SINTA Journal – *Science, Technology and Agriculture Journal*
Available online at : ***http://journal.pdmbengkulu.org/index.php/sinta***
DOI:https://doi.org/10.37638/sinta.5.2.145-152

Application Of Programming Logic And Algorithm To Improve Data Security Of Rantau Panjang Village Citizens In The Village Information System

Penerapan Logika Dan Algoritma Pemrograman Untuk Meningkatkan Keamanan Data Warga Desa Rantau Panjang Dalam Sistem Informasi Desa

Ozi Harianto[1], Muhammad Husni Rifqo[2], RG Guntur Alam[3], Ujang Juhardi[4]
[1,2,3,4)]Universitas Muhammadiyah Bengkulu, Indonesia
Corespondent Author: oziharianto4@gmail.com

How to Cite :
Harianto, O., M. H. Rifqo., RG. G. Alam., U. Juhardi. (2024). Application Of Programming Logic And Algorithm To Improve Data Security Of Rantau Panjang Village Citizens In The Village Information System. *SINTA Journal (Science, Technology, and Agricultural)*, 5 (2), 145-152. DOI: https://doi.org/10.37638/sinta.5.1.145-152

ARTICLE HISTORY
Received [29 May 2024]
Revised [23 June 2024]
Accepted [31 July 2024]

KEYWORDS
Data security, Encryption, Access management, Cyber threats, Information technology

ABSTRAK

Semua aktivitas manusia selalu dikaitkan dengan kemajuan teknologi dan informasi saat ini. Karena komputer dapat mengelola data dengan lebih cepat daripada manusia, penggunaan komputer sangat penting untuk mempermudah pekerjaan manusia. Kemajuan dalam telekomunikasi dan komputer saat ini memungkinkan pengguna menyimpan data secara digital. Namun, diyakini bahwa bagian keamanan data penting untuk data sensitif karena orang yang tidak bertanggung jawab dapat merusak data sensititif. Dalam hal ini desa rantau panjang memiliki data yang sangat penting yaitu data warga. Tujuan penelitian ini adalah untuk melindungi data warga desa rantau panjang di dalam sistem informasi desa dengan menerapkan algoritma AES (Advanced Encryption Standart). Untuk menyelesaikan permasalahan skripsi ini, metode perkembangan digunakan. Tujuan dari metode ini adalah untuk mempelajari perubahan terhadap waktu atau pola pertumbuhannya. Metode kuantitatif dan kualitatif berbeda. Notepad++ dan Xampp digunakan untuk menyelesaikan masalah skripsi ini. Penelitian ini menemukan bahwa algoritma AES (Advanced Encryption Standart) dapat mengamankan data warga di sistem informasi desa. Kesimpulannya adalah bahwa mengembangkan metode kriptografi yang menggunakan algoritma AES pada bahasa pemrograman PHP dapat meningkatkan keamanan data warga di sistem informasi desa. Teknik kriptografi memiliki kemampuan untuk mengenkripsi data warga sehingga hanya individu yang memiliki kunci dekripsi yang tepat yang dapat membacanya. Saat mengembangkan aplikasi, algoritma AES adalah algoritma pengaman data yang kuat yang dapat digunakan dalam bahasa pemrograman PHP. Untuk memastikan keamanan dan kehandalan aplikasi, tahapan desain sistem yang matang dan pengujian yang teliti diperlukan. Juga diperlukan pemahaman yang mendalam tentang metode kriptografi dan penggunaan algoritma AES pada PHP.

ABSTRACT

All human activities are always associated with current advances in technology and information. Because computers can manage data faster than humans, the use of computers is very important to make human work easier. Advances in telecommunications and computers now allow users to store data digitally. However, it is believed that the data security part is important for sensitive data as irresponsible people can damage sensitive data. In this case, Rantau Panjang village has very important data, namely resident data. The aim of this research is to protect the data of Rantau Panjang village residents in the village information system by implementing the AES (Advanced Encryption Standard) algorithm. To solve the problem of this thesis, the development method is used. The aim of this method is to study changes over time or growth patterns. Quantitative and qualitative methods are different. Notepad++ and Xampp were used to solve this thesis problem. This study found that the AES (Advanced Encryption Standard) algorithm can secure citizen data in village information systems. The conclusion is that developing a cryptographic method that uses the AES algorithm in the PHP programming language can improve the security of citizen data in village information systems. Cryptographic techniques have the ability to encrypt citizen data so that only individuals who have the correct decryption key can read it. While developing applications, the AES algorithm is a powerful data security algorithm that can be used in the PHP programming language. To ensure application security and reliability, a thorough system design stage and thorough testing are required. Also required is a deep understanding of cryptographic methods and the use of the AES algorithm in PHP..

PENDAHULUAN

Seiring dengan kemajuan teknologi serta informasi yang berkembang pesat pada zaman sekarang ini selalu ber iringan dengan semua aktivitas manusia. karena kemampuan computer mengelolah data melebihi kecepatan manusia. Penggunaan komputer dalam megelola data sangat dibutuhkan dalam mempermudah pekerjaan manusia. Pesatnya kemajuan tele komunikasi dan computer pada saat ini memungkinkan dilakukan penyimpanan secara digital oleh pengguna. Namun, diyakini bahwa komponen keamanan data penting untuk data sensitif. kerana juga memilki efek negatif dari orang yang tidak bertanggung jawab meretas data penting.

Muhammad Azhari, dkk (2022) menyimpulkan bahwa keamanan pada data atau dokumen hasil seleksi para peserta JAMKESMAS sehingga dapat lebih maksimal karena data yang disimpan telah terenkripsi dan hanya bisa dilihat keaslian file tersebut jika file tersebut telah didekripsi.

Dalam penelitian pada tahun 2017, Ami Aisiah Ibrahim menemukan bahwa membuat aplikasi sistem pengamanan data dengan enkripsi, dekripsi, dan file tesk menggunakan Mikrosoft Visual Studio 2010 mendukung kemajuan zaman. Salah satu algoritma harulah yang tepat adalah algoritma AES. Rijndael memiliki kelebihan karena algoritma ini saat ini cukup sulit dipecahkan karena belum ada serangan atau pemecahan yang belum mampu secara efektif dan efisien di analisis matematika karena pola yang dibentuknya cukup acak. (Ibrahim, 2017)

Angga Aditya Permana, dkk (2018) menyimpulkan bahwa algoritma AES: Rijndeal memiliki keunggulan karena memiliki daya memori dan kecepatan komputasi dalam pengoprasian. Pengoprasian yang tidak memakan memori yang terlalu besar ini banyak diminati pasar karena kebutuhan efisiensi waktu yang relatif cepat.

Sulta Lubis, dkk (2018) dalam penelitiannya menyimpulkan bahwa dalam menganalisa masalah yang terjadi terkait dengan pengamanan data TASPEN di PT.Pos Indonesiacabang medan menggunakan algoritma AES (*Advanced Encryption Standart*) maka dilakukan proses enkripsi untuk data taspen dari nama, tanggal lahir dan gaji untuk menyelesaikan permasalahan tersebut. Perancangan sistem kriptografi yang mengadopsi algoritma AES (*Advanced Encryption Standart*) denga metode sistem Block Cipher di dalam menyelesaikan masalah terkait pengamanan data TASPEN di PT.Pos Indonesia cabang medan menggunakan pemrograman yang berbasis dekstop yaitu *Visual Basic.*

Keamanan adalah bagian paling penting dalam pertukaran informasi, karena informasi hanya dapat diserahkan pada golongan tertentu. Jadi, penting melakukan pencegahan agar tidak dipersalahgunakan oleh golongan-golongan yang tidak memiliki kewajiban dan hak dalam pentingnya informasi. Keamanan ialah suatu yang berguna sehingga perlu diamati dan dicermati dalam perkembangan yang sangat pesatnya dunia internet. Jaringan internet ialah jaringan global yang mempublikasikan kepada halayak umum. Jarinagn internet bisa terdapat beragam jenis dampak baik dan buruk. Karena disebabkan internet merupakan jalan informasi yang tepat. Dikarenakan pada

saat ini jaringan computer menjadi kecenderungan maka diperlukan keamanan untuk mencegah suatu yang buruk dari jaringan internet.

Pemerintah adalah lembaga yang memiliki otoritas untuk membuat dan menerapkan undang-undang di wilayah tertentu. salah satunya yaitu desa. Desa ialah satuan masyarakat hukum yang mempunyai kewenangan untuk menanggung rumah tangganya sendiri berdasarkan hak asal-usul dan adat istiadat yang dibenarkan dalam pemerintahan nasional dan bertempat didaerah kabupaten. Desa diketuai atau dipimpin oleh seorang kepala desa yang dipilih langsung oleh warganya melalui pemilihan kepala desa. Untuk memudahkan dalam hal pengolahan data penduduk, maka desa menciptakan data penduduk secara digital dan dapat digunakan kapan dan dimana saja.

Dalam pengolahan data penduduk desa secara digital diperlukan keamanan agar data penduduk desa tersebut aman dari individu yang tidak bertanggung jawab yang mungkin merugikan penduduk. Ramainya kasus pembobolan data dan penyalahgunaan data untuk kepentingan yang salah, hingga perlunya keamanan data digital. tujuan penelitian ini ialah mengimplementasikan algoritma AES(*Advanced Encryption Standart*) untuk melindungi data warga desa rantau panjang di dalam sistem informasi desa.

METODE PENELITIAN

Tempat dan Waktu Penelitian

Penelitian ini telah dilaksanakan di Desa Rantau Panjang, Kecamatan Semidang Alas, Kabupaten Seluma April s/d Mei 2024.

Metode Pengumpulan Data dan Analisis Data

Pengumpulan data menggunakan wawancara, Observasi, Dokumentasi, Menganalisis dari data yang telah terkumpul dengan mengidentifikasi masalah yang ada dan menemukan penyelesaian atau algoritma yang akan digunakan dalam pengolahan data yang telah didapatkan.

Penyeleksian Data

Dimana data warga yang telah penulis kumpulkan akan melalui tahap penggolongan dimana data dipilih sesuai keperluan. Selanjutnya dilakukan

pembersihan data terhadap data yang tidak diperlukan pada penelitian ini, terakhir data akan di tranformasi sehingga bisa diterapkan menggunakan perangkat studi yang digunakan penulis dalam penelitian ini. Menghasilkan implementasi algoritma AES(Advanced Encryption Standart) untuk pengamanan data warga dalam sistem informasi desa terlebih dahulu login dengan username dan password. untuk melihat data warga.

Perancangan Sistem

Metode adalah urutan langkah-langkah yang harus diikuti untuk melakukan sesuatu. Dalam penelitian ini penulis menggunakan metode *Sysem Development Life Cycle* (SDLC) model waterfall. Seorang system analyst menggunakan proses logika *System Development Life Cycle* (SDLC) untuk membangun sistem informasi. Proses ini mencakup persyaratan, validasi, pelatihan, dan pemilik sistem.

***Data Flow Diagram* (DFD)**

Dengan menggunakan alat pembuatan model Data Flow Diagram (DFD), profesional sistem dapat menggambarkan sistem sebagai suatu jaringan proses fungsional yang terhubung satu sama lain dengan alur data, baik secara komputerisasi maupun manual.

***Entity Relationship Diagram* (ERD)**

ERD, atau diagram hubungan entitas, adalah diagram yang menggambarkan sebuah susunan data yang disimpan dari sistem. ERD terdiri dari entitas, atribut, dan hubungan masing-masing entitas, yang masing-masing memiliki atribut yang terhubung.

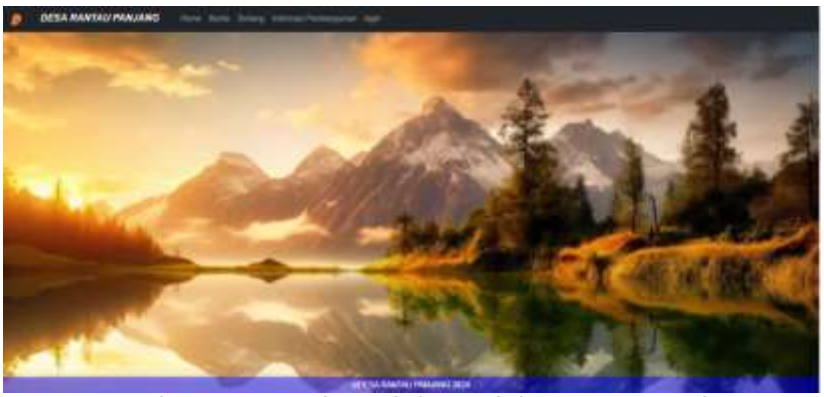
Rancangan Pengujian

Pada penelitian ini, metode pengujian Black Box digunakan untuk menguji hasil input dan output perangkat lunak tanpa mengetahui struktur kodenya. Setelah pembuatan perangkat lunak selesai, pengujian ini dilakukan untuk memastikan apakah itu berfungsi dengan baik.

HASIL DAN PEMBAHASAN

Hasil

Penelitian ini menghasilkan pengimpllementasian algoritma AES(Advanced Encryption Standart) untuk melindungi data warga desa Rantau Panjang dalam sistem informasi desa.



Gambar 1. menu sistem informasi desa rantau panjang

Hasil penelitian ini adalah pengimplementasian algoritma AES (*Advanced Encryption Standart*) untuk melindungi data warga desa rantau panjang didalam sistem informasi desa. Implementasi algoritma AES (*advanced encryption standart*) untuk meningkatkan keamanan data warga desa rantau panjang di dalam sistem informasi desa, fiturnya enkripsi dan dekripsinya menggunakan bahasa PHP. Lingkungan pengembangan terpadu (IDE) yang digunakan yaitu Notepad++.
Berikut uraian implementasi rancangan untuk proses enkripsi:

1. Menginisialisasi kunci enkripsi :
   $key = str_pad($key, 32, "\0");
2. Generate vektor inisialisasi (IV) secara acak :
   $iv_size = openssl_cipher_iv_length('AES-256-CBC');
   $iv ="22mei2024abqwsd7";
3. Selanjutnya melakukan enkripsi data :
   $encrypted = openssl_encrypt($data, 'AES-256-CBC', $key, 0, $iv);
   return base64_encode($data);
4. Menggabungkan vektor inisialisasi (IV) dan teks terenkripsi menjadi satu string :
   $result = base64_encode($iv . $encrypted);

Untuk uraian proses dekripsinya disajikan sebagai berikut :

1. Fungsi untuk melakukan dekripsi AES :
   function decryptAES($data, $key)
2. Menginisialisasi kunci enkripsi yang digunakan pada proses enkrisi :
   $key = str_pad($key, 32, "\0");
3. Melakukan decode base64 :
   $data = base64_decode($data);
4. Ambil vektor inisialisasi (IV) dari data terenkripsi :
   $iv_size = openssl_cipher_iv_length('AES-256-CBC');
   $iv = substr($data, 0, $iv_size);
5. Ambil teks terenkripsi dari data terenkripsi :
   $encrypted = substr($data, $iv_size);
6. Selanjutnya melakukan dekripsi :
   $result = openssl_decrypt($encrypted, 'AES-256-CBC', $key, 0, $iv);
   return base64_decode($data);

Uji coba (*Testing*)

Pada tahap testing, penulis menggunakan metode black box testing. Metode bleck box testing memungkinkan pengujian software tanpa memperhatikan detailnya. (Priyaungga, 2020), berikut ini beberapa uji coba yang dilakukan :

Tabel 4. Uji Coba

No	Skenario Pengujian	*Tase Case*	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
1	Memasukkan username dan password yang salah		Sistem akan menolak dan menampilkan pesan “username atau password salah”		Valid

2	Memasukkan username dan password yang benar		Sistem akan menerima dan langsung ditampilkan halaman data penduduk		Valid
3	Mengklik tambah data penduduk untuk menginput data dengan beberapa identitas		Jika mengklik simpan sistem akan langsung menyimpan data pada data base		Valid
4	Mengklik tombol berita baru untuk manambahkan berita dengan mengisi beberapa kolom		Dengan mengklik tambah berita, sistem akan langsung mengupload berita		Valid

Penggunaan teknik kriptografi dalam sistem informasi desa menawarkan solusi efektif untuk meningkatkan keamanan data warga. Dalam konteks ini, algoritma AES (Advanced Encryption Standard) yang diterapkan melalui bahasa pemrograman PHP telah terbukti sebagai metode yang tangguh dan efisien. AES dikenal karena kemampuannya mengenkripsi data dengan tingkat keamanan yang tinggi, membuatnya hampir mustahil diakses oleh pihak yang tidak memiliki otorisasi. Dengan menerapkan algoritma ini, sistem informasi desa dapat melindungi data sensitif warga dari akses yang tidak sah, sehingga memberikan rasa aman dan kepercayaan lebih kepada para pengguna sistem.

Teknik kriptografi bekerja dengan cara mengubah data asli (plaintext) menjadi bentuk terenkripsi (ciphertext) yang tidak dapat dibaca tanpa kunci dekripsi yang tepat. Ini berarti hanya individu atau sistem yang memiliki akses ke kunci tersebut yang dapat mengembalikan data ke bentuk aslinya. Implementasi AES dalam PHP memungkinkan pengembang untuk menyematkan lapisan keamanan tambahan pada aplikasi mereka, dengan memanfaatkan fungsi-fungsi kriptografi yang tersedia. Hal ini sangat penting dalam konteks desa, di mana data pribadi warga harus dilindungi dari ancaman siber dan kebocoran data.

Namun, implementasi teknik kriptografi tidak hanya sekedar menambahkan lapisan enkripsi pada aplikasi. Proses ini memerlukan perencanaan dan desain sistem yang matang untuk memastikan integritas dan keandalan aplikasi secara keseluruhan. Tahapan desain yang komprehensif, termasuk analisis kebutuhan dan perencanaan arsitektur sistem, sangat penting agar aplikasi dapat berfungsi secara optimal. Selain itu, penting untuk melakukan pengujian yang cermat terhadap sistem yang dikembangkan untuk mengidentifikasi potensi celah keamanan atau bug yang mungkin terjadi selama penggunaan.

Pemahaman yang mendalam tentang algoritma AES dan cara penerapannya dalam PHP adalah prasyarat penting bagi pengembang yang ingin memanfaatkan teknik ini. Pengembang harus familiar dengan berbagai konsep kriptografi seperti kunci simetris, mode operasi, dan manajemen kunci untuk memastikan implementasi yang efektif. Selain itu, pemilihan parameter kriptografi seperti panjang kunci dan mode operasi harus dilakukan dengan hati-hati agar sistem tetap aman dari serangan kriptografi yang berkembang.

KESIMPULAN DAN SARAN

Kesimpulan

Pengembangan sistem informasi desa dengan mengadopsi teknik kriptografi menggunakan algoritma AES dalam PHP memiliki potensi signifikan untuk meningkatkan keamanan data warga. Dengan desain sistem yang tepat dan pengujian yang cermat, aplikasi ini dapat berfungsi sebagai solusi yang handal dalam melindungi data sensitif warga. Selain itu, dengan memahami dan menerapkan teknik kriptografi yang tepat, desa dapat memanfaatkan teknologi ini untuk menciptakan lingkungan digital yang lebih aman dan terpercaya.

Saran

Berikut adalah beberapa rekomendasi untuk penelitian lebih lanjut tentang pengamanan data: Pertama, penting untuk melakukan pengembangan dan peningkatan keamanan aplikasi secara terus-menerus. Penelitian ini dapat menjadi dasar untuk pengembangan lebih lanjut pada aplikasi yang telah ada, termasuk peningkatan keamanannya, agar tetap dapat diakses dengan aman. Kedua, meskipun algoritma AES cukup aman, disarankan untuk menggabungkan beberapa algoritma yang lebih kuat atau mengembangkan algoritma baru guna meningkatkan keamanan data. Terakhir, aplikasi yang telah dikembangkan memiliki potensi untuk digunakan dalam mengamankan data penduduk di tingkat nasional. Oleh karena itu, disarankan untuk memulai penerapan aplikasi ini secara nasional agar dapat digunakan secara luas dan meningkatkan keamanan data penduduk di seluruh wilayah.

DAFTAR PUSTAKA

Amin, M. M. (2016). Komunikasi Berbasis Teks. Jurnal Pseudocode, III(September), 129–136.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

F, K. Ge. (1967). Proses Perhitungan Algoritma AES Lengkap. Angewandte Chemie International Edition, 6(11), 951–952., D, 5–27.

Hermiati, R., Asnawati, A., & Kanedi, I. (2021). Pembuatan E-Commerce Pada Raja Komputer Menggunakan Bahasa Pemrograman Php Dan Database Mysql. Jurnal Media Infotama, 17(1), 54–66. https://doi.org/10.37676/jmi.v17i1.1317

Ibrahim, A. A. (2017). Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard). Jurnal Teknik Informatika STMIK Antar Bangsa, 3(1), 53–60.

Kurnia Wardhani, Y. (2022). Aplikasi Absensi Guru Dan KAaryawan Berbasis WEB Pada MTs Negeri 1 Lumajang. Jurnal Teknik Industri, Sistem Informasi Dan Teknikinformatika, 1(2), 93–110. https://ejournal.ubibanyuwangi.ac.id/index.php/jurnal_tinsika

Lubis, M. T. S., Nugroho, N. B., & Ginting, R. I. (2018). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Data Taspen Di Pt.Pos Indonesia. Jurnal CyberTech, x. No.x(x).

No Titleبیبی. (n.d.).

Nurnaningsih, D., & Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). Jurnal Teknik Informatika, 11(2), 177–186. https://doi.org/10.15408/jti.v11i2.7811

Saragih. (2019). Pemrograman C++. P. Wandi, 1–132.

Silitonga, P. D. ., & Purba, D. E. R. (2021). Implementasi System Development Life Cycle Pada Rancang Bangun Sistem. Jurnal Sistem Informasi Kaputama (JSIK), 5(2), 196–203.

Simbolon, I. A. R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. (2020). Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar. Journal of Computer System and Informatics (JoSYC), 1(2), 54–60.

Tulloh, A. R., Permanasari, Y., Harahap, E., Matematika, P., Matematika, F., Ilmu, D., & Alam, P. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption. Jurnal Matematika UNISBA, Vol 2(1), 1–8.