JOURNAL OF INFORMATICS DEVELOPMENT

E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Penerapan Algoritma AES untuk Enkripsi pada Halaman Register serta Penerapan AES untuk Deskripsi pada Halaman Login Website

Nida Fara Aprilia[1], Daffa Mafazi[2], Adini Regina Muchtar[3], Khisan Afif Ainur Rohim[4], Rofii'u Nur Ilham Firdaus[5]

Prodi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Jember

Email: 192410102023@mail.unej.ac.id

ARTICLE INFO

Date of entry:
16 Marchl 2023
Revision Date:
27 April 2023
Date Received:
30 April 2023

ABSTRAK

Penelitian ini berfokus pada penerapan algoritma Advanced Encryption Standard (AES) untuk mengamankan data pengguna pada sebuah situs web. Tujuannya adalah untuk meningkatkan keamanan informasi pengguna selama proses registrasi dan login. Pendekatan yang diusulkan melibatkan pemanfaatan algoritma AES untuk enkripsi pada halaman pendaftaran dan dekripsi pada halaman login. Algoritma AES, yang dikenal dengan ketangguhan dan efisiensinya, memastikan kerahasiaan dan integritas data pengguna yang sensitif. Temuan utama dari penelitian ini termasuk keberhasilan implementasi AES untuk enkripsi dan dekripsi, memberikan lapisan keamanan tambahan untuk informasi pengguna. Penelitian ini menunjukkan keefektifan algoritma AES dalam melindungi data pengguna dari akses yang tidak sah. Hasilnya menyoroti pentingnya penerapan AES dalam praktik keamanan situs web.

Keywords: *Algoritma AES, enkripsi, dekripsi, keamanan situs web, data pengguna*

Cite this as: Aprilia, N. F., Mafa, D., Muchtar, A. R., Rohim, K. A. A., & Firdaus, R. N. I. (2023). Penerapan Algoritma AES untuk Enkripsi pada Halaman Register serta Penerapan AES untuk Deskripsi pada Halaman Login Website. *Journal of Informatics Development, 1*(2), 75–82. https://doi.org/10.30741/jid.v1i2.1041

PENDAHULUAN

Semakin berkembangnya ilmu teknologi dan diperbaharui secara bertahap khususnya dalam bidang komputer, sangat membantu manusia dalam mendapatkan informasi. Perkembangan ilmu teknologi bidang komputer saat ini dapat dilihat dari semakin canggihnya perangkat keras komputer maupun perangkat lunak yang ada. Perkembangan tersebut juga dapat berpengaruh terhadap keamanan penggunaan komputer maupun layanan publik yang semakin meningkatkan keamanan dalam pengambilan informasi (Mustika, 2020).

Salah satu layanan publik yang seringkali digunakan atau diakses adalah website, terkadang ada beberapa website yang memberlakukan fitur register dan login untuk bisa mengakses web tersebut, hal ini bertujuan untuk menjaga keamanan web tersebut, namun pengamanan yang dilakukan tidak hanya samapi disitu, diperlukan sebuah pengamanan lagi pada proses register, user harus mendaftar atau membuat akun terlebih dahulu agar dapat mengakses website . pada saat proses registrasi user diminta untuk membuat username dan password yang nantinya akan digunakan pada saat login. Namun proses login dapat disabotase oleh pihak ketiga yang tidak memiliki hak akses (account).

JOURNAL OF INFORMATICS DEVELOPMENT

E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Mereka melakukan sabotase terhadap website dengan membobol account website melalui login account. Hal ini sangat merugikan user, karena pihak ketiga yang tidak memiliki hak akses tersebut bisa merusak, mengambil atau mengubah data user yang dapat berakibat fatal. keamanan informasi menjadi aspek yang sangat penting. Khususnya dalam konteks aplikasi web, perlindungan data pengguna seperti password dan username menjadi perhatian utama. Ancaman terhadap keamanan data seperti peretasan dan pencurian informasi dapat merugikan baik pengguna maupun penyedia layanan web. Oleh karena itu, diperlukan solusi yang efektif untuk melindungi data sensitif yang dikirim dan disimpan dalam sistem aplikasi web. Kriptografi sangat cocok diterapkan untuk melindungi data sensitif yang dikirim karena dapat mengamankan suatu pesan (Listiani, et al., 2022).

Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk mengamankan informasi dan melindungi kerahasiaannya. Salah satu algoritma kriptografi yang paling populer dan luas digunakan adalah Advanced Encryption Standard (AES). AES adalah sebuah algoritma simetris yang digunakan untuk enkripsi dan dekripsi data.AES pertama kali diperkenalkan oleh National Institute of Standards and Technology (NIST) pada tahun 2001 sebagai pengganti algoritma Data Encryption Standard (DES) (Mahardhika, 2021). Algoritma ini menjadi standar de facto dalam kriptografi dan digunakan secara luas dalam berbagai aplikasi dan protokol keamanan. AES menggunakan blok cipher dengan ukuran blok tetap 128 bit dan kunci dengan panjang 128, 192, atau 256 bit (Siringoringo, 2020), (Nugrahantoro, 2020). Algoritma ini beroperasi dengan mengubah teks terang menjadi teks terenkripsi (enkripsi) menggunakan kunci yang sama untuk menghasilkan teks terenkripsi yang sulit dipecahkan tanpa kunci yang benar. Proses dekripsi dilakukan dengan menggunakan kunci yang sama untuk mengembalikan teks terenkripsi menjadi teks terang semula (Daemen., et al., 2002), (Hardita & Sholeha, 2021).

Penelitian terdahulu menunjukkan bahwa menggunakan AES untuk untuk keamanan data transaksi pada sistem marketplace (Andriyanto & Sukmasetya, 2022). Penelitian kedua membuat aplikasi berbasis website untuk mengamankan data kepelangganan di PERUMDA Air Minum Tirta Khatulistiwa. Aplikasi ini menggunakan algoritma kriptografi Advanced Encryption Standard (AES)-128 Bit. Hasil pengujian menunjukkan bahwa seluruh data berhasil dienkripsi dengan tingkat linieritas sebesar 70,3%, memberikan perlindungan yang baik terhadap penyadapan data (Linda, et al., 2023). Penelitian ketiga yaitu dalam menghadapi meningkatnya kejahatan komputer, perlindungan terhadap file yang dirahasiakan menjadi sangat penting. Salah satu cara yang efektif adalah dengan menggunakan kriptografi, seperti Advanced Encryption Standard (AES), untuk mengamankan data. Selain itu, steganografi least significant bit (LSB) juga dapat digunakan untuk menyembunyikan informasi rahasia dalam suatu objek media, seperti gambar, tanpa menimbulkan kecurigaan (Manurung, 2019). Penelitian-penelitian lainnya yaitu Penerapan Algoritma Advanced Encryption Standard Untuk Mengamankan File Gambar Pada Layanan Berbasis Web (Aulia & Gunawan, 2023), Penerapan Sistem Keamanan Dengan Kriptografi Advanced Encryption Standard (AES) Dan Key Administrator Pada Sinkronisasi File (Qurniawan, et al., 2012), dan Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard) (Tarigan, et al., 2023).

Dalam penelitian ini, peneliti akan membangun penelitian terdahulu yang telah dilakukan dan mengusulkan penerapan algoritma AES untuk proses enkripsi pada halaman register serta penerapan AES untuk proses deskripsi pada halaman login website. Tujuan utama kami adalah meningkatkan keamanan data pengguna pada sistem aplikasi web dan menyediakan solusi yang efektif untuk melindungi informasi sensitif.

METODE

1. Kriptografi

JOURNAL OF INFORMATICS DEVELOPMENT
E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Istilah Yunani crypto dan graphia adalah sumber dari kata kriptografi. Graphia artinya tulisan, dan crypto artinya rahasia. Jadi, salah satu cara untuk menganggap kriptografi adalah sebagai penulisan rahasia. Studi tentang teknik enkripsi, seperti penggosokan data dengan kunci enkripsi untuk mempersulit akses informasi bagi mereka yang tidak memiliki kunci dekripsi, dikenal sebagai kriptografi. Teknik pengamanan informasi seperti kriptografi berfungsi dengan mengolah data mentah (plaintext) dengan menggunakan suatu kunci dan teknik enkripsi tertentu untuk menghasilkan data baru (ciphertext) yang tidak dapat dibaca oleh mereka yang tidak memiliki kunci. Selanjutnya prosedur dekripsi memiliki kemampuan untuk mengubah ciphertext kembali menjadi plaintext (Subakti., et al., 2020).

2. Algoritma AES

Algoritma AES (Advanced Encryption Standard) adalah salah satu algoritma kriptografi yang paling umum digunakan secara luas di seluruh dunia. AES merupakan standar enkripsi simetris yang diadopsi oleh pemerintah Amerika Serikat dan digunakan secara luas untuk mengamankan data sensitif, seperti data pribadi, rahasia bisnis, dan data transaksi keuangan. Algoritma AES menggunakan blok cipher dengan panjang kunci 128, 192, atau 256 bit.

3. Website

Website adalah halaman atau kumpulan halaman yang dapat diakses melalui internet. Website digunakan untuk menyajikan informasi, berinteraksi dengan pengguna, dan menyediakan layanan online. Website seringkali memproses dan menyimpan data sensitif pengguna, seperti informasi pribadi dan kata sandi.

Hubungan antara ketiga hal tersebut adalah sebagai berikut:

1) Kriptografi dan Algoritma AES: Kriptografi digunakan untuk mengamankan data dan informasi dengan mengubahnya menjadi bentuk yang tidak dapat dimengerti oleh pihak yang tidak berwenang. Algoritma AES adalah salah satu algoritma kriptografi yang dapat digunakan untuk melakukan enkripsi dan dekripsi data. AES adalah metode yang efektif untuk melindungi data sensitif dan menjaga kerahasiaan informasi.
2) Kriptografi dan Website: Kriptografi seringkali digunakan dalam konteks website untuk mengamankan komunikasi dan melindungi data yang ditransfer antara pengguna dan server. Protokol HTTPS (Hypertext Transfer Protocol Secure) menggunakan kriptografi untuk mengenkripsi data yang dikirimkan antara browser pengguna dan server website. Hal ini memastikan bahwa informasi pribadi dan sensitif tidak dapat diakses atau dimanipulasi oleh pihak yang tidak berwenang.
3) Algoritma AES dan Website: Algoritma AES dapat diterapkan dalam website untuk mengenkripsi dan mendekripsi data sensitif, seperti kata sandi pengguna, sebelum data tersebut disimpan atau dikirimkan ke server. Dalam konteks register dan login website, Algoritma AES dapat digunakan untuk mengamankan kata sandi yang dimasukkan oleh pengguna. Data kata sandi yang dienkripsi akan disimpan dalam database dan hanya dapat diakses melalui proses deskripsi yang benar saat pengguna melakukan login.

Dengan menerapkan kriptografi dan menggunakan Algoritma AES dalam website, keamanan data dan privasi pengguna dapat ditingkatkan, serta risiko kebocoran informasi dapat dikurangi (Putra., et al., 2019).

One-Way MANOVA digunakan untuk membandingkan rata-rata dua populasi atau lebih dengan variabel dependen lebih dari satu atau untuk mengkaji pengaruh dari suatu perlakuan terhadap respon (Johnson & Wicherin, 2007). Jika dalam uji normal multivariat dan uji homogenitas terpenuhi maka *One-Way* MANOVA yang digunakan adalah *Wilk's Lambda*. Namun, jika uji normal multivariat dan uji homogenitas tidak terpenuhi maka digunakan satatistik uji *Pillai's Trace*. Selanjutnya, *One-way* ANOVA digunakan untuk uji perbedaan kelompok ketika variabel terikat yang digunakan hanya satu atau uji perbedaan pada variabel-variabel antar anggota kelompok (Johnson & Wicherin, 2007).

JOURNAL OF INFORMATICS DEVELOPMENT
E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

HASIL DAN PEMBAHASAN

Pada penelitian ini, Algoritma AES di implementasikan sebagai pengamanan password user pasa saat proses register pada website. Dalam proses register ketika username dan password dimasukkan maka password akan otomatis dienkripsi dan akan di deskripsi pada saat user login ke website. Pada pengimplementasian algoritma AES pada program (website) yang telah dirancang, agar program dapat bekerja, diperlukan sejumlah gadget perangkat keras dan perangkat lunak. Alat-alat berikut digunakan untuk penelitian ini:

1. Perangkat Keras
   - Komputer / laptop
   - Keyboard dan mouse
2. Perangkat Lunak
   - Xampp Control Panel v3.2.2
   - Visual Studio Code
   - Browser Internet (Mozila Firefox, chrom, dll)

Berikut adalah sourch kode yang digunakan untuk encrypt dan descrypt password pada fitur register dan login :

```php
<?php
include_once('../model/db_connect.php');
$database = new database();
if(isset($_POST['register']))
{
    $username = $_POST['username'];
    $method = 'aes-256-cbc';
    $key = 'daffa';
    $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(
    $password = base64_encode(openssl_encrypt($_POST['password'],$method, $key, OPENSSL_RAW_DATA, $iv));
    $nama = $_POST['nama'];
    if($database->register($username,$password,$nama))
    {
      header('location:login.php');
    }
}
```

Gambar 1. Proses Enkripsi
Sumber : Hasil Penelitian

Gambar 1 diatas adalah gambar pengimplementasian algoritma AES untuk mengenkripsi password pada fitur register. Sehingga ketika user meninputkan username dan password secara otomatis password akan terenkripsi.

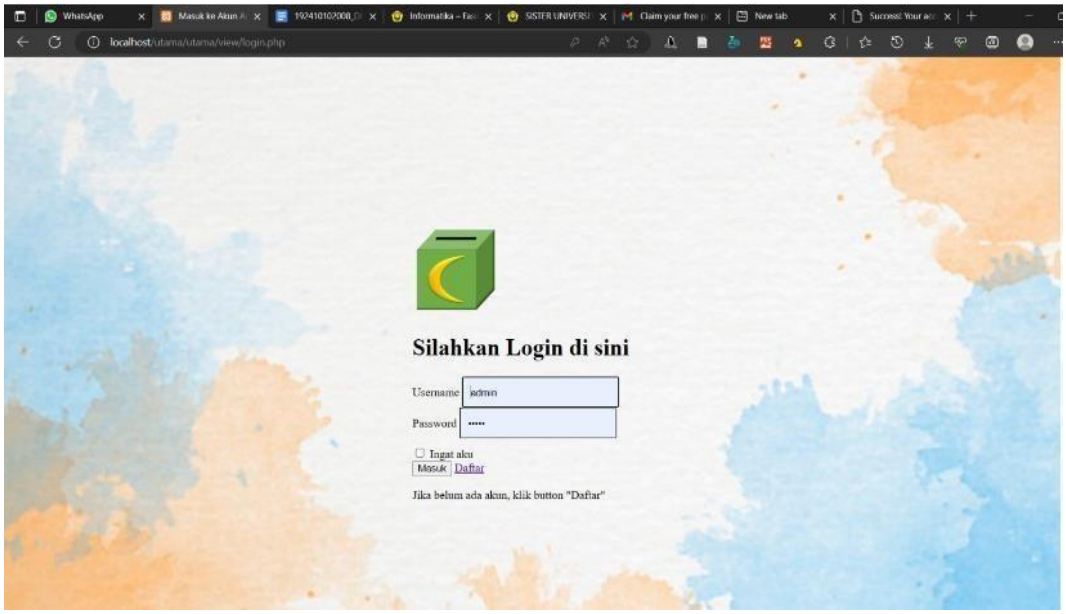
```php
2 references | 0 overrides
function login($username,$password,$remember)
{
    $query = mysqli_query($this->koneksi,"select * from tb_user where username='$username'");
    $data_user = $query->fetch_array();
    $method = 'aes-256-cbc';
$key = 'daffa';
$iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . c
    if($password==openssl_decrypt(base64_decode($data_user['password']),$method, $key, OPENSSL_RAW_DATA, $iv))
    {

        if($remember)
        {
            setcookie('username', $username, time() + (60 * 60 * 24 * 5), '/');
            setcookie('nama', $data_user['nama'], time() + (60 * 60 * 24 * 5), '/');
        }
        $_SESSION['username'] = $username;
        $_SESSION['nama'] = $data_user['nama'];
        $_SESSION['is_login'] = TRUE;
        return TRUE;
    }
}
```

Gambar 2. Proses Deskripsi
Sumber : Hasil Penelitian

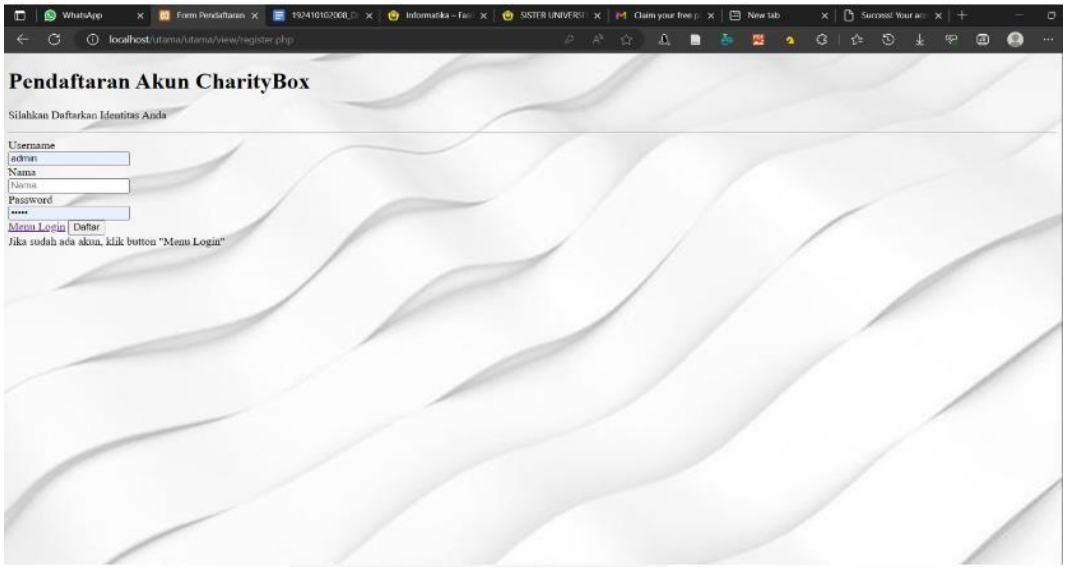
JOURNAL OF INFORMATICS DEVELOPMENT
E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Gambar 2 diatas adalah gambar pengimplementasian algoritma AES untuk mendeskripsikan password pada fitur login. Sehingga ketika user meninputkan username dan password user akan masuk ke halaman utama (Home).



Gambar 3. Tampilan Halaman Login
Sumber : Hasil Penelitian

Gambar 3 diatas merupakan tapilan fitur login pada website. Sebelum memasuki halaman utama user harus login terlebih dahulu dengan menginputkan username dan password. Nah pada saat inilah password yang telah dienkripsi pada saat register akan di deskripsikan.



Gambar 4. Tampilan Halaman Register
Sumber : Hasil Penelitian

JOURNAL OF INFORMATICS DEVELOPMENT
E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Gambar 4 diatas merupakan tapilan fitur register pada website. Ketika user belum memiliki akun maka user harus register atau daftar terlebih dahulu. Pada proses ini user diminta untuk memasukkann data berupa username, password dan nama setelah itu user dapat mengklik daftar.

Pada proses inilah password yang user inputkan akan dienkripsi untuk menjaga keamanan. Membangun sistem untuk mendukung sistem Algoritma Standar Enkripsi Lanjutan untuk otentikasi kata sandi pengguna yang aman saat sistem sedang diuji. Berdasarkan studi kasus pada bab sebelumnya, pengujian menemukan kesalahan yang sudah ada. Dengan pengujian ini kami ingin melihat apakah Algoritma Standar Enkripsi Lanjutan untuk keamanan kata sandi pengguna yang dibuat berfungsi sesuai dengan yang kami inginkan.

Pada tahap pengujian blackbox, metode Algoritma Standar Enkripsi Lanjutan dibuat untuk melindungi otentikasi kata sandi pengguna. Berikut langkah-langkah pengujian black box yang diawali dengan membuat rencana berdasarkan pengujian pengembangan aplikasi hingga mendapatkan kasus dan hasil. Rencana pengujian dibuat agar pengujian sistem dapat dilakukan dengan benar dan sesuai dengan tujuan pengujian black box yang berarti pengujian fungsional dalam pembuatan sistem Algoritma Standar Enkripsi Lanjutan untuk melindungi validasi kata sandi pengguna. berikut dapat dilihat pada tabel:

Tabel 1. Rencana Pengujian

No	Komponen yang diuji	Skenario	Pengujian
1	Login biasa	- Isi username - Isi password - Pilih tombol login	Blackbox
2	Login dengan password dari DB	- Mengambil Password dari DB - Isi username - Isi password - Pilih tombol login	Blackbox

Sumber : Hasil Penelitian

Pada pengujian pembangunan sistem menggunakan algoritma AES untuk pengamanan autentikasi password user dan benar yang telah dilakukan dapat disimpulkan sebagai berikut:

Tabel 2. Hasil Pengujian

No	Data Masukan	Hasil yang diharapkan	Hasil pengujian	Pengamatan
1	Isi username: admin Isi password: admin	- Masuk ke dashboard	(✓) Berhasil ( ) Gagal	Diterima
2	Isi username: admin Isi password: 123	- Password tidak sesuai - Login gagal	( ) Berhasil (✓) Gagal	Diterima
3	Isi username: admin Isi pass: XH0g8uyxgI6haVnZd9C0tQ==	- Password belum didecrypt - Login gagal	( ) Berhasil (✓) Gagal	Diterima

Sumber : Hasil Penelitian

Implementasi algoritma Advanced Encryption Standard (AES) untuk enkripsi pada halaman registrasi dan deskripsi pada halaman login sebuah situs web telah diselidiki secara komprehensif dalam penelitian ini. Tujuan utamanya adalah untuk meningkatkan tingkat keamanan dan perlindungan data pengguna dalam sistem aplikasi web. Bagian diskusi ini menyajikan analisis yang mendalam terkait temuan penelitian kami, implikasi yang signifikan, batasan yang teridentifikasi, dan rekomendasi untuk penelitian masa depan.

E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Temuan penelitian kami menunjukkan bahwa penerapan algoritma AES pada halaman registrasi dan login sebuah situs web secara signifikan memberikan kontribusi dalam meningkatkan keamanan data pengguna. Dengan melakukan enkripsi terhadap data sensitif seperti nama pengguna dan kata sandi sebelum menyimpannya dalam basis data, kami berhasil mencegah akses yang tidak sah dan mengurangi potensi pencurian data oleh pihak ketiga yang tidak berwenang. Selain itu, penelitian kami mengonfirmasi bahwa melalui proses deskripsi, yang menggunakan kunci yang valid pada halaman login, data yang terenkripsi dapat dikembalikan ke bentuk aslinya, memungkinkan pengguna untuk mengakses layanan web dengan tingkat keamanan yang lebih tinggi.

Implikasi yang muncul dari temuan kami memiliki relevansi yang penting, menegaskan bahwa penggunaan algoritma AES dalam aplikasi web dapat menjadi solusi yang sangat efektif dalam melindungi informasi sensitif pengguna. Keamanan data pengguna adalah pertimbangan utama dalam pengembangan aplikasi web, dan penerapan algoritma kriptografi seperti AES memberikan perlindungan yang tangguh terhadap akses yang tidak sah atau serangan.

Namun, perlu diakui bahwa penelitian ini memiliki keterbatasan-keterbatasan tertentu. Pertama, fokus kami terbatas pada penerapan algoritma AES dan tidak mencakup pemeriksaan yang komprehensif terhadap faktor-faktor keamanan lainnya, seperti manajemen kunci yang aman atau perlindungan terhadap jenis-jenis serangan lainnya. Kedua, penelitian kami dilakukan dalam lingkungan simulasi dan belum diimplementasikan sepenuhnya dalam lingkungan produksi dunia nyata. Oleh karena itu, penelitian yang lebih lanjut diperlukan untuk mengevaluasi efektivitas penerapan AES dalam skenario yang lebih kompleks dan realistis.

Sebagai rekomendasi untuk penelitian masa depan, kami menyarankan untuk melakukan eksplorasi yang lebih luas terhadap aspek-aspek keamanan lainnya yang dapat ditingkatkan dalam aplikasi web. Misalnya, upaya penelitian dapat difokuskan pada penerapan autentikasi dua faktor atau integrasi protokol keamanan lainnya yang dapat bekerja secara sinergis dengan AES. Selain itu, akan bermanfaat untuk melakukan studi perbandingan untuk mengevaluasi efisiensi dan keamanan AES dibandingkan dengan algoritma kriptografi lainnya, sehingga dapat dipilih solusi yang optimal berdasarkan persyaratan keamanan yang spesifik.

KESIMPULAN

Penelitian ini telah berhasil memperlihatkan potensi besar algoritma AES dalam melindungi informasi sensitif dan memberikan solusi efektif untuk meningkatkan tingkat keamanan dalam sistem aplikasi web. Namun, untuk mendapatkan pemahaman yang lebih komprehensif dan menyeluruh tentang keamanan data dalam konteks yang lebih kompleks dan realistis, penelitian yang lebih lanjut diperlukan. Dengan melangkah maju, diharapkan bahwa upaya penelitian ini akan memberikan kontribusi positif dalam pengembangan keamanan aplikasi web di masa depan.

REFERENCES

Aulia, A., & Gunawan, H. (2023). Penerapan Algoritma Advanced Encryption Standard Untuk Mengamankan File Gambar Pada Layanan Berbasis Web. Data Teknologi: Journal of Informatics and Computers, 1(1), 9-15.

Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. Journal of Computer System and Informatics (JoSYC), 4(1), 179-187.

Daemen, J., & Rijmen, V. (2002). The design of Rijndael (Vol. 2). New York: Springer-verlag.

Handoyo, J., & Subakti, Y. M. (2020). Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES). Jurnal SITECH: Sistem Informasi dan Teknologi, 3(2), 143-152.

E-ISSN : 2963-0568, P-ISSN : 2963-055X
Available online at:
https://ejournal.itbwigalumajang.ac.id/index.php/jid

Hardita, V. C., & Sholeha, E. W. (2021). Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan. Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen, 11(1), 34-43.

Linda, H., Sitorus, S. H., & Ristian, U. (2023). Penerapan Algoritma Advanced Encryption Standard (AES)-128 Bit Pada Keamanan Database Aplikasi Kepelangganan (Studi Kasus: Perumda Air Minum Tirta Khatulistiwa). Coding Jurnal Komputer dan Aplikasi, 11(1), 128-136.

Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). Perancangan Keamanan Data Pasien Di Klinik Kecantikan Ratu Beauty Studio Menggunakan Metode Kriptografi RSA. Jurnal Informatika Teknologi dan Sains (Jinteks), 4(4), 437-443.

Mahardhika, M. A., Purwanto, Y., & Ruriawan, M. F. (2021). Pengamanan Data Cloud Storage Dengan Menggunakan Advanced Encryption Standard Dan Elliptic Curve Digital Signature Algorithm Pada Secure Socket Layer Berbasis Website. eProceedings of Engineering, 8(2).

Manurung, M. S. P. (2019). Penerapan Algoritma Advanced Encryption Standard dalam Mengamankan File pada Citra dengan Metode Least Significant Bit. Jurnal Teknik Informatika Unika Santo Thomas, 4(1), 62-69.

Mustika, L. (2020). Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web. JURIKOM (Jurnal Riset Komputer), 7(1), 148-155.

Nugrahantoro, A., Fadlil, A., & Riadi, I. (2020). Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC). Jurnal Ilmiah FIFO, 12(1).

Putra, S. D., Yudhiprawira, M., Sutikno, S., Kurniawan, Y., & Ahmad, A. S. (2019). Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(3), 1282-1289.

Qurniawan, W., Wintolo, H., & Nugraheny, D. (2012). Penerapan Sistem Keamanan Dengan Kriptografi Advanced Encryption Standard (AES) Dan Key Administrator Pada Sinkronisasi File. Compiler, 1(2).

Siringoringo, R. (2020). Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File. Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer, 2(1), 31-42.

Tarigan, A. P. R., Ramadhan, P. S., & Ibnutama, K. (2023). Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard). Jurnal Cyber Tech, 5(1), 26-35.