JURNAL TEKNIK INFORMATIKA DAN MULTIMEDIA Vol 5, No.2, Oktober 2025, pp.164 -171
p-ISSN : 2808-909X (print)
e-ISSN : 2798-2505 (online)
http://journal.politeknik-pratama.ac.id/index.php/JTIM · page 164
DOI : https://doi.org/10.51903/informatika.v5i2.1367

IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK MENINGKATKAN KEAMANAN PASSWORD PADA APLIKASI TO-DO LIST BERBASIS ANDROID DENGAN METODE AGILE

Dede Sahrul Bahri [1)], Muhammad 'Arda Rizqy Fauzan [2)]
[1]Universitas Pamulang
e-mail: dosen00271@unpam.ac.id
[2]Universitas Pamulang
e-mail: ardarizqyfauzan0301@gmail.com

ARTICLE INFO

Article history:

Received 10 Mei 2025
Received in revised form 24 June 2025
Accepted 8 Oktober 2025
Available online 15 Oktober 2025

ABSTRACT

Applications that implement user authentication, such as the To-Do List Application, often store sensitive information, requiring strong security protection. Passwords serve as the primary key for user authentication and must be secured to prevent unauthorized access. Therefore, this study applies the Advanced Encryption Standard (AES) algorithm to the To-Do List Application to enhance password security. AES was chosen due to its high level of security and efficiency, making it highly effective in safeguarding user data. The Agile method was utilized to ensure flexibility and responsiveness to requirements throughout the application development process. This approach allows for a more efficient development process while maintaining quality. The result of this research is an Android-based To-Do List Application that not only meets user needs but also provides a high level of security, ensuring users feel more comfortable using the application.

Keywords: *Encryption, AES, Cryptography, To-Do List, Agile*.

Abstrak

Aplikasi yang di dalamnya terdapat autentikasi pengguna, seperti Aplikasi *To-Do List*, seringkali menyimpan informasi penting, sehingga diperlukan perlindungan keamanan yang baik. Password berperan sebagai kunci utama pintu masuk dalam autentikasi pengguna, sehingga harus diamankan untuk mencegah akses yang tidak sah. Untuk itulah, penelitian ini menerapkan algoritma *Advanced Encryption Standard* (AES) pada Aplikasi To-Do List guna meningkatkan keamanan password pengguna. Pemilihan AES ini didasarkan pada tingkat keamanan dan efisiensi tinggi yang dimilikinya, sehingga sangat cocok untuk mengamankan data pengguna dengan efektif. Metode Agile digunakan untuk memastikan fleksibilitas dan responsifitas terhadap kebutuhan selama pengembangan aplikasi, sehingga membuat proses pengembangan lebih efisien, dengan tetap menjaga kualitas. Hasil dari penelitian ini adalah Aplikasi *To-Do List* berbasis

Received August 10, 2025; Accepted Oktober 2, 2025; Available online Oktober 10, 2025

p-ISSN : 0000-0000 e-ISSN : 2798-2505

Android yang tidak hanya dapat memenuhi kebutuhan pengguna, tetapi juga memiliki tingkat keamanan yang tinggi, sehingga pengguna dapat merasa lebih nyaman dalam menggunakan aplikasi.

Kata Kunci: *Enkripsi, AES, Kriptografi, To-Do List, Agile*

1. PENDAHULUAN

Aplikasi *To-Do List* merupakan aplikasi berbasis *Android* yang dibuat untuk memudahkan dalam mengelola tugas sehari–hari. Aplikasi ini seringkali menyimpan informasi sensitif seperti jadwal rapat penting, deadline proyek, atau data pribadi lainnya yang sangat rentan terhadap kebocoran data atau pencurian informasi jika tidak dilindungi dengan baik. Hal ini membuat kebutuhan akan keamanan pada aplikasi menjadi kebutuhan yang khusus. Oleh karena itu, kriptografi menjadi salah satu solusi untuk mengatasi permasalahan tersebut. Kriptografi merupakan ilmu yang berkaitan dalam menjaga kerahasiaan data melalui kode atau sandi. Salah satu teknik dalam kriptografi adalah enkripsi, yaitu proses mengubah informasi yang dapat dibaca (*plaintext*) menjadi bentuk yang tidak dapat dibaca (*ciphertext*). Sebaliknya, proses mengubah *ciphertext* menjadi informasi yang dapat dibaca, disebut dekripsi. Dalam proses enkripsi dan dekripsi ini diperlukan kunci (*key*) sebagai representasi alat untuk memastikan hanya pihak yang berwenang yang dapat mengakses informasi tersebut.

Dalam dunia kriptografi, terdapat berbagai macam algoritma yang dapat digunakan untuk mengenkripsi data, salah satunya yang paling populer adalah *Advanced Encryption Standard* (AES). AES termasuk ke dalam jenis algoritma *cipher block symmetric*, karena untuk melakukan proses enkripsi dan dekripsi diperlukan kunci (*key*) yang sama. AES sudah dikenal luas dikalangan pemerintah ataupun industri dunia, karena algoritmanya yang andal dan mampu melakukan enkripsi dengan tingkat kompleksitas yang tinggi membuatnya sulit diretas tanpa kunci enkripsinya.

Selain itu, metode Agile dipilih dalam penelitian ini karena sifatnya yang fleksibel dan adaptif terhadap perubahan serta kebutuhan akan keamanan, sehingga pengembangan aplikasi dapat lebih efisien dengan tetap menjaga kualitas. Dengan implementasi algoritma AES dan metode Agile pada penelitian ini diharapkan dapat mengembangkan aplikasi *To-Do List* yang aman dan dapat diandalkan, sehingga pengguna dapat merasa lebih nyaman dalam menggunakan aplikasi.

2. TINJAUAN PUSTAKA

2.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang banyak digunakan untuk mengamankan sebuah data. Banyak perusahaan-perusahaan besar yang menggunakan AES sebagai standarisasi keamanan mereka, seperti Google Cloud, Amazon, Alibaba. AES bermula pada tahun 1998 diadakan sebuah sayembara oleh NIST (*National Institute of Standard and Technology*) untuk membuat kriptografi baru sebagai pengganti algoritma DES (*Data Encryption Standard*). Adapun syarat untuk algoritmanya haruslah bersifat *public*. NIST memilih 5 finalis yang memenuhi syarat dari 15 proposal yang masuk. Setelah itu, dilakukan voting dan hasilnya *Vincent Rijmen* dan *Joan Daemen* dari Belgia, dinobatkan sebagai pemenang dengan 86 suara. Pada tahun 2001 tepatnya 26 November 2001, NIST mengumumkan bahwasanya algoritma *Rijndael* yang diusul oleh *Vincent Rijmen* dan *Joan Daemen* ditetapkan sebagai kriptografi sah dan dapat digunakan. Algoritma *Rijndael* kemudian distandarisasi sebagai AES [11].

Dibandingkan dengan DES, AES memiliki beberapa keunggulan signifikan. DES menggunakan kunci 56-bit yang dianggap tidak aman lagi di era komputasi modern, sementara AES mendukung ukuran kunci 128-bit, 192-bit, dan 256-bit, menjadikannya jauh lebih tahan terhadap serangan *brute-force*. Selain itu, AES dirancang untuk efisien baik dalam implementasi perangkat keras maupun perangkat lunak, sementara DES awalnya dioptimalkan untuk implementasi perangkat keras. AES juga memiliki struktur yang lebih fleksibel, memungkinkannya untuk beradaptasi dengan perkembangan teknologi di masa depan.

Kelebihan utama AES terletak pada keamanannya yang tinggi dan efisiensi komputasinya. Algoritma ini tahan terhadap berbagai jenis serangan kriptanalisis yang diketahui dan dapat diimplementasikan dengan efisien pada berbagai platform, dari perangkat *mobile* hingga *server* berskala besar. AES juga memiliki fleksibilitas dalam hal ukuran kunci, memungkinkan pengguna untuk memilih tingkat keamanan yang sesuai dengan kebutuhan mereka.

Namun, AES juga memiliki beberapa keterbatasan. Salah satunya adalah kompleksitas implementasi yang lebih tinggi dibandingkan dengan algoritma yang lebih sederhana seperti DES, terutama untuk ukuran kunci yang lebih besar. Ini dapat menjadi tantangan dalam lingkungan dengan sumber daya terbatas. Selain itu, meskipun AES sendiri sangat aman, implementasi yang buruk atau manajemen kunci yang lemah dapat membuat sistem yang menggunakan AES rentan terhadap serangan. Terakhir, seperti semua algoritma enkripsi simetris, AES menghadapi tantangan dalam distribusi kunci aman, yang sering kali memerlukan penggunaan protokol pertukaran kunci atau infrastruktur kunci publik tambahan.

Terlepas dari keterbatasan ini, AES tetap menjadi standar enkripsi yang paling banyak digunakan dan diandalkan di seluruh dunia, melindungi data sensitif dalam berbagai aplikasi, dari komunikasi internet hingga penyimpanan data terenkripsi.

2.2 Aplikasi To-Do List

Umumnya, kita membuat *todo list* secara manual dengan menggunakan kertas lalu menempelkannya disuatu tempat sebagai pengingat. Namun, cara itu membuat akses kita terbatas, terutama ketika kita sedang berada di luar. Karena itu, dikembangkan sebuah aplikasi berbasis *Android* yaitu Aplikasi *To-Do List*, yang dirancang untuk membantu kita dalam mengelola daftar tugas sehari-hari.

Aplikasi *To-Do List* ini dapat diakses kapan saja dan dimana saja melalui perangkat *Android*, dengan begitu kita dapat mengelola daftar tugas dengan baik sehingga dapat memaksimalkan produktivitas kita setiap saat.

3. METODOLOGI PENELITIAN

Penelitian ini mengadopsi pendekatan kualitatif untuk memahami bagaimana algoritma AES diterapkan dalam aplikasi *To-Do List*. Prosesnya dibagi menjadi tiga tahap utama. Tahap pertama, dilakukan pengumpulan data dengan studi literatur dari berbagai sumber tepercaya, termasuk jurnal, artikel, dan referensi relevan lainnya. Tahap kedua, dilakukan perancangan model dan perangkat lunak yang mencakup algoritma AES dan aplikasi *To-Do List*. Terakhir, tahap ketiga adalah implementasi dan pengujian perangkat lunak untuk memverifikasi fungsionalitasnya sesuai dengan tujuan yang telah ditetapkan.

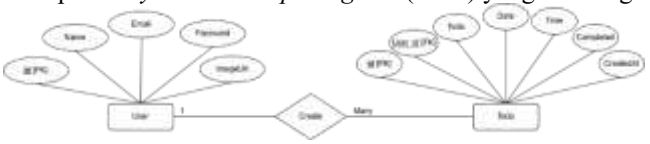
Untuk menguji aplikasi secara langsung, kuesioner disebarkan kepada responden yang diminta untuk mengunduh dan mencoba aplikasi terlebih dahulu. Tujuannya adalah untuk mengevaluasi efektivitas sistem dalam penggunaan nyata dan mendapatkan masukan serta saran langsung dari pengguna.

3.1 Perancangan Sistem

Perancangan sistem menyajikan rancangan perangkat lunak dan implementasi dalam penelitian ini

3.1.1 Perancangan Basis Data

Perancangan basis data berupa *Entity Relationship Diagram* (ERD) yang akan digunakan dalam sistem



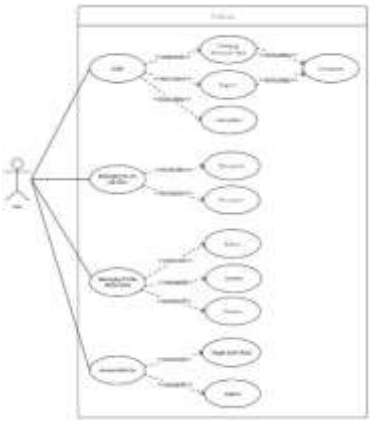
Gambar 1 Rancangan ERD

ERD ini menampilkan dua entitas utama *User* dan *Todo* yang saling berhubungan secara *one-to-many*. Entitas *User* memiliki atribut id (PK), *name*, *email*, *password*, dan *imageUrl* untuk menyimpan data akun dan profil. Entitas *Todo* terdiri dari id (PK), *user_id* (FK), *todo* (deskripsi tugas), *date*, *time*, *completed* (status *boolean*), dan *createdAt* (waktu pembuatan). Hubungan "Membuat" (1:N) direalisasikan dengan meletakkan *user_id* di tabel *Todo*, sehingga setiap tugas terkait langsung dengan satu pengguna, sementara satu pengguna dapat memiliki banyak tugas.

3.1.2 Perancangan UML

Perancangan berupa UML (*Unified Modelling Language*) sebagai gambaran aspek alur kerja sistem

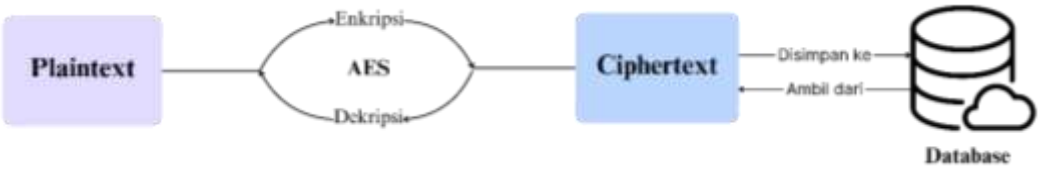
p-ISSN : 0000-0000 e-ISSN : 2798-2505



Gambar 2 Rancangan UML

Use Case Diagram ini menggambarkan alur utama bagi pengguna aplikasi *To-Do List*. Pertama, pengguna harus melakukan *login* (atau *register* jika belum punya akun) sebelum mengakses fitur apa pun, termasuk mengubah *password*. Setelah berhasil masuk, mereka bisa mengelola data *to-do list*, membuat, memperbarui, dan menghapus tugas, serta mengatur foto profil dengan pilihan mengunggah dari galeri atau mengambil lewat kamera, dan mengganti atau menghapusnya. Di menu pengaturan, pengguna dapat mengaktifkan atau menonaktifkan mode gelap dan melakukan *logout*, yang akan mengarahkan pengguna kembali ke layar *login* aplikasi. Pada Use Case diatas, terdapat *encryption* dan *decryption* yang berarti terdapat fitur enkripsi dan dekripsi dalam aplikasi To-Do List ini, untuk mengamankan data pengguna.

3.1.3 Perancangan AES



Gambar 3 Rancangan AES

Diatas adalah alur dari proses AES berjalan. Pengguna memasukkan password berupa (plaintext) yang dapat dibaca, kemudian terjadi proses enkripsi di belakangnya menggunakan algoritma AES, menghasilkan sebuah (ciphertext) tidak dapat dibaca, setelah itu disimpan di database. Lalu proses sebaliknya, ciphertext diambil dari database, kemudian terjadi proses dekripsi di belakangnya menggunakan algoritma AES, menghasilkan plaintext.

4. HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem dan Hasil

Dibawah ini adalah implementasi dari aplikasi To-Do List berdasarkan rancangan sistem diatas

a. Implementasi Splash Screen



Gambar 4 Implementasi Splash Screen

p-ISSN : 0000-0000 e-ISSN : 2798-2505

b. Implementasi Register Screen



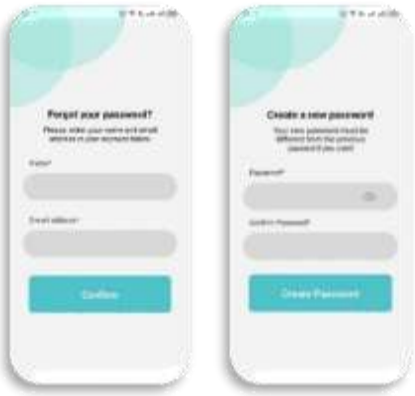
Gambar 5 Implementasi Register Screen

c. Implementasi Login Screen



Gambar 6 Implementasi Login Screen

d. Implementasi Forgot Password Screen



Gambar 7 Implementasi Forgot Password Screen

e. Implementasi Dashboard

p-ISSN : 0000-0000 e-ISSN : 2798-2505



Gambar 8 Implementasi Dashboard

f. Implementasi Add ToDo



Gambar 9 Implementasi Add ToDo

g. Implementasi Profile Photo Menu



Gambar 10 Implementasi Profile Photo Menu

h. Implementasi Settings Menu

p-ISSN : 0000-0000 e-ISSN : 2798-2505



Gambar 11 Implementasi Settings Menu

i. Implementasi AES

```
const crypto = require('crypto');

const algorithm = 'aes-256-cbc';
const key = crypto.createHash('sha256').update(process.env.AES_SECRET_KEY).digest();
const iv = crypto.randomBytes(16);
const ivUser = iv.toString('hex');

const encrypt = (text) => {
  const cipher = crypto.createCipheriv(algorithm, key, iv);
  let encrypted = cipher.update(text, 'utf8', 'hex');
  encrypted += cipher.final('hex');
  return {
    iv: ivUser,
    encryptedData: encrypted,
    userPassword: `${encrypted}${ivUser}`
  };
};

const decrypt = (encryptedData, iv) => {
  const decipher = crypto.createDecipheriv(algorithm, key, Buffer.from(iv, 'hex'));
  let decrypted = decipher.update(encryptedData, 'hex', 'utf8');
  decrypted += decipher.final('utf8');
  return decrypted;
};

module.exports = { encrypt, decrypt };
```

Hasil pengujian pada sistem menunjukkan bahwa implementasi AES pada Aplikasi *To-Do List* berhasil meningkatkan keamanan data pengguna. *Password* akan dienkripsi terlebih dahulu sebelum disimpan di *database*, lalu akan didekripsi pada saat proses *login*. Proses enkripsi dan dekripsi berlangsung tanpa menggangu performa dan kinerja aplikasi, sehingga pengguna dapat menggunakan aplikasi dengan nyaman.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan implementasi Algoritma *Advanced Encryption Standard* (AES) pada aplikasi *To-Do List* berbasis *Android*, didapatkan kesimpulan yang tercakup dalam beberapa poin yaitu:

a. Untuk meningkatkan keamanan data pengguna, khususnya *password*, pada aplikasi *To-Do List*, langkah-langkah yang dapat dilakukan adalah menggunakan kombinasi *password* yang kuat, yang terdiri dari angka, huruf, dan karakter khusus. Selain itu, data *password* juga harus dienkripsi sebelum disimpan di *database*, salah satunya dengan menggunakan Algoritma *Advanced Encryption Standard* (AES).
b. Implementasi algoritma AES berhasil meningkatkan keamanan data pengguna pada aplikasi *To-Do List*, terutama pada penyimpanan dan pengelolaan *password*. Enkripsi ini memastikan bahwa data pengguna terlindungi dari akses yang tidak sah.

Hasil kuesioner yang sudah dibagikan, didapatkan bahwa hasil termasuk ke dalam kategori **Sangat Baik**, yang menunjukkan bahwa penelitian dan sistem yang dikembangkan dinilai berhasil. Walaupun begitu, penelitian ini masih memiliki banyak peluang untuk pengembangan lebih lanjut, seperti penerapan *Two-Factor Authentication* (2FA) untuk meningkatkan lapisan keamanan, pengembangan aplikasi lintas *platform* seperti *IOS*, dan penambahan fitur seperti pengingat berbasis notifikasi.

DAFTAR PUSTAKA

[1] 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 Cyber Tech, vol. 4, no. 5, 2021. doi: https://doi.org/10.53513/jct.v4i5.1943.
[2] F. Sulianta, *Dasar Sistem Manajemen Basis Data*. 2024.
[3] J. R. Fauzi, “Algoritma dan Flowchart Dalam Menyelesaikan Suatu Masalah,” Jurnal Hukum Progresif, 2023.
[4] L. Clara and A. Budi, “IMPLEMENTASI METODE ALGORITMA AES PADA PERLINDUNGAN DATA SISTEM LOGIN,” Jurnal Informatika Dan Bisnis, vol. 10, no. 2, 2021. Diakses dari https://jurnal.kwikkiangie.ac.id/index.php/JIB/article/view/791.
[5] M. P. Sukumar, M. N. Ganapathiram, and D. S. Karthikeyan, “Android Odyssey: A journey into the world of mobile applications,” 2024.
[6] N. Khesya, “Mengenal Flowchart Dan Pseudocode Dalam Algoritma Dan Pemrograman,” 2021. doi: https://doi.org/10.31219/osf.io/dq45e.
[7] P. A. Lestari and A. H. Masitoh, “Aplikasi Me-List Berbasis Android Menggunakan Framework React Native,” Jurnal Esensi Infokom, vol. 6, no. 2, 2022.
[8] R. Abdillah et al., “Pengujian Perangkat Lunak Sistem Informasi Inventori pada Usaha Jasa Pengiriman Paket,” Polygon: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam, vol. 2, no. 4, pp. 166–175, 2024. doi: https://doi.org/10.62383/polygon.v2i4.199.
[9] S. P. Lestari, H. N. Fadlan, R. A. Purba, and I. Gunawan, “Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp,” Jurnal Media Informatika, vol. 4, no. 1, pp. 1–8, 2022. doi: https://doi.org/10.55338/jumin.v4i1.423.
[10] Y. Kurniawan, F. Jingga, and N. Limantara, Analisis Solusi Bisnis Berbasiskan Sistem Informasi. Deepublish, 2023.
[11] Y. Putra, Y. Yuhandri, and S. Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting," *Jurnal Sistim Informasi dan Teknologi*, pp. 56-63, 2021. doi: https://doi.org/10.37034/jsisfotek.v3i2.44.