Jurnal Bintang Pendidikan Indonesia (JUBPI)
Vol.1, No.2 Mei 2023
e-ISSN: 2963-4768; p-ISSN: 2963-5934, Hal 251-263

Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi

[1] Fadlullah Fadlullah, [2] Muhlis Tahir, [3] Briliant Pijar Bintari, [4] Mia Liana Dewi, [5] Muhammad Fahri Ilmy, [6] Syafi' Syafi', [7] Rama Ardiansyah

Prodi Pendidikan Informatika
Alamat: Pendidikan Informatika, Universitas Trunojoyo Madura
Jalan Raya Telang, Bangkalan, 69162, Indonesia
Korespondensi penulis: [1] 190631100001@student.trunojo.ac.id , [2] muhlis.tahir@trunojoyo.ac.id , [3]190631100004@student.trunojo.ac.id , [4] 190631100008@student.trunojo.ac.id ,[5]190631100010@student.trunojo.ac.id , [6] 190631100013@student.trunojo.ac.id [7] 190631100017@student.trunojo.ac.id

Abstract.

The more rapid development of information technology, this has an impact and can cause changes in people's thinking patterns in communicating. In the past, the way people used to communicate remotely was still manual, namely by using letters. The lack of efficiency in sending letters encourages people's mindsets to create innovations that facilitate long-distance communication, namely via SMS, email, WhatsApp and the internet. One of the impacts of the development of message delivery technology is the tapping of data which makes the user feel insecure. One way to secure data breaches is by securing the sender's and recipient's email passwords using AES (Advanced Encryption Standard) cryptography. We conclude that the AES algorithm can be applied to encrypt passwords, so that passwords cannot be easily read by other users. In addition, the password will not be easily cracked.

Keywords*: Website, AES (Advanced Encryption Standard), waterfall*.

Abstrak.

Semakin pesatnya perkembangan teknologi informasi, hal tersebut berdampak dan dapat menyebabkan berubahnya pola berfikir masyarakat dalam berkomunikasi. Dulu cara yang dilakukan oleh masyarakat untuk berkomunikasi jarak jauh masih manual yaitu dengan menggunakan surat. Kurangnya efisiensi dalam pengiriman surat mendoronng pola pikir masyarakat untuk menciptakan inovasi yang memudahkan komunikasi jarak jauh yakni melalui SMS, email, whatsapp dan internet. Salah satu dampak dari perkembangan teknologi pengiriman pesan adalah adanya penyadapan data yang membuat user merasa kurang aman. Salah satu cara untuk mengamankan kebobolan data yaitu dengan mengamankan password email pengirim dan penerima dengan menggunakan kriptografi AES (Advanced Encryption Standard). Kita menyimpulkan bahwa algoritma AES dapat diterapkan untuk melakukan enkripsi pada password, sehingga password tidak dapat dengan mudah dibaca oleh pengguna lain. Selain itu password tidak akan mudah dibobol.

Kata kunci: AES (Advanced Encryption Standard), waterfall, Website.

Received Maret 30, 2022; Revised April 12, 2022; Accepted Mei 15, 2023
* Fadlullah Fadlullah, 190631100001@student.trunojo.ac.id

LATAR BELAKANG

Seiring berselangnya masa ke masa, juga semakin pesat pula perkembangan teknologi di bidang informasi. Perkembangan tesebut dapat menyebabkan berubahnya pola berfikir masyarakat dalam berkomunikasi. Dulu cara yang dilakukan oleh masyarakat untuk berkomunikasi jarak jauh masih manual yaitu dengan menggunakan kertas yang bertuliskan pesan penting atau yang disebut dengan surat (Rosyadi, 2012). Surat merupakan sebuah sarana untuk komunikasi dan menyampaikan pesan atau informasi yang tertulis pada kertas yang dilakukan oleh pihak penulis kepada pihak penerima baik perseorangan maupun kelompok (Junus, 2018). Ternyata cara ini kurang efisien jika surat tersebut dibutuhkan dalam waktu yang singkat, kemudian kurang terjaganya keamanan dari isi surat tersebut, dan juga memerlukan biaya yang mahal. Selain itu, penyimpanan surat tidak bisa di simpan di sembarang tempat harus menggunakan pengamanan khusus untuk menyimpannya.

Kurangnya efisiensi dalam pengiriman surat mendoronng pola pikir masyarakat untuk menciptakan inovasi yang memudahkan komunikasi jarak jauh. Media komunikasi saat ini yang masih sering digunakan untuk mengirimkan dokumen-dokumen penting dapat melalui SMS, email, whatsapp dan internet (Rosyadi, 2012). Perkembangan teknologi informasi ini juga memberikan efek positif dan negatif. Efek negatif dari perkembangan teknologi pengiriman pesan adalah adanya penyadapan data yang membuat user merasa kurang aman (Prameshwari & Sastra, 2018). Salah satu cara untuk mengamankan kebobolan data yaitu dengan mengamankan password email pengirim dan penerima (Nuari & Ratama, 2020).

Metode yang digunakan untuk mengamankan password login sebuah sistem informasi ini dengan menggunakan kriptografi AES (Advanced Encryption Standard). Penggunaan kriptografi dalam pengamanan password login sebuah sistem informasi akan lebih terjaga. AES (Advanced Encryption Standard) merupakan sebuah algoritma selaras yang biasanya digunakan untuk enkripsi dan deskripsi sebuah dokumen, password dll (Azhari et al., 2022). Pada penelitian ini, algorita AES ini digunakan atau diterapkan untuk proses enkripdi dan deskripsi sebuah password login sebuah sistem informasi. User sistem informasi tersebut harus memiliki sebuah akun yang nantinya kriptografi AES ini akan mengubah tampilan password tersebut yang awalnya berbentuk karakter atau deskripsi akan dirubah menjadi enkripsi atau simbol tidak jelas dan belum terbaca

(Prayudha et al., 2019). Dengan adanya pengamanan password login sistem informasi, diharapkan mampu untuk menjaga pesan yang akan disampaikan oleh pengirim dan meminimalisir transparasi data pengguna.

AES merupakan salah satu algoritma simetris yang dapat dimanfaatkan sebagai algoritma dekripsi dan enkripsi sebuah file dan data. Algoritma AES diterapkan untuk proses enkripsi dan deskripsi sebuah e-mail (Azhari et al., 2022). Penggunaan kriptografi dengan algoritma AES melalui penyandiaan yang berulang atau ronde (Mustika, 2020). Kriptografi merupakan sebuah ilmu yang digunakan untuk teknik enkripsi data dokumen. Proses kriptografi yang nantinya akan dilakukan pengacakan sebuah kunci enkripsi yang nantinya diubah menjadi sebuah kunci acak yang tidak dapat terbaca tanpa mengetahui kuncinya (Sarofa, 2017).

Pembuatan sistem informasi ini berbasis website dengan bahasa pemrograman PHP dan HTML Alasan dalam pembuatan dengan pemilihan menggunakan sistem informasi adalah sistem informasi dapat mempermudah dalam proses pengelolaan data (Hasan & Muhammad, 2020). HTML adalah salah satu bahasa pemrograman yang dapat digunakan dalam penampilan data dokumen dalam sebuah web (Jayanti & Siska, 201M). Website adalah kumpulan halaman web yang saling berkaitan untuk menyajikan informasi tertentu, yang bisa diakses di internet menggunakan web browser (Chrome, Firefox, dll). Website merupakan situs yang terdiri dari beberapa halaman yang dapat menampilkan sebuah informasi, teks, gambar, suara dan lainnya (Haerulah & Ismiyatih, 2017).

Bahasa pemrograman PHP atau yang disebut dengan Hypertext Preprocessor merupakan salah satu bahasa pemrograman yang digunakan untuk penulisan skrip atau kode yang terbuka yang dominan digunakan di dalam bahasa pemrograman dan pengembangan sebuah website (Setiawan, 2022). Bahasa pemrograman PHP ini biasanya banyak digunakan dan di aplikasikan di dalam komunikasi server, dan hal tersebut juga di tunjang hampir keseluruhan sistem. XAMPP merupakan salah satu software web server yang berfungsi untuk mendesain dan membuat sebuah situs website lebih berkembang, terutama pada server lokal. XAMPP atau yang disebut dengan localhost XAMPP ini berfungsi untuk membuat sebuah server lokal di sebuah komputer atau PC. Penggunaan XAMPP terdabat data-data yang harus dibuat biasanya disebut dengan database. Data base memiliki pengertian sebagai kumpulan dari beberapa data yang disesuaikan dengan

kebutuhan dalam pembuatan website. Selain itu database juga disebut dengan mekanisme dalam penggunaan XAMPP sebagai penyimpanan informasi atau data (Octafian, 2011).

HTML atau Hypertext Markup Language merupakan sebuah bahasa yang digunakan untuk tanda standarnya sebuah dokumen yang nantinya akan dirancang dan akan ditampilkan di jejaring media sosial atau internet. Bahasa HTML ini biasanya disandingkan atau dilengkapi dengan CSS atau Cascading Style Sheets agar tampilan website nya lebih menarik user pengguna. Selain dilengkapi dengan CSS, HTML juga dilengkapi dengan bahasa skrip yang lain seperti bahasa pemrograman JavaScript dan PHP. CSS berasal dari Cascading style sheets yang memiliki arti skrip yang dapat digunakan dalam proses desain sebuah website (Anindhita, 2016). Meskipun HTML memiliki vitur untuk mengatur tampilan website, namun pada dasarnya kemampuannya masih kurang maksimal. Oleh karena, itu perlunya CSS sebagai pendukung dalam pemberian pengaturan yang lebih lengkap. Hal ini digunakan agar website yang dibuat dapat terstruktur, rapi dan menarik (Josi, 2017).

KAJIAN TEORITIS

A. HTML

HTML merupakan bahasa markup yang menjadi standar untuk membuat halaman pada aplikasi website. Menurut Rio dalam (Sri Lestari dan Ardina Desi Susana, 2016). HTML merupakan bahasa markup yang fleksibel dimana kita bisa menuliskan script dari bahasa pemrogaman lain seperti java, C, visual basisc dan lain-lain. HTML digunkan untuk membuat sebuah paragraf, heading atau link pada sebuah halaman web. HTML menjadi pondasi dasar yang harus dipelajari untuk mengembangkan website.

B. CSS

CSS (cascading style sheet) bahasa pemrograman berfungsi untuk mempercantik tampilan web (Solichin, 2016:10). CSS digunakan untuk mempercantik tampilan website. CSS dapat dengan mudah di program untuk menentukan tata letak dan mempercantik halaman web dengan mengatur elemen warna, sudut bulat, hingga animasi.

C. PHP

PHP (Hypertext Preprocessor) adalah sebuah Bahasa pemograman yang memiliki fungsi untuk menerjemahkan baris kode program menjadi kode mesin yang dapat dibaca oleh computer (Supono dan Putratama, 2016). Betha sidik mengemukakan dalam bukunya yang berjudul Pemrograman Web Dengan PHP, mengatakan bahwa PHP PHP sebagai Bahasa pemrograman yang menjadikan dokumen HTML akan di eksekusi pada server web, dokumen yang dihasilkan bukanlah dokumen yang dibuat dengan menggunakan editor teks HTML. Sedangkan Solichin, Achmad (2016 : 11) menyebutkan bahwa PHP merupakan sebuah bahasa pemrograman berbasis web yang ditulis untuk pengembang web.

D. *Electronic Mail*

Electronic mail atau yang biasa disebut *email* merupakan sebuah *platform* berbasis digital yang berupa metode pengiriman surat secara elektronik sesuai dengan namanya(Marwasih, 2014). *Email* memiliki keunggulan dalam kecepatan dan kepraktisan dalam pengiriman surat secara elektronik, jangka pengiriman hanya berjeda beberapa detik saja sejak pengguna mengirim pesan tersebut. *Electronic mail* memiliki pengaruh yang cukup besar dalam bidang ilmu komunikasi untuk seluruh kalangan di penjuru dunia.

E. Autentikasi

Autentikasi merupakan suatu proses dalam memverifikasi suatu otoritas atau hak terhadap seseorang untuk menakses sebuah aplikasi maupun *website*(Guntoro & Muhammad. 2018). Seorang pengguna akan dituntut untuk memenuhi berbagai syarat yang dibutuhkan bagi autentikasi agar dapat melakukan pengaksesan. Autentikasi diperlukan sebagai upaya perintegrasian dalam suatu sistem layanan aplikasi untuk meningkatkan tingkat keamanan data.

F. AES

AES merupakan salah satu algoritma simetris yang dapat dimanfaatkan sebagai algoritma dekripsi dan enkripsi sebuah file dan data. Algoritma AES diterapkan untuk proses enkripsi dan deskripsi sebuah e-mail (Azhari et al., 2022). Penggunaan kriptografi dengan algoritma AES melalui penyandiaan yang berulang atau ronde (Mustika, 2020). Kriptografi merupakan sebuah ilmu yang digunakan untuk teknik

enkripsi data dokumen. Proses kriptografi yang nantinya akan dilakukan pengacakan sebuah kunci enkripsi yang nantinya diubah menjadi sebuah kunci acak yang tidak dapat terbaca tanpa mengetahui kuncinya (Sarofa, 2017).

G. Database

Database adalah sebuah sistem yang memudahkan dalam memproses data dikarenakan semua data saling berhubungan dan terorganisir ke dalam satu himpunan (Andi dalam (Rusmayanti, 2014)). Dalam praktiknya, semua data di dalam database terhubung melalui tabel-tabel yang berkaitan satu sama lain untuk keperluan tertentu seperti kepemilikan barang dan lain lain

H. Sistem Informasi

Sistem informasi merupakan sebuah sistem yang ditujukan untuk keperluan organisasi, dimana sebuah organisasi memiliki berbagai kebutuhan seperti transaksi harian, informasi kegiatan operasi (manajerial), dan memperlancar pembuatan laporan bulanan (Puspitasari, 2016).

METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah metode waterfall. Menurut Oka dalam (Utami & Apridiansyah, 2019) waterfall adalah salah satu model pengembangan simpel dan memiliki metode yang sejalan pada setiap tahapnya, output dari tahap sebelumnya adalah input untuk tahap selanjunya. Aktifitas yang dilakukan ialah analisis kebutuhan, desain sistem, tahap pengkodean, tahap uji coba dan perawatan sistem.

Penelitian ini menggunakan metode waterfall. Tahapan penelitian pengembangan ini dapat dilihat sebagai berikut:

A. Analisis Kebutuhan Sistem

Kebutuhan sistem aplikasi yang dikembangkan terbagi menjadi beberapa bagian yaitu kebutuhan sistem, kebutuhan pengguna, kebutuhan perangkat keras dan perangkat lunak.

1. Kebutuhan sistem

   website yang dibuat untuk mengamankan password untuk login sistem informasi membutuhkan data atau akun user yang hendak login ke dalam sistem informasi. Website ini dapat dikelola oleh admin untuk mengenkripsikan password user.

2. Kebutuhan perangkat keras

   Kebutuhan perangkat keras dari sistem ini meliputi 1) PC/Laptop 2) Smartphone 3) Koneksi Internet.

3. Kebutuhan perangkat lunak

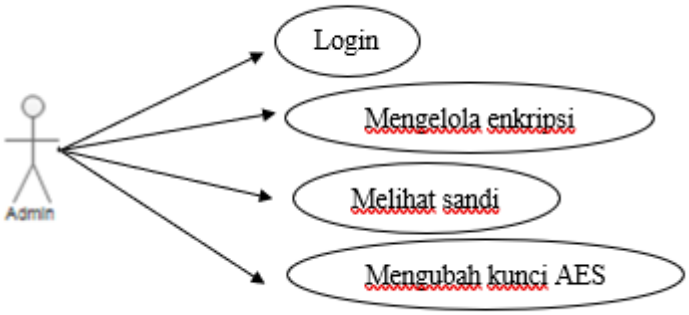
   Kebutuhan perangkat lunak yang diperlukan untuk mengembangkan website ini meliputi PHP versi 7.2,, Xampp, Web Browser

4. Kebutuhan pengguna

   Adapun pengguna dari website ini ialah admin dan masyarakat umum sebagai pengunjung.

B. Desain Sistem

1. Use case diagram



Gambar 1. Use Case Diagram

2. Perancangan basis data

   a. Tabel Pengaturan

      Tabel 1. Pengaturan Data base

No	Nama Field	Type Data	Lebar	Keterangan
1.	id_pengaturan	Int	-	Primary Key
2.	nm_app	Varchar	-	
3.	enkripsi	Varchar	-	

b. Tabel User

Tabel 2. Tabel User

No	Nama Field	Type Data	Lebar	Keterangan
1.	id_users	Int	-	Primary Key
2.	nama_users	Varchar	-	
3.	email_users	Varchar	-	
4.	nomor_users	Varchar	-	
5.	pass_users	Varchar	-	

C. Koding

Tahap ini merupakan implementasi pengkodean dari pembuat sistem.

D. Pengujian Sistem

Pada tahap pengujian sistem ini dilaksanakan menggunakan uji ahli sistem dengan menggukan uji black box dan uji pengguna yang menggunakan skala likert.

E. Perawatan Sistem

Tahap terakhir yang dilakukan yaitu tahap perawatan. Sistem informasi yang telah jadi akan dijalankan dan dilakukan perawatan. Perawatan yang dimaksud meliputi perawatan dalam perbaikan kesalahan pada langkah sebelumnya yang belum diketahui.

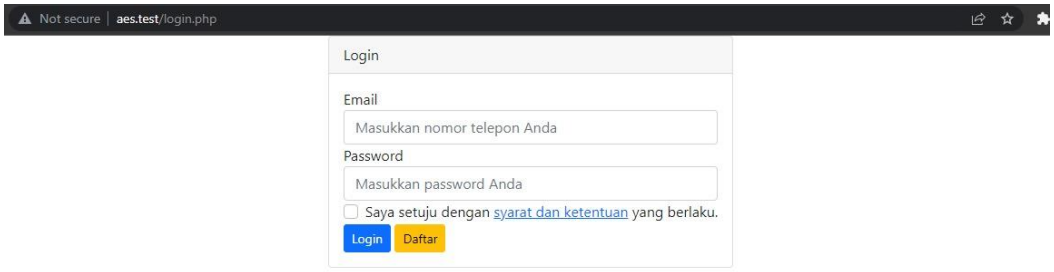
HASIL DAN PEMBAHASAN

A. Hasil

Hasil yang diperoleh dari penelitian ini merupakan sebuah website sederhan yang mengamankan password user sebuah sistem informasi.

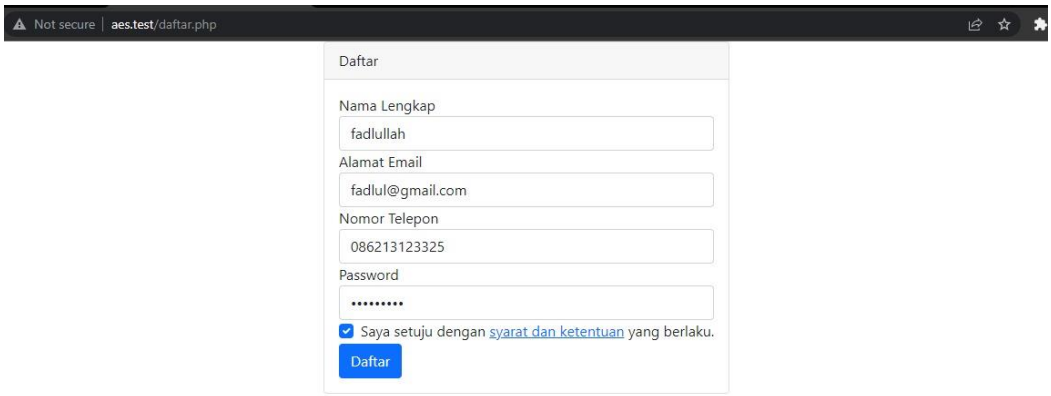
e-ISSN: 2963-4768; p-ISSN: 2963-5934, Hal 251-263

1. Halaman Login



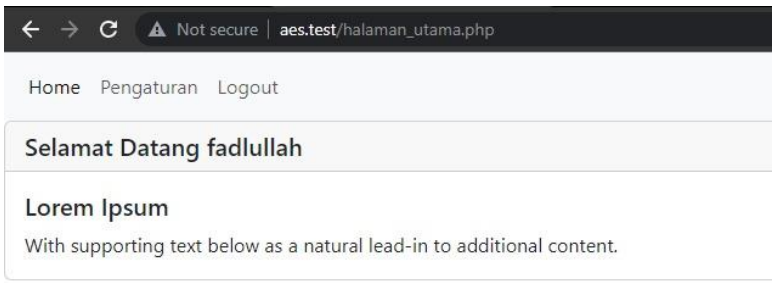
Gambar 2. di atas merupakan halaman login yang berisikan form untuk menginputkan email dan password. Setelah mengisi selurun inputan maka pengguna dalam klik tombol Login.

2. Halaman daftar



Gambar 3. Halaman daftar merupakan halaman bagi pengguna untuk mendaftarkan akun baru di website sederhana ini. Pengguna dapat mengisikan data sesuai dengan form yang disediakan.

3. Halaman Utama

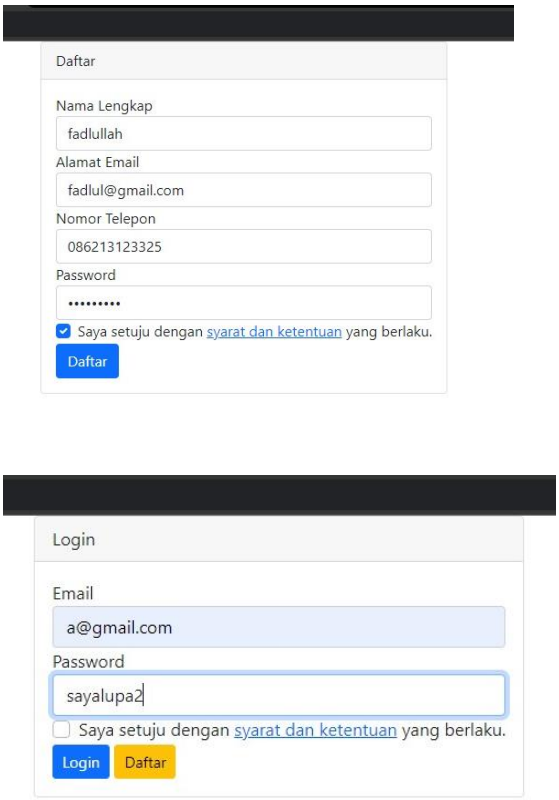


Gambar 4. Halaman Utama merupakan halaman yang akan ditampilkan ketika pengguna berhasil melakukan Login.

B. Hasil proses enkripsi dan deskripsi

1. Proses enkripsi

Tabel 3. Tabel Proses Enkripsi

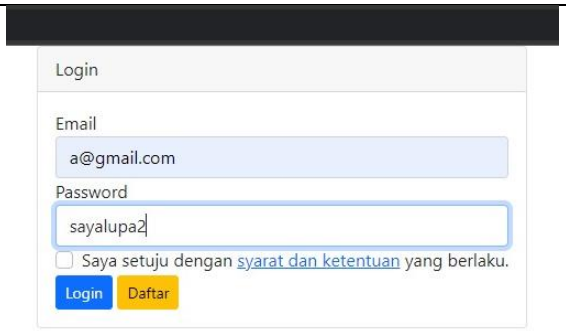
Skenario pengujian	Hasil pengujian
Pengguna mengetikkan password dengan plaintext pada halaman daftar dan login	
Pengamatan	Setelah dilakukan proses enkripsi maka hasil chipertext nya sebagai berikut: 
Kesimpulan	sukses

2. Proses dekripsi

Langkah awal dari proses deskripsi adalah dengan cara mengambil password berdasarkan email yang di inputkan.

e-ISSN: 2963-4768; p-ISSN: 2963-5934, Hal 251-263

Tabel 4. Tabel Proses Deskripsi

Skenario pengujian	Hasil pengujian
Pengguna mengetikkan email dan password dengan plaintext pada halaman login kemudian klik Login	
Pengamatan	Setelah dilakukan proses dekripsi maka hasil plaintext nya sebagai berikut: 
Kesimpulan	sukses

KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian proses enkrisi dan deskripsi menggunakan Algoritma AES maka kita menyimpulkan bahwa algoritma AES dapat diterapkan untuk melakukan enkripsi pada password, sehingga password tidak dapat dengan mudah dibaca oleh pengguna lain. Selain itu password tidak akan mudah dibobol.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih atas dukungan Universitas Trunojoyo Madura melalui skema Penelitian Universitas Trunojoyo Madura Tahun 2023. Penelitian ini merupakan bagian dari grup riset Informatics Learning

DAFTAR REFERENSI

Artikel Jurnal

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

Guntoro & Muhammad. 2018. Perancangan Aplikasi *Single-On* (SSO) Menggunakan Otentikasi Gambar. *Jurnal Teknologi & Komunikasi Digital Zone*. 9 (1). Universitas Lancang Kuning

Haerulah, E., & Ismiyatih, S. (2017). Aplikasi E-Commerce Penjualan Souvenir Pernikahan Pada Toko " Xyz ." Jurnal PROSISKO, 4(1), 43–47. http://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/146

Hasan, S., & Muhammad, N. (2020). Sistem Informasi Pembayaran Biaya Studi Berbasis Web Pada Politeknik Sains Dan Teknologi Wiratama Maluku Utara. IJIS - Indonesian Journal On Information System, 5(1), 44. https://doi.org/10.36549/ijis.v5i1.66

Jayanti, D., & Siska, I. (201M). Sistem Informasi Penggajian Pada CV . Blumbang Sejati Pacitan. Journal Speed - Sentra Penelitian Engineering dan Edukasimasalah, 6(3), 36–43. http://ijns.org/journal/index.php/speed/article/view/1041%0Ahttp://ijns.org/journal/index.php/speed/article/view/1041/1029

Josi, A. (2017). Penerapan Metode Prototyping Dalam Membangun Website Desa (Studi Kasus Desa Sugihan Kecamatan Rambang). Jti, 9(1), 50–57.

Junus, M. (2018). Sistem Informasi Pengelolaan Surat Masuk & Surat Keluar Jurusan Teknik Elektro Politeknik Negeri Malang Berbasis Web Melalui Jaringan Intranet Polinema. Jurnal Eltek, 16(2), 18. https://doi.org/10.33795/eltek.v16i2.97

Lestanti, Sri, and Ardina Desi Susana. 2016. "Sistem Pengarsipan Dokumen Guru Dan Pegawai Menggunakan Metode Mixture Modelling Berbasis Web." ANTIVIRUS: Jurnal Ilmiah Teknik Informatika 10 (2): 69–77. https://doi.org/10.30957/antivirus.v10i2.164.

Marwasih, Anhar. 2014. Pengaruh Electronin Mail Sebagai Media Komunikasi Terhadap Mengerjakan Tugas Kuliah Mahasiswa. *eJournal Ilmu Komunikasi*. 2 (1). Universitas Mulawarman

Mustika, L. (2020). Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web. JURIKOM (Jurnal Riset Komputer), 7(1), 148. https://doi.org/10.30865/jurikom.v7i1.1943

Nuari, R., & Ratama, N. (2020). Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping. Journal Of Artificial Intelligence And Innovative Applications, 1(2), 2716–1501. http://openjournal.unpam.ac.id/index.php/JOAIIA

Octafian, D. T. (2011). DESAIN DATABASE SISTEM INFORMASI PENJUALAN BARANG (Studi Kasus : Minimarket "Grace" Palembang). Jurnal Teknologi Dan Informatika (Teknomatika), 1(2), 148–157.

Puspitasari, D. (2016). Sistem Informasi Perpustakaan Sekolah Berbasis Web. *Jurnal Pilar Nusa Mandiri Vol. XII*, *12*(2), 227–240.

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. Eksplora Informatika, 8(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Prayudha, J., _ S., & _ I. (2019). Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), 18(2), 119. https://doi.org/10.53513/jis.v18i2.150

Rusmayanti, A. (2014). Sistem Informasi Pengelolaan Keuangan Pada Desa Ngadirejan. *Journal Speed-Sentra Penelitian Engineering Dan Edukasi*, *6*(2), 35–39.

Rosyadi, A. (2012). Implementasi Algoritma Kriptografi AES untuk Enkripsi dan Deskripsi Email. Transient, 1(3), 2–6.

Sarofa, ardo. P. (2017). Implementasi Algoritma AES (Advanced Encryption Standard) untuk Enkripsi URL pada Aplikasi Inventaris Aset Berbasis Web.

Solichin, A. (2016). Pemrograman web dengan PHP dan MySQL. Penerbit Budi Luhur.

Buku Teks

Anindhita. (2016). *Pengenalan HTML dan CSS*.

Setiawan, D. (2022). *Buku Sakti Pemrograman Web*.