Application of Data Security with Encryption Method Using AES Algorithm at PLN Rayon Perawang

by Silfia Andini

Submission date: 11-Nov-2023 04:17PM (UTC+0700)
Submission ID: 2224659074
File name: plication_of_Data_Security_with_Encryption_Method_Using_AES.pdf (665.43K)
Word count: 1393
Character count: 7441

INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES)
LLDIKTI WILAYAH X
Vol. 8, No. 1, Mei 2023
e-ISSN: 2502-0692

Application of Data Security with Encryption Method Using AES Algorithm at PLN Rayon Perawang

Silfia Andini*[1], Deval Gusrion[2]
[123] University Putra Indonesia YPTK Padang

doi. 10.22216/jod.v8i1.2379
*Correspondence should be addressed to sifliaandini@upiyptk.ac.id

Article Information

Submitted :
15 Mar 2023

Accepted :
20 May 2023

Published :
30 May 2023

Abstract

Technology continues to develop, especially in the computer field, so it is very necessary to use computer security properly. Security and confidentiality are important aspects of a message, data or information. Encryption is one method of securing documents that maintains the confidentiality and authenticity of documents, and can increase the security aspects of a document or information. Advanced Encryption Standard (AES) is a symmetric algorithm used for encryption with the aim of protecting sensitive data or information using encryption and decryption techniques with key lengths of 128 bits, 192 bits and 256 bits. The results of the encryption web implementation can lock important files with a 128-Bit key. So that the level of vulnerability to data security breaches is getting lower. Which means that encryption using AES is able to overcome the prevention of vulnerabilities in the collapse of important data.

Keywords: Data Security, Encryption, AES, 128-Bit.

1. Introduction

Technology continues to develop, especially in the computer field, so it is very necessary to use computer security properly. Security and confidentiality are important aspects of a message, data or information. [1]. One important aspect for secure communication is that it can be defined as the conversion of data into a decipherable cipher code. [2]. PLN Rayon Perawang is a company engaged in electricity. In the object of this research there is a problem, namely the absence of data security or important files. So it is still potentially vulnerable to security from irresponsible people.

Cryptography is a document security method that maintains the confidentiality and authenticity of documents, and can increase the security aspects of a document or information. [3]. There are 5 aspects to data security, namely:

1.Privacy: ensuring that data or information is stored securely and privately.

2. Integrity: the authenticity of messages sent over a network and can ensure that the information sent is not changed during the transmission process.

3.Authenticity: ensuring the authenticity of data when receiving the data.

4. Avaibility: the information system is attacked or broken into can hinder access to information such as sending multiple servers.

5. Access Control: regulates the way information is accessed such as a combination of id and password. [4].

In cryptography there are 2 ways of encoding, namely encryption and decryption. Encryption is an encoding process that changes a message code that is easy to understand. Meanwhile, decryption is the opposite of encryption, which is the

process of encryption. encoding that converts an incomprehensible message code into an understandable message code. [5].

The Advanced Encryption Standard (AES) is a symmetric algorithm that It is used for encryption with the aim of protecting sensitive data or information by using encryption and decryption techniques with key lengths of 128 bits, 192 bits and 256 bits. [6]. In this study using 128-Bit AES encryption. The 128-bit AES algorithm sequence is called a data block or plaintext, while what will be encrypted becomes ciphertext. [7]. The AES algorithm encryption process has 4 types of bytes transformation, namely: AddRoundKey, SubBytes, ShiftRows and Mixcolumns. Initially the input copied to the state will undergo a byte transformation in the form of AddRoundKey, after which the state will experience SubBytes, ShiftRows, Mixcolumn and AddRoundKey byte transformations repeatedly as many as Nr. This process is called a round function. The last round does not occur in the Mixcolumn transformation. [8].

2. Research Method

The research framework is a concept that describes all the stages carried out in the research process, which connects the visualization of one variable with another. So that the research is organized systematically.

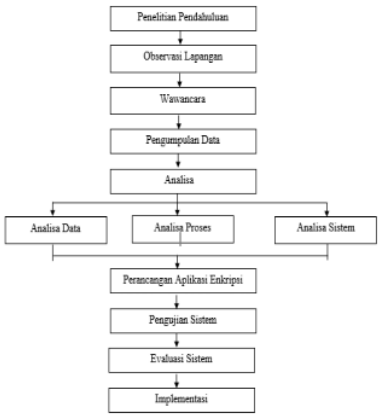

Figure 1: Research Framework

a. Study Introduction

Problem identification is carried out by approaching the object of research. The purpose of this stage is to find out the problems that occur precisely, so that it is hoped that the research can provide the most optimal solution to solving these problems.

b. Data Collection

Data collection is done by studying books and journals related to the research.

c. Analysis

This stage aims to identify the problems that exist in the system and determine the system requirements for the system being built.

1. Data Analysis

This stage is carried out after collecting data and information that has been taken through direct interviews, this data analysis stage is a process for processing data that is used as a sample. The data obtained is in the form of an Excel file. And at this stage data cleaning is also carried out by correcting data that is not formatted in excel.

2. Process Analysis

This stage of research is carried out by applying the Cryptography method using the AES (Advanced Encryption Standard) algorithm.

3. System Analysis

Description of a complete information system in its component parts.

d. System Design

The design process has 2 methods, namely designing models and designing interfaces. Model design focuses on designing the Unified Modeling Langueage (UML) which will be applied to the website, while the interface design focuses more on the appearance of the page intended for admin and staff.

3. Results of the Discussion

The system created is a website that uses the PHP programming language. Encrypted files are *.pdf and *.xls which can only be 5 MB in size.

1. Login View

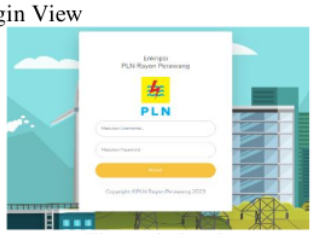

Figure 2: Login

2. Encryption Form Display

Figure 3: Form Encrypted

In Figure 3 there is a form that will be filled in by inputting the file to be encrypted, then entering the key and description of the file.

3. Display of files that have been successfully encrypted

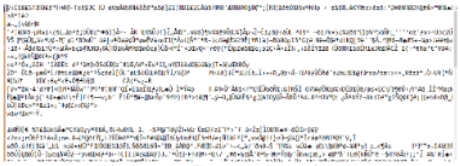

Figure 4: Encryp Result

Figure 4 is the result of a file that has been encrypted with the AES algorithm opened with notepad.

4. Display of decryption form

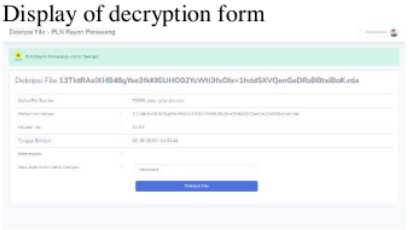

Figure 5: Form Decrypt

Figure 5 contains a form that contains a description of the file name that has been encrypted, then if you want to decrypt the file, please enter the key created during encryption.

5. Encrypted database view

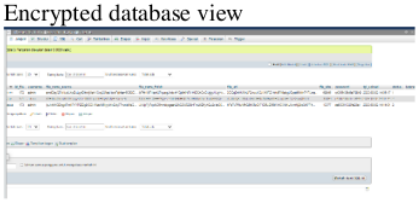

Figure 6: An Encrypted Database

Figure 6 is a database view for storing encryption and decryption files that have been done.

4. Conclusion

With the implementation of encryption on customer data at PLN Rayon Perawang, improving the security system that previously did not exist. As well as maintaining the integrity of existing data. The AES algorithm method is effectively used when decrypting a file.

References

[1] S. Aripin and M. Syahrizal, "Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 461, 2020, doi: 10.30865/mib.v4i2.2039.

[2] C. Irawan *et al*., "KEAMANAN DATA MENGGUNAKAN GABUNGAN KRIPTOGRAFI AES DAN RSA," pp. 978–979, 2021.

[3] B. E. Widodo, A. S. Purnomo, P. S. Informatika, F. T. Informasi, U. Mercu, and B. Yogyakarta, "IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN THE IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD ON THE ENCRYPTION AND DECRYPTION OF THE CONFIDENTIAL DOCUMENTS AT," vol. 1, no. 2, pp. 69–77, 2020.

[4] S. W. Deni Lestiono, "Konsep Penerapan Keamanan Jaringan Publik Di Lingkungan Kampus Stmik Bina Patria," *Transformasi*, vol. 16, no. 1, pp. 91–101, 2020, doi: 10.56357/jt.v16i1.220.

[5] R. Firdaus and R. R. Santika,

"Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security," *Semin. Nas. Mhs. Fak. Teknol. Inf. Univ. Budi Luhur*, vol. 1, no. 1, pp. 111–120, 2022.

[6] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[7] I. Dian Widyawan, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite," vol. 4, no. 1, pp. 15–22, 2021.

[8] C. Irawan and A. Winarno, "Kombinasi Algoritma Kriptogarafi Aes Dan Des Untuk Enkripsi File Dokumen Proposal," *Sendiu*, pp. 2–8, 2020.

Application of Data Security with Encryption Method Using AES Algorithm at PLN Rayon Perawang

ORIGINALITY REPORT

19%	12%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

3%

★ jom.fti.budiluhur.ac.id

Internet Source

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		