Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI) p-ISSN: 2620 – 5327
Volume 7 Nomor 2, Oktober 2024 e-ISSN: 2715 – 5501
DOI : 10.57093/jisti.v7i2.269

# Implementasi Algoritma *Advanced Encryption Standard* Untuk Keamanan Data Customer Pegadaian UPC Pacongkang

**Hasbi[1], Andi Nurlinda Thamrin[2]**
Program Studi Rekayasa Perangkat Lunak, Universitas Muhammadiyah Palopo[1,2]
Jl. Jenderal Sudirman No.Km. 03, Binturu, Kec. Wara Sel., Kota Palopo, Sulawesi Selatan[1,2]
hasbi@umpalopo.ac.id*[1], andinurlindathamrin@umpalopo.ac.id[2]

**Kata Kunci :**
*Advanced Encryption Standard*, Kemanan Data, Website,

**ABSTRAK**
Permasalahan yang ada pada Pegadaian UPC Pacongkang adalah sering terjadi kebocoran data customer yang membuat perubahan data secara tiba-tiba, seperti jangka waktu peminjaman customer berubah dan bahkan jumlah peminjaman customer berubah. Hal ini tentunya merugikan pihak Pegadaian UPC Pacongkang dan *customer*. Melihat permasalahan tersebut pihak Pegadaian UPC Pacongkang membutuhkan metode pengamana data yang dapat membantu menjaga kerahasiaan data *customer*. Tujuan penelitian ini untuk memuat sistem keamanan data dengan penerapan konsep kriptografi. Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Untuk menerapkan kriptografi pada sistem keamanan data dibutuhkan suatu algoritma mesin autentukasi data. Salah satu metode yang dapat digunakan adalah *Advanced Encryption Standard (AES). Hasil penelitian menunjukkan dengan* diimplementasikan Kriptografi Superenkripsi Menggunakan Metode *Advanced Encrytion Standard* Pada Pengamanan Data *Customer* Pegadaian UPC Pacongkang. File data nasabah Pegadaian UPC Paconggkang menjadi aman dan tidak mudah dimanipulasi oleh orang lain karena pesan asli sudah diubah menjadi file acak yang tidak bisa dimengerti.

***Keywords***
*Data Mining Advanced Encryption Standard, Data Security, Website.*

***ABSTRACT***
*The problem that exists at Pegadaian UPC Pacongkang is that customer data leaks often occur which make sudden changes to data, such as the customer's loan period changes and even the amount of customer loans changes. This is certainly detrimental to the Pacongkang UPC Pawnshop and the customer. Seeing this problem, Pacongkang UPC Pawnshop needs a data security method that can help maintain the confidentiality of customer data. The purpose of this research is to load a data security system by applying the concept of cryptography. Cryptography aims to secure data content or maintain the confidentiality of information from people who are not entitled to know the contents of the data. To apply cryptography to the data security system, a data authentication engine algorithm is needed. One method that can be used is Advanced Encryption Standard (AES). The results showed that by implementing Superencryption Cryptography Using the Advanced Encrytion Standard Method on Customer Data Security Pegadaian UPC Pacongkang. Paconggkang UPC Pegadaian customer data files are safe and not easily manipulated by others because the original message has been converted into a random file that cannot be understood.*

## PENDAHULUAN

Pegadaian atau rumah gadai adalah sebuah individu atau lembaga yang menawarkan jasa peminjaman uang kepada masyarakat dengan jaminan benda milik masyarakat yang ingin melakukan pinjaman uang. Bila suatu barang digadaikan untuk mendapatkan pinjaman dari pegadaian, maka pada waktu yang telah ditentukan oleh pegadai boleh membeli kembali atau menebus kembali barang yang telah digadaikan dengan biaya tambahan atau bunga sebagai keuntungan pihak pegadaian. Dalam menjalankan aktifitas pelayanan pegadaian, membutuhkan administrasi baik data administrasi *customer* atau data peminjaman dipegadaian (Lestari et al., 2015).

Data pegadaian merupakan suatu hal yang sangat berharga di zaman teknologi informasi saat ini. Khusunya jika data tersebut sangat rahasia dan tidak semua orang boleh mengaksesnya. Perusahaan atau lembaga lainnya memiliki data yang sangat penting sehingga data tersebut tidak boleh diakses setiap orang, terutama perusahaan atau lembaga yang bergerak dibidang jasa pegadaian.

Salah satu pegadaian yang ada di Kabupaten Soppeng adalah Pegadaian UPC Pacongkang. Pegadaian UPC Pacongkang memiliki data yang sangat rahasia yang tidak boleh diketahui oleh setiap orang, khususnya data *customer*. Hal ini disebabkan data ini hanya ditujukan untuk pihak perusahaan dan tidak boleh terpublikasi. Maka diperlukan suatu keamanan data. Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan. Salah satu dampak negatif dalam perkembangan teknologi adalah pencurian data. Pencurian data ini tentunya merugikan bagi pemilik data, untuk menghindari kejahatan tersebut maka dibutuhkan pengamanan dalam penyimpanan data yang dianggap penting agar terhindar dari kejahatan teknologi informasi atau tidak mudah dapat diakses oleh orang yang tidak memiliki hak.

Permasalahan yang ada pada Pegadaian UPC Pacongkang adalah sering terjadi kebocoran data customer yang membuat perubahan data secara tiba-tiba, seperti jangka waktu peminjaman customer berubah dan bahkan jumlah peminjaman customer berubah. Hal ini tentunya merugikan pihak Pegadaian UPC Pacongkang dan *customer*. Melihat permasalahan tersebut pihak Pegadaian UPC Pacongkang membutuhkan metode pengamana data yang dapat membantu menjaga kerahasiaan data *customer*.

Perkembangan teknologi dibidang pengamanan data sudah banyak yang dapat digunakan oleh pihak perusahaan. Salah satu metode teknologi keamanan data adalah kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data**.** Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut (Han & goleman, daniel; boyatzis, Richard; Mckee, 2019). Untuk menerapkan kriptografi pada sistem keamanan data dibutuhkan suatu algoritma mesin autentukasi data. Salah satu metode yang dapat digunakan adalah *Advanced Encryption Standard (AES).*

Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext* sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai *plaintext.*

Keuntungan menggunakan algoritma *Advanced Encryption Standard* pada kriptografi Sistem Keamanan data *customer* pada Pegadaian UPC Pacongkang dapat menyembunyikan informasi asli dari data sehingga tidak mudah diketahui oleh orang yang tidak berkepentingan. Dengan sistem keamanan *Advanced Encryption Standard* orang lain tidak dapat mengerti dengan isi data didalam file sehinggah susah untuk merubah data.

## KAJIAN PUSTAKA

### 1. Sistem Keamanan Data

Keamanan data adalah prosedur yang didukung oleh peraturan dan tekhnologi untuk melindungi data terhadap perusakandata, pengubahan data, dan distribusi data yang disengaja atau tidak disengaja. Keamanan Data Ada tiga alasan mengapa keamanan data itu penting. Yang pertama adalah untuk mencegah potensi kerugian material. Kedua, risiko penyalahgunaan data/informasi harus dimitigasi (Uminingsih et al., 2022). Yang terakhir membantu meminimalkan peluang untuk kegiatan kriminal. Keamanan data sangat penting akhir-akhir ini, karena setiap kebijakan pengambilan keputusan harus berbasis data. Banyak data berisi informasi penting dan terbatas pada pengetahuan mereka yang terkena dampak. Faktor keamanan data sangat penting dan harus diperhatikan. Salah satu cara untuk meningkatkan keamanan data Anda adalah mengenkripsinya dengan metode kriptografi. (Karman et al., 2019)

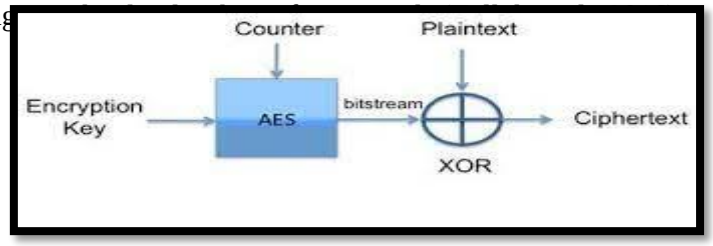
### 2. Kriptografi

Kriptografi berasal dari kata Yunani yang menggabungkan dua kata: cryptocurrency dan graphene. Kryptos artinya tersembunyii atau *secret* dan *graphenee* artinya menulis. Kriptografi secara harfiah berarti menulis rahasia untuk mengirim pesan yang harus dirahasiakan. Arti lain dari kriptografi adalah mengenkripsi teks biasa (*plaintext*) secara acak dengan kunci penyandian, membuat plainteks sulit dibaca oleh pihak yang tidak memiliki kunci dekripsi (*ciphertext*). Ilmu kriptografi berkembang seiring dengan kemajuan teknologi. Secara kronologis, ilmu kriptografi dapat dibedakan menjadi dua pengertian, yaitu kriptografi klasik dan kriptografi modern. Kedua interpretasi tersebut didasarkan pada penggunaan alat analisis kriptografi dan generator pesan (Febriana & S, 2017). Kriptografi adalah ilmu kriptografi di mana "teks asli" (plaintext) dienkripsi dengan kunci sandi menjadi "skrip acak" (ciphertext) yang sulit diuraikan oleh seseorang yang tidak memiliki kunci dekripsi. Anda dapat mengembalikan data asli dengan mendekripsi dengan kunci dekripsi. Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris, dimana kunci dekripsi sama dengan kunci enkripsi. Kriptografi kunci publik membutuhkan kriptografi asimetris, dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi, dan pembangkitan kunci untuk skema enkripsi asimetris lebih intensif secara komputasi daripada enkripsi simetris. Ini karena enkripsi asimetris menggunakan angka yang sangat besar (Ismail, Nusri & Rahman, 2023).

### 3. Algoritma *Advanced Encryption Standard*

*Advanced Encryption Standard (AES)* adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES 128, 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Setiap elemen *state* berukuran 1 *byte.* Proses enkripsi pada AES merupakan transformasi terhadap state secara berulang dalam 10 ronde. Setiap ronde AES membutuhkan satu kunci hasil dari generasi kunci yang menggunakan 2 transformasi yaitu subtitusi dan transformasi. Pada proses enkripsi AES mengunakan 4 transformasi dasar dengan urutan trasformasi *subbytes, shiftrows, mixcolumns,* dan *addroundkey.* Sedangkan pada proses dekripsi mengunakan invers semua transformasi dasar pada algoritma AES kecuali *addroundkey* dengan urutan transformasi *invshiftrows, invsubbytes, addroundkey,dan invmixcolumns.* Pada data teks, proses enkripsi diawali dengan mengkonversi teks menjadi kode ASCII dalam bilangan heksadesimal yang dibentuk menjadi matriks byte 4x4. Selanjutnya dilakukan beberapa trnsformasi dasar seperti *subbytes,*

*shiftrows, mixcolumns,* dan *addroundkey*. Akan tetapi ketika melakukan trasformasi data yang diproses pada setiap trasformasi berupa data biner dari matriks heksadesimal. Kriptografi AES 128 bit memiliki ruang kunci 2 128 yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehing




Gambar 1 : Alur Algoritma AES

Dari beberapa pendapat diatas dapat disimpulkan algoritma *Advanced Encryption Standard (AES)* adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit:

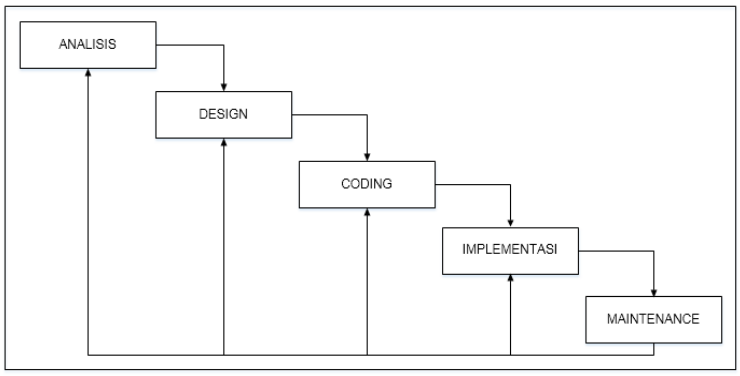
### 4. Enkripsi Data

Secara umum Enkropsi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plaintext) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (ciphertext) yang tidak dapat dibaca seecara langsung. Ciphertext tersebut dapat dikembalikan menjadi informasi awal (plaintext) melalui proses deskripsi (Ismail, Syahrir, 2021). Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal(Tahir, 2018). Contoh enkripsi pada penggunaan browser yaitu ditemukannya tanda locked pada address bar, tepat sebelum nama alamat situs. Dapat kita lihat pada support google, Ini artinya situs tersebut bersifat pribadi dan aman untuk melakukan pengiriman ataupun penerimaan data. tujuan utama enkripsi adalah untuk melindungi kerahasiaan data digital yang disimpan pada sistem komputer atau ditransmisikan melalui internet atau jaringan komputer lainnya (Riskayani et al., 2023).

## METODE PENELITIAN

### 1. Tahapan Penelitian

Penelitian ini menggunakan metode yang menerapkan model waterfall pada tahapan pengerjaan disertasi dari awal hingga akhir (Nafian et al., 2023).




Gambar 2 : Tahapan Penelitian

**2. Teknik Pengumpulan Data**

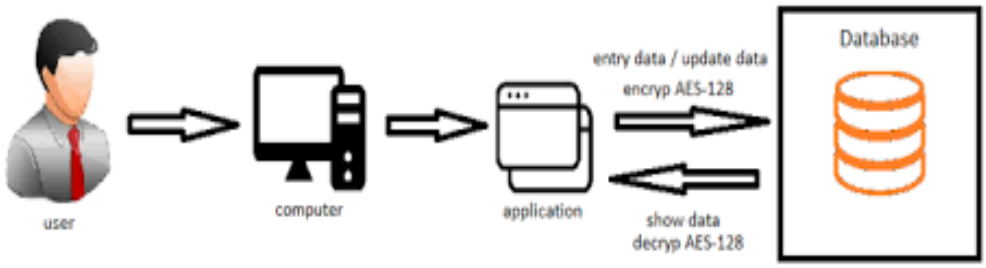
Pada penelitian ini dilakukan beberapa teknik untuk melakukan pengumpulan data yang dibutuhkan, diantaranya yaitu:

a. Observasi
Observasi merupakan pengumpulan data terkait kepuasan pengunjung yang dilakukan dengan cara mengamati proses yang berlangsung di Pegadaian UPC Pacongkang.

b. Studi Literatur
Studi literatur dilakukan dengan cara melakukan pengumpulan data berupa teori-teori yang berkaitan dengan penelitian ini dan diperoleh melalui jurnal-jurnal penelitian terkait sebelumnya.

**3. Perancangan Sistem**

Langkah-langkah yang diambil dalam merancang sistem ini membuat saran logis dan lainnya untuk pemecahan masalah. Berikut ini adalah diagram Implementasi Algoritma Advanced Encryption Standard Untuk Keamanan Data Customer Pegadaian Upc Pacongkang:



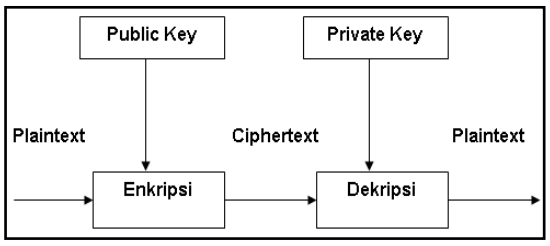

Gambar 3 : Proses Pengamanan Data dengan Metode AES

Cara kerja Advanced Encryption Standard (AES) adalah salah satu metode kriptografi kunci simetris yang paling umum digunakan untuk mengamankan data. AES menggunakan blok chiper dengan ukuran tetap (128 bit) dan mendukung kunci dengan panjang 128, 192, atau 256 bit.

## HASIL DAN PEMBAHASAN

**1. Model Algoritma**

Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Dengan teknik atau algoritma tertentu yang disebut proses enkripsi (encrypt), data diubah menjadi data sandi yang bentuknya berbeda dengan data aslinya. Berikut alur sistem Kriptografi yang digambarkan pada blok diagram.




Gambar 4 : Alur Kerja Kriptografi

p-ISSN: 2620 – 5327
e-ISSN: 2715 – 5501

Gambar 4 diatas merupakan alur kerja kriptografi, Alur kerja kriptografi mencakup langkah-langkah berikut:

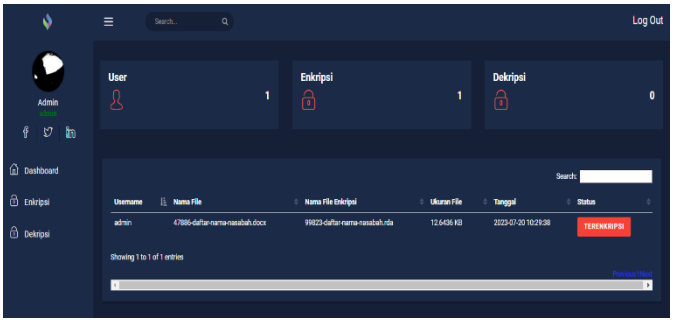
1. Tahap pertama adalah memilih algoritma kriptografi yang akan digunakan. Ada berbagai jenis algoritma yang tersedia, termasuk algoritma kunci simetris (sama kunci digunakan untuk enkripsi dan dekripsi) dan algoritma kunci publik (terdiri dari sepasang kunci - kunci publik dan pribadi)
2. Proses enkripsi adalah langkah di mana pesan asli diubah menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma kriptografi dan kunci enkripsi. Hanya penerima yang memiliki kunci dekripsi yang benar yang dapat mengembalikan pesan ke bentuk semula
3. Proses dekripsi adalah langkah di mana penerima menggunakan kunci dekripsi yang sesuai untuk mengubah ciphertext kembali menjadi pesan asli yang dapat dibaca
4. Manajemen kunci adalah bagian penting dari kriptografi, terutama pada algoritma kunci simetris. Ini melibatkan pembangkitan, distribusi, penyimpanan, dan penggunaan kunci enkripsi dan dekripsi dengan aman.

## 2. Implementasi Sistem

Pada tahapan ini dilakukan implementasi aplikasi dengan menggunakan bahasa pemrograma php. Berikut ini hasil implementasi aplikasi.

### *Halaman Utama Aplikasi*

Berikut adalah gambar tampilan halaman utama aplikasi kriptografi keamanan file:

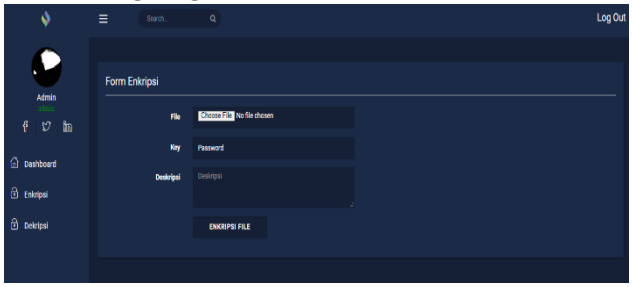



Gambar 5 : Halaman Utama Aplikasi

Gambar 5 diatas merupakan hasil implementasi halaman utama aplikasi. Halaman ini merupakan halaman yang pertama kali tampil pada saat aplikasi kriptografi dibuka.

### *Halaman Enkripsi File*

Berikut adalah gambar tampilan halaman enkripsi file kriptografi keamanan file data nasabah pegadaian UPC Pacongkang :




Gambar 6 : Halaman Enkripsi File

Gambar diatas merupakan tampilan implementasi halaman enkripsi file pada aplikasi kriptografi keamanan file. Halaman ini bertujuan untuk memproses file data nasabah menjadi pesan rahasia yang beda dengan file aslinya.

***Halaman Dekripsi File***

Berikut adalah gambar tampilan halaman Dekripsi file Kriptografi keamanan file data nasabah pegadaian UPC Pacongkang:


Gambar 7 : Halaman Ekstrak File

Gambar diatas merupakan tampilan implementasi halaman dekripsi file pada aplikasi kriptografi keamanan file data nasabah. Halaman ini bertujuan untuk memproses file yang telah dienkripsi dengan mengembalikan file aslinya/

## 3. Pengujian Sistem

Tabel 1. Hasil Pengujian Sistem

| Tes | Prosedur yang dijalankan | Hasil yang diharapkan | Hasil uji | |
|---|---|---|---|---|
| | | | Sukses | Gagal |
| Enkripsi | file tampil jika diload pada tombol add file | file tampil | 5 | 0 |
| Dekripsi File | File yang sudah di enkripsi akan didekripsi menjadi file aslinya | Dekripsi file | 5 | 0 |

Pengujian dilakukan sebanyak dua kali untuk tiap-tiap fungsi, dimana jika pengujian tiap fungsi sukses maka bernilai 1 dan jika tidak sukses maka bernilai 0.

Dari lima tabel pengujian untuk tiap-tiap fungsi diatas, akan didapat nilai persentasi hasil pengujian secara keseluruhan sebagai berikut:

Rumus: $\frac{(P1 + P2)}{F} \times 100\%$

Dimana:

P = Total Pengujian Masing-masing Tabel

F = Fungsi(Pengujian)

F= 12

Hasil: $\frac{6 + 6}{12} \times 100\% = (12/12) \times 100\% = 100\%$

Berdasarkan perhitungan diatas, maka dapat disimpulkan bahwa nilai hasil pengujian sistem yang dirancang adalah seratus persen (100%) sukses

## DAFTAR PUSTAKA

Febriana, I., & S, G. A. (2017). Penerapan Teknik Kriptografi Pada Keamanan Smsandroid. *JOEICT (Jurnal of Education and Information Communication Technology)*, *1*(1), 29–36.

Han, E. S., & goleman, daniel; boyatzis, Richard; Mckee, A. (2019). Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah. *Journal of Chemical Information and Modeling*, *53*(9), 2.

Ismail, Nusri, A. Z., & Rahman, S. (2023). Sistem Smart Trash Pemilah Sampah Organik dan Anorganik Berbasis Internet of Things. *Jurnal Saitekom*, *9*(2), 193–201.

Ismail, Syahrir, M. (2021). Sistem keamanan pesan email menggunakan algoritma kriptografi klasik. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *4*(1), 47–57.

Karman, J., Nurhasan, A., Studi, P., Informasi, S., & Insan, U. B. (2019). *PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG DI TOKO NANDA BERBASIS WEB MENGGUNAKAN METODE KRIPTOGRAFI VIGENERE CIPHER*. *11*(01), 29–36.

Lestari, A., Coyanda, J. R., & Dasrial, 2015. (2015). Sistem Infomasi Pelelangan Barang Secara Online Pada PT . Pegadaian ( Persero ) Unit Pelayanan Cabang Pasar 26 ILIR Palembang. *Jurnal Informatika Global*, *6*(1), 8–12.

Nafian, K., Irwansyah, M. A., & Sukamto, A. S. (2023). Aplikasi E-commerce Badan Usaha Milik Desa (BUMdes) Berbasis Website. *JURISTI (Jurnal Riset Sains Dan Teknologi Informatika)*, *1*(2), 17–26. https://doi.org/10.26418/juristi.v1i2.68253

Riskayani, R., Nurnaningsih, N., & Utari, E. R. (2023). Sistem Absensi Karyawan Menggunakan Radio Frequency Identification (RFID) Berbasis Mikrokontroller pada PT.Sarah Cell Telkomsel Soppeng. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *6*(1), 60–67. https://doi.org/10.57093/jisti.v6i1.149

Tahir, M. A. (2018). Implementasi Ajax Pada Aplikasi Index Artikel Berbasis Web. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika*, *1*(2), 60–68.

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. *Prosiding Matematika*, *Vol 2*(1), 1–8.

Uminingsih, Nur Ichsanudin, M., Yusuf, M., & Suraya, S. (2022). Pengujian Fungsional Perangkat Lunak Sistem Informasi Perpustakaan Dengan Metode Black Box Testing Bagi Pemula. *STORAGE: Jurnal Ilmiah Teknik Dan Ilmu Komputer*, *1*(2), 1–8. https://doi.org/10.55123/storage.v1i2.270