

2. METODE PENELITIAN

2.1. Metode Pengembangan Sistem

Dalam penelitian yang dilakukan ini, metode pengembangan sistem digunakan pada penelitian yang ini adalah metode *waterfall*. Metode *waterfall* memiliki 5 proses yang saling berkaitan dengan aktivitas pengembangan. Lima proses tersebut yaitu analisis kebutuhan data, desan dan rancangan sistem, implementasi, pengujian, dan yang terakhir adalah pemeliharaan dan pengembangan [4]. Dari kelima tahapan itu, tahapan per tahapan harus diselesaikan terlebih dahulu agar bisa ke tahapan yang selanjutnya.

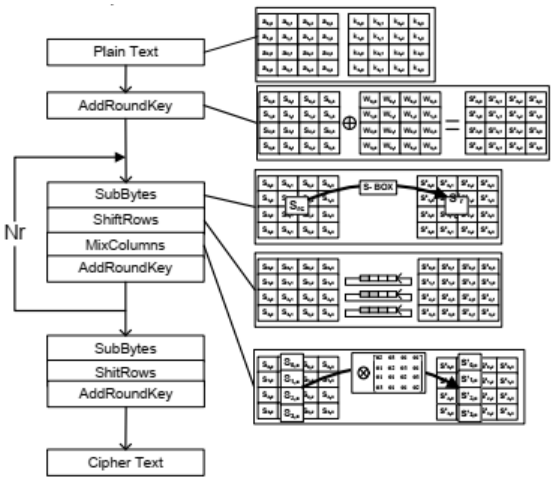


Gambar 1. Metode *Waterfall*

2.2. Algoritma AES (Advanced Encryption Standard)

Algoritma AES *(Advanced Encryption Standard)* merupakan algoritma enkripsi yang membutuhkan suatu kunci dalam proses enkripsi dan dekripsi. Proses enkripsi pada AES dilakukan secara berulang yang bisa disebut dengan ronde. Jumlah ronde tergantung dengan panjang kunci dimana setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya. Algoritma AES *(Advanced Encryption Standard)* memiliki kemampuan untuk mengenkripsi dan mendekripsi data dengan berbagai panjang kunci, termasuk 128 bit, 192 bit, dan 256 bit. Kunci pada enkripsi AES menggunakan proses yang berulang dimana biasa disebut *ronde*. Proses enkripsi dan deskripsi pada AES memiliki 4 jenis transformasi [5]. 4 transformasi pada proses enkripsi, yaitu:

a. *SubBytes*,
b. *ShiftRows*,
c. *MixColumns*,
d. *AddRoundKey* [6]

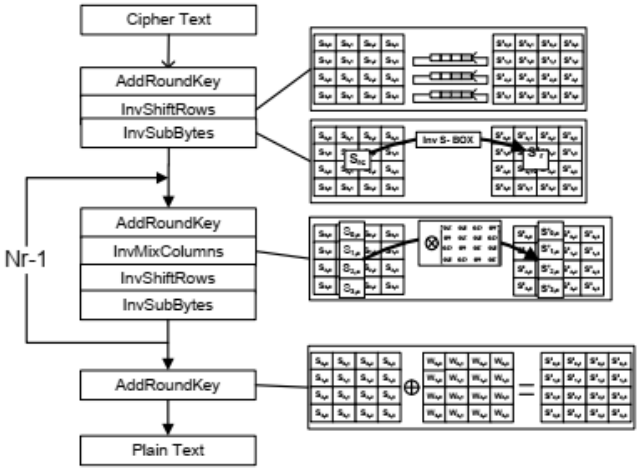


Gambar 2. Proses Enkripsi AES

Sedangkan transformasi pada proses deskripsi, antara lain :

a. *InvShiftRow*,
b. *InvSubBytes*,
c. *InvMixColumn*,

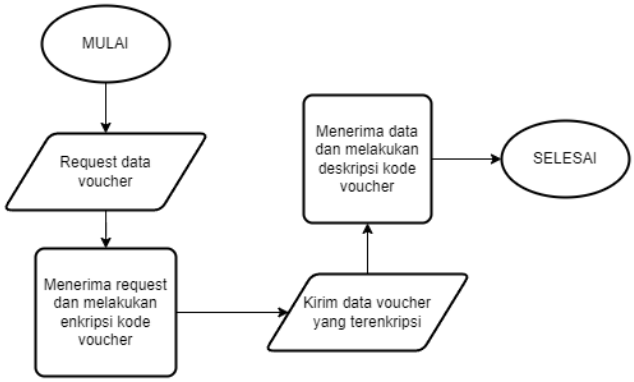
d. AddRoundKey [6]



Gambar 3. Proses Deskripsi AES

3. HASIL DAN PEMBAHASAN

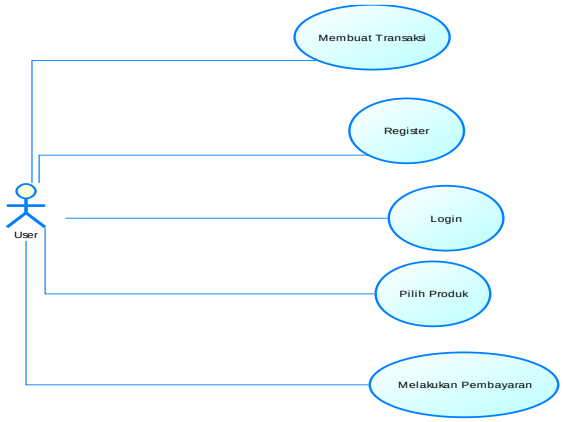
3.1. Flowchart Sistem



Gambar 4. Flowchart Sistem

Gambar 4 menunjukkan alur aplikasi dalam implementasi enkripsi dan deskripsi *voucher hotspot*. Pertama dari sisi aplikasi android akan melakukan request data *voucher* ke *server*. Kemudian *server* akan menerima *request* tersebut dan melakukan proses enkripsi. Setelah proses enkripsi selesai, data *voucher* yang telah terenkripsi tersebut dikirimkan kembali ke aplikasi, dan aplikasi akan memproses deskripsi *voucher* agar dapat digunakan untuk proses autentikasi ke *hotspot*.

3.2. Use Case Diagram

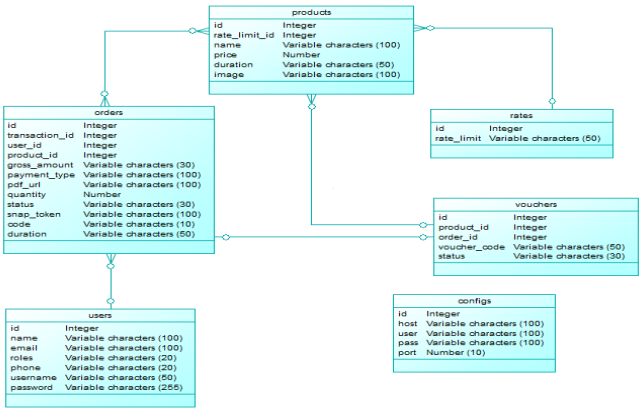


Gambar 5. Use Case Diagram

Use Case Diagram pada gambar 5 menunjukkan *actor user/*pengguna bisa melakukan aksi sebagai berikut:

a. *Register,*
b. *Login,*
c. Memilih produk,
d. Memproses transaksi, dan
e. Melakukan pembayaran.

3.3. Desain Database



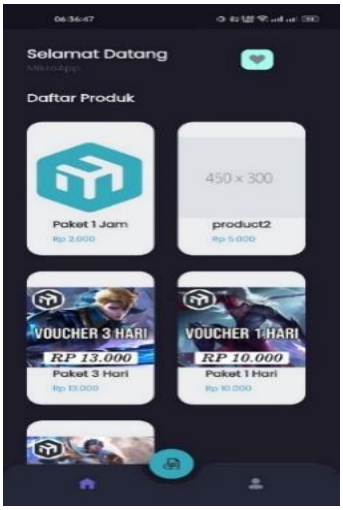
Gambar 6. Desain Database

3.4. Implementasi Sistem

Hasil implementasi dari aplikasi pembelian *voucher hotspot* berbasis android adalah sebagai berikut:

3.4.1. Halaman Utama

Halaman utama ini merupakan tampilan yang akan dilihat oleh pengguna pertama kali saat pengguna membuka aplikasi ini.



Gambar 7. Halaman Utama

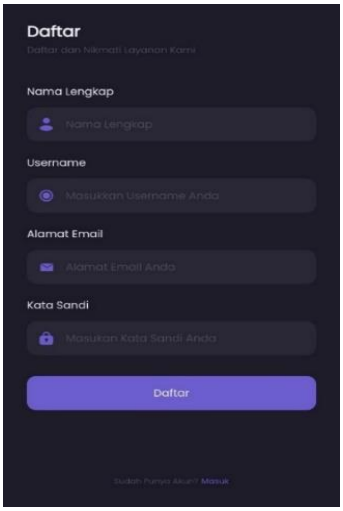
3.4.2. Halaman Detail Produk

Halaman ini menampilkan beberapa informasi produk yang telah dipilih oleh *user* dari halaman utama. Halaman ini menampilkan informasi seperti nama produk, harga, deskripsi dan juga terdapat tombol untuk menambah menghapus favorit dan tombol ”Buat Pesanan”.

Gambar 8. Halaman Detail Produk

3.4.3. Halaman Pendaftaran Pengguna

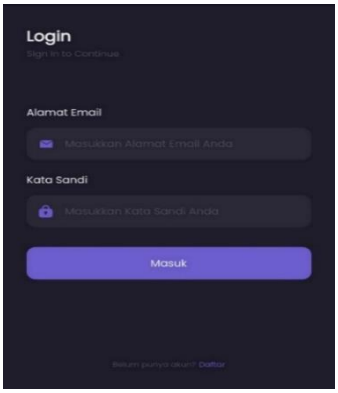
Halaman pendaftaran digunakan untuk mendaftarkan diri agar dapat melakukan transaksi pada aplikasi. Pada halaman ini, diperlukan beberapa isian yang harus dilengkapi seperti nama, *username*, *email*, dan kata sandi.



Gambar 9. Halaman Pendaftaran

3.4.4. Halaman Masuk

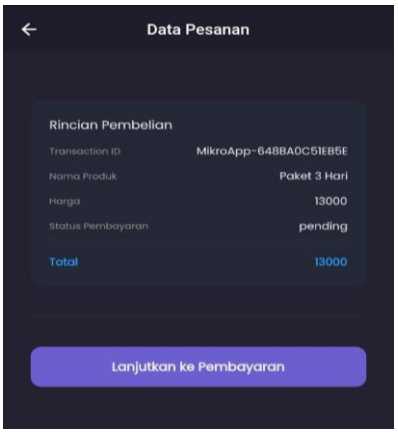
Halaman ini berfungsi sebagai proses authentikasi untuk masuk ke dalam aplikasi ketika pengguna sudah memiliki akun. Pada halaman masuk terdapaat isian alamat *email* dan kata sandi.



Gambar 10. Halaman Masuk

3.4.5. Halaman Data Pesanan

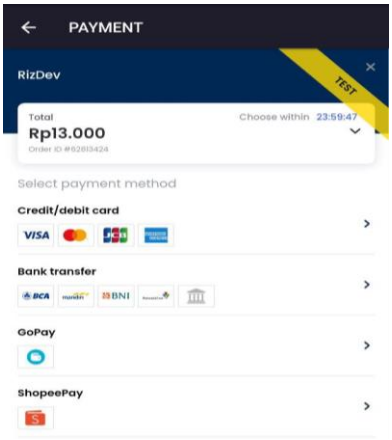
Halaman ini akan ditampilkan ketika pengguna menekan tombol ”Buat Pesanan” pada halaman detail produk. Buat pesanan disini berarti sistem akan membuat transaksi sesuai dengan produk yang dipilih oleh pengguna.



Gambar 11. Halaman Data Pesanan

3.4.6. Halaman Pembayaran

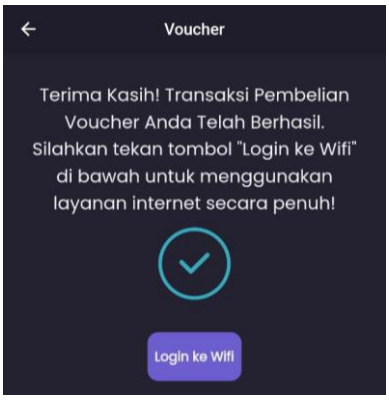
Halaman pembayaran digunakan untuk proses pembayaran produk *voucher* yang telah dipilih oleh pengguna. Disini akan ditampilkan beberapa metode pembayaran yang tersedia yang dapat dipilih sesuai dengan keinginan pengguna.



Gambar 12. Halaman Pembayaran

3.4.7. Halaman Sukses

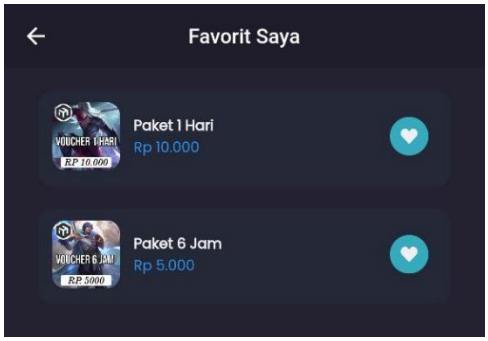
Pada halaman ini, transaksi/pembayaran yang dilakukan oleh pengguna sudah terverifikasi berhasil. Jika transaksi/pembayaran belum dilakukan, maka halaman ini tidak akan tampil. Halaman ini berguna untuk melakukan *login* ke jaringan *wi-fi hotspot*.



Gambar 13. Halaman Sukses

3.4.8. Halaman Produk Favorit

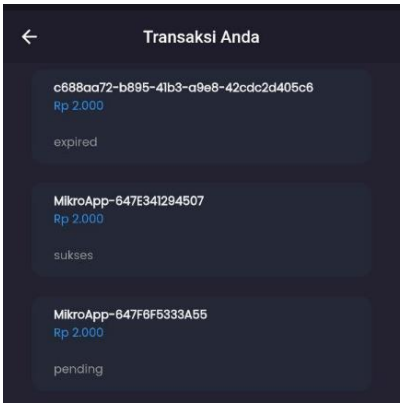
Halaman produk favorit ini menampilkan produk-produk yang telah ditandai favorit oleh pengguna. Disini pengguna juga dapat menghapus produk dari halaman favorit.



Gambar 14. Halaman Produk Favorit

3.4.9. Halaman Riwayat

Pada halaman riwayat, transaksi-transaksi yang telah dilakukan bisa dilihat kembali oleh pengguna. Riwayat transaksi ini juga menunjukkan status transaksi yang dilakukan apakah statusnya sukses, *pending*, *expired*, atau status lainnya.



Gambar 15. Halaman Riwayat

3.5. Pengujian

Pengujian pada aplikasi diperlukan untuk mengetahui apakah aplikasi sudah berjalan sesuai dengan harapan atau belum. Proses pengujian pada penelitian ini menggunakan metode *blackbox testing*. Berikut hasil dari pengujian yang telah dilakukan pada aplikasi ini:

Tabel 1. Pengujian aplikasi

No	Deskripsi Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1	Daftar dengan melengkapi isian dengan benar	Pendaftaran berhasil dan otomatis terautentikasi sesuai akun.	Sesuai harapan	Diterima
2	Daftar dengan data yang tidak lengkap dan tidak sesuai	Pendaftaran gagal, muncul notifikasi "Pendaftaran Gagal"	Sesuai harapan	Diterima
3	Masuk dengan akun yang sudah terdaftar	Autentikasi berhasil	Sesuai harapan	Diterima
4	Masuk dengan akun yang tidak terdaftar	Autentikasi gagal dan muncul notifikasi "Gagal *Login*"	Sesuai harapan	Diterima
5	Menekan salah satu produk	Diarahkan ke halaman detail produk	Sesuai harapan	Diterima
6	Menekan tombol favorit	Diarahkan ke halaman favorit dan menampilkan produk favorit yang sudah ditandai	Sesuai harapan	Diterima
7	Menekan "Buat Pesanan"	Diarahkan ke halaman data pesanan	Sesuai harapan	Diterima
8	Menekan "Lanjutkan Pembayaran"	Diarahkan ke halaman pembayaran	Sesuai harapan	Diterima
9	Menyelesaikan pembayaran	Kembali ke aplikasi dan menampilkan halaman transaksi sukses	Sesuai harapan	Diterima
10	Tidak menyelesaikan pembayaran	Kembali ke aplikasi dan menampilkan data pesanan	Sesuai harapan	Diterima
11	Menekan "*Login* ke *Wifi*"	Otomatis *login* ke jaringan *hotspot* dan terhubung ke internet secara penuh.	Sesuai harapan	Diterima

4. SIMPULAN

Berdasarkan hasil yang telah disampaikan diatas, kesimpulan yang dapat diambil dari penelitian ini adalah algoritma enkripsi AES telah berhasil diimplementasikan pada aplikasi pembelian *voucher hotspot* berbasis android, dan berdasarkan pengujian yang telah dilakukan, aplikasi sudah berjalan sesuai dengan harapan dan seluruh proses dapat dijalankan dengan baik.

5. SARAN

Saran yang dapat diberikan pada pengembangan aplikasi ini kedepannya yaitu implementasi algoritma enkripsi AES dapat dilakukan di seluruh proses pertukaran data dari *server* ke aplikasi android agar data lebih terjamin keamanannya.

DAFTAR PUSTAKA

[1] T. S. Fitria and A. Prihanto, "IMPLEMENTASI GENERATE VOUCHER HOTSPOT DENGAN BATASAN WAKTU (TIME BASED) DAN KUOTA (QUOTA BASED) MENGGUNAKAN USER MANAGER DI MIKROTIK," 2018. [Online]. Available: www.mikrotik.com.

[2] A. Syaputra and D. Stiadi, "PEMANFAATAN MIKROTIK UNTUK JARINGAN HOTSPOT DENGAN SISTEM VOUCHER PADA DESA UJANMAS KOTA PAGAR ALAM," *JIRE (Jurnal Informatika & Rekayasa Elektronika)*, vol. 3, no. 2, Nov. 2020.

[3] A. Zakaria, A. Prihantara, and A. A. Hartono, "Integrasi Application Programming Interface, PHP, dan MySQL untuk Otomatisasi Verifikasi dan Aktifasi Pengguna Layanan Hotspot MikroTik," *JUITA : Jurnal Informatika*, vol. 7, no. 2, pp. 63–69, Sep. 2019.

[4] I. Sommerville, *Software engineering*. Pearson, 2011.

[5] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.

[6] K. Muttaqin and J. Rahmadoni, "Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 1, no. 2, pp. 113–123, May 2020, doi: 10.37385/jaets.v1i2.78.