Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Implementation of Advanced Encryption Standard (AES) Algorithm for Employee Data Security at Binjai Religious Court

Dilla Silfani[1]*, Darjat Saripurna[2*], Ratih Puspadini[3*]

[1,2,3]*STMIK Kaputama Binjai, Indonesia*
dillasilfani05@gmail.com[1*], darjatsaripurna@gmail.com[2*], puspadiniratih@gmail.com[3*]

Abstract

In the digital era, data security in government institutions has become crucial, including at the Binjai Religious Court, which manages employee data in digital document form. Sensitive employee information such as identity, work history, and financial records is highly vulnerable to leakage and unauthorized access. To address this issue, this research implements the Advanced Encryption Standard (AES-128) algorithm as a data protection solution. The research methodology includes problem identification, literature study, system requirements analysis, design, implementation, and testing. The system was developed as a web-based application using PHP programming language, the CodeIgniter framework, and a MySQL database. AES is applied to encrypt and decrypt files in *.docx* and *.xlsx* formats. The test results show that encrypted files cannot be accessed without the correct key, while decrypted files can be fully restored to their original form. The encryption and decryption processes also run in relatively short times, making the system efficient and stable. In conclusion, the implementation of AES-128 successfully enhances the security of employee data at the Binjai Religious Court and can serve as a reference for other institutions in developing cryptography-based data security systems.

Keywords: *Data Security, Cryptography, Advanced Encryption Standard (AES), Encryption, Decryption*

1. Introduction

In today's digital era, the management and storage of employee data in government institutions, including the Binjai Religious Court, is increasingly dependent on electronic systems. This condition does bring benefits in terms of efficiency and ease of access, but at the same time it also poses a major challenge related to data security. The stored employee data includes sensitive information such as personal identity, employee identification numbers, employment history, and financial data, so that if it falls into the hands of unauthorized parties, it can pose serious risks. These risks include data misuse, information leakage, identity theft, and even the potential for broader cybercrime. Therefore, an encryption method is needed that is able to provide a high level of security in maintaining the confidentiality and integrity of employee data. One effective method to improve data security is to apply cryptographic techniques. Cryptography is a science used to protect information by converting it into an unreadable format without legal permission. One of the most widely used cryptographic algorithms today is the AdvancedBinjai Religious Court, the level of data security can be improved, thereby reducing the risk of illegal access and information leakage. In addition, the implementation of AES will also give more confidence to employees and related parties that their data is managed with high security standards [1].

2. Theoretical Foundation

2.1. Definition of Implementation

Implementation is a dynamic process, where policy implementers carry out an activity or activity, so that in the end they will get a result that is in accordance with the goals or objectives of the policy itself .[2]

2.2. Religious Courts

The Religious Court is one of the judicial institutions under the Supreme Court that has the authority to resolve certain civil cases for Muslims, including marriage, inheritance, will, grants, waqf, zakat, infaq, shadaqah, and sharia economics. The existence of the Religious Court has strong legitimacy after the enactment of Law Number 7 of 1989 which was later updated with Law Number 3 of 2006 and Law Number 50 of 2009. In its development, the Religious Court not only plays a role as a judicial institution, but is also required to improve the quality of public services, including the use of digital technology in administration and data management. This shows that the Religious Court is also facing the challenge of modernization in the digital era.

2.3. Definition of Cryptography

Cryptography comes from the Greek language, according to the language it is divided into two cryptos and graphia, crypto means secret and graphia means writing. According to its terminology, cryptography is a science and art to maintain the security of messages when messages are sent from one place to another. The word "art" comes from the historical fact that in the early days of cryptographic history, everyone may have had a unique way of keeping their messages secret. Securing data is carried out to maintain information confidentiality and to be safe from irresponsible people, data security is carried out using cryptographic algorithms.[3]

2.4. Definition of Advanced Encryption Standard (AES) Algorithm

The Advanced Encryption Standard is a symmetric cryptographic algorithm that operates in block cipher mode that processes 128-bit blocks of data with 128-bit, 192-bit and 256-bit key lengths. Some of the operating modes that can be applied to the AES block encoding cryptographic algorithm include Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB). The implementation of AES with the ECB, CBC, CFB and OFB modes of operation certainly has certain advantages and disadvantages in terms of the level of data security. A cryptographic algorithm named Rijndael, designed by Vincent Rijmen and John Daemen from Belgium, emerged as the winner of the DES alternative cryptographic algorithm contest held by NIST (National Institutes of Standards and Technology) of the United States government on November 26, 2001. Rijndael's algorithm became known as the Advanced Encryption Standard (AES). After undergoing several standardization processes by NIST, Rijndael was officially adopted as a cryptographic algorithm standard on May 22, 2002. In 2006, AES was one of the most popular algorithms used in symmetric key cryptography.[4]

2.5. Definition Understanding Unified Modeling Language (UML)

UML stands for Unified Modeling Languange which means standard modeling language. Wazlawick says "language that can be used to describe things". What when translated is that UML can be used to describe something. According to Wazlawick, there is a writing symbol that helps the writer to explain the expected result. The symbols in question are called notation and process. [5]

2.6. Flowchart

A flowchart is a graphical representation that shows the sequence of processes or steps in a systematic way in running a program. Flowcharts help in the process of analysis, design, and coding to solve problems in more detail. It is generally used to facilitate evaluation in problem solving. A flowchart is also a diagram that uses graphic symbols to describe the flow of a process, where each step is represented by a specific symbol. In general, a flowchart is a visualization of the steps of a program procedure with a specific purpose and serves to clarify the process to make it easier to understand, especially in showing the sequence between steps. [6]

3. Research Method

3.1. Research Methods

The research methodology is a step used to achieve the goal of this study, which is to implement the Advanced Encryption Standard (AES) algorithm to secure employee data in files with .docx and .xlsx formats at the Binjai Religious Court. This research is applied research, where the process of information collection, analysis, system design, and implementation is carried out in stages and Structured.

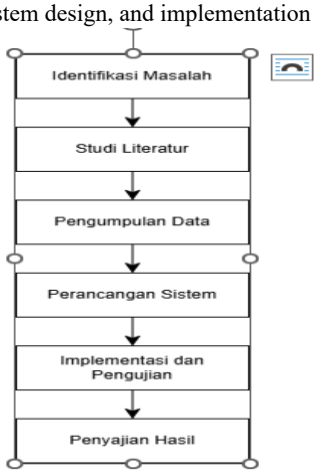

Fig. 1: Research Workflow

The explanation of each stage is as follows:

1. Identify the Problem At this stage, an analysis was carried out on the needs of the employee data security system at the Binjai Religious Court. The problem found is that there is still a potential for leakage or unauthorized access to important files containing employee data, especially those in the form of .docx and .xlsx. Therefore, it is necessary to implement an encryption-based security system to protect the data.

2. Literature Studies This stage includes the collection of relevant references and theories, such as the study of Advanced Encryption Standard (AES) algorithms, digital data security, and document and spreadsheet file processing techniques in the context of programming. This literature is the scientific basis for designing and implementing the right security system.
3. Data Collection The data collected includes .docx and .xlsx file structures, sample employee data files used as a test, as well as interviews or observations about the flow of file storage and distribution in the agency environment. The goal is to understand how files are used and where their potential security loopholes lie.
4. System Planning This stage includes designing the security system architecture to be developed, starting from file encryption and decryption workflows, user interface design, to integration schemes with .docx and .xlsx files. This design was made with reference to the results of needs analysis and theories that have been studied previously.
5. Implementation and Testing At this stage, the system that has been designed will be developed using the PHP programming language, by applying the AES algorithm for the process of encrypting and decrypting files. Testing is done to ensure that encrypted files cannot be opened without proper decryption and that the data remains intact once decrypted.
6. Presentation of Results The results of the system implementation will be presented in the form of documentation and analysis, such as the success rate of encryption, processing time, and ease of use of the system. These results also include an evaluation of whether the system has met the initial purpose of the study, which is to maintain the confidentiality of employee data at the Binjai Religious Court.

3.2. System Planning

System design is an important stage in application development that aims to ensure that the system built is in accordance with the functional and non-functional needs that have been analyzed beforehand. In this study, the system is designed to implement the Advanced Encryption Standard (AES) algorithm in carrying out the process of encrypting and decrypting files, in order to maintain the security of employee data within the Binjai Religious Court.

4. Results and Discussion

4.1. Implementation Overview

The implementation stage is the realization of the needs analysis and system design that has been carried out in the previous chapter. The system is built based on a web application using the PHP programming language and CodeIgniter framework, as well as the MySQL database as a data storage medium. The algorithm implemented is the Advanced Encryption Standard (AES-128) which functions to encrypt and decrypt employee document files in .docx and .xlsx formats. This implementation aims to protect sensitive data of employees at the Binjai Religious Court from unauthorized access, while ensuring that only authorized parties with encryption keys can access the information.

4.2. Implementasi Algoritma AES dalam Sistem

The implementation of the Advanced Encryption Standard (AES-128) algorithm in this study was realized through a web-based application. The system is built using the PHP programming language and the CodeIgniter framework which has an MVC (Model–View–Controller) structure, making it easier to separate business logic, data processing, and interface display. Meanwhile, MySQL databases are used to store information related to file metadata, such as the original file name, size, file type, encryption or decryption status, and records process time. The selection of this technology combination is based on the reasons of stability, flexibility, and broad community support, making it easier to develop and maintain the system. With this architecture, AES implementations can be executed consistently, scalably, and in accordance with data security standards.

4.3. System Interface Implementation

Antarmuka pengguna dirancang sederhana, responsif, dan mudah dipahami, dengan beberapa halaman utama sebagai berikut:

Fig. 2: Dashboard Page

Files that have gone through the encryption process cannot be opened using standard applications such as Microsoft Word or Microsoft Excel. This indicates that the contents of the file have been transformed into ciphertext that cannot be recognized in structure without going through the decryption process with the correct key. Thus, the system manages to keep the data confidential from unauthorized access.

Fig. 3: Encryption Results

The decryption process using the correct password is able to restore the file to its original form in its entirety without damaging or altering the content. The results of this test prove that the AES-128 algorithm implemented in the system can maintain data integrity, so that employee information is guaranteed to be accurate after processing.

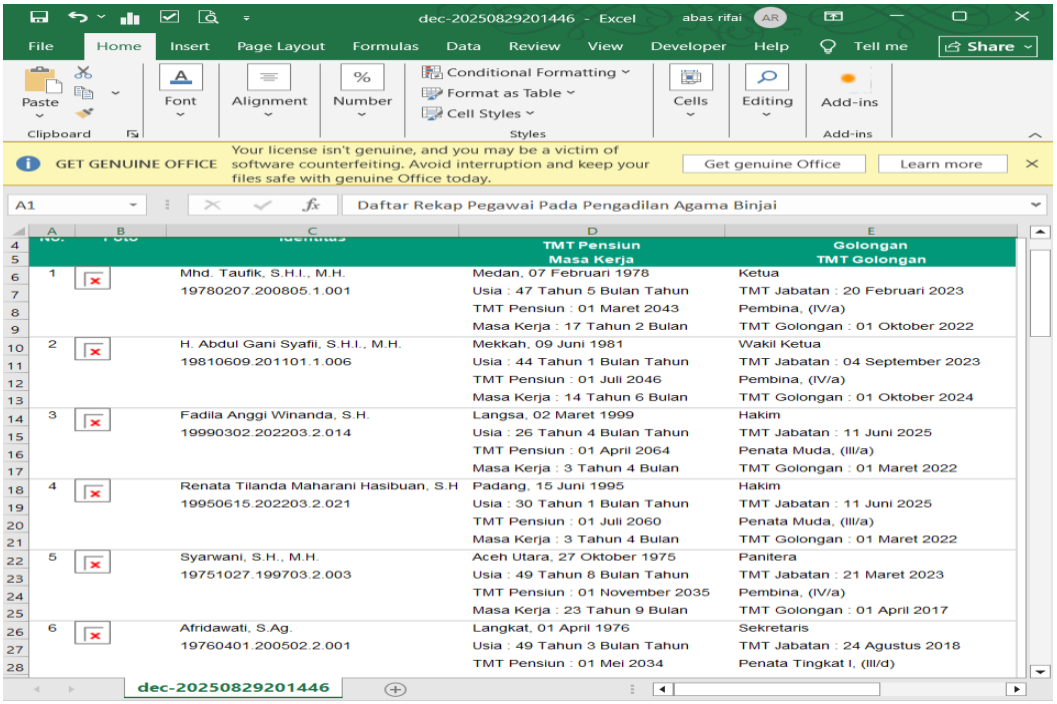

Fig. 4: Decryption Results

5. Conclusions and Suggestions

5.1. Conclusion

From the results of the association pattern analysis carried out using the A priori method, several conclusions can be drawn regarding the attributes contained in the intensity of playing online games with learning interest as follows:

1. There is no effort to balance time playing online games and studying (WUB3), then interest in lectures will be minimal (KMK1) with a confidence value of 92.3%. This proves that the tendency to play online games without any effort to balance time playing online games and learning can affect interest in learning.
2. The age factor can also affect the level of playing games and also learning interest, this is evidenced by the results of the previous analysis which shows that the age range of >20 years (UMR3) tends to affect minimal interest in lecture materials (KMK1) so it can be concluded that the age factor is an additional indicator that affects the pattern of the relationship between playing games and learning interests.
3. A priori effectiveness in decision-making The A priori method is very effective in uncovering every pattern that exists in each related attribute. These findings can be used as a basis for better time management between playing online games and learning in order to balance the time between playing and learning which can affect students' interest in learning at STMIK Kaputama.

5.2. Suggestions

The suggestions that can be given for further development and research are as follows:
1. Expansion of file formats. The system can be further developed to support other file formats such as PDF, JPG, and PNG, thus extending the reach of data security.
2. Increased lock length. To strengthen the level of security, the encryption key can be upgraded to AES-192 or AES-256 so that it is more resistant to brute force attacks.
3. User authentication integration. The system should be equipped with authentication or user management features, so that only the authorities can encrypt or decrypt files.
4. Cloud-based storage. The system can be integrated with cloud storage services so that encrypted files can be accessed securely from different locations and easier in terms of distribution.
5. Large-scale testing. Advanced research needs to test systems with more file counts and more varied data sizes to assess the stability of the system in real-world scenarios.

References

[1] F. Ardianto and T. Fatimah, "3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)," in *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi*, Jakarta, Aug. 2023.
[2] K. Wijaya, R. Supariyanto, and E. Istiawan, "Implementasi Framework Bootstrap Dalam Perancangan Sistem Penerimaan Mahasiswa Baru Pada Sekolah Tinggi Ilmu Tarbiyah Al-Quran Al-Ittifaqiah (STITQI) Indralaya berbasis Web," *J. Sist. Inf. dan Komputerisasi Akunt.*, vol. 4, no. 2.
[3] J. Prayudha, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *SAINTIKOM*, vol. 18, pp. 119–129, 2019.
[4] D. Setiawan and I. Mufarrihah, "Implementasi Metode Kriptografi Advanced Encryption Standard 128 Bit (AES 128 Bit) Pada Keamanan File Dokumen".
[5] Yuyun, Nurul Hidayah, and Supriadi Sahibu, "Algoritma Multinomial Naïve Bayes Untuk Klasifikasi Sentimen Pemerintah Terhadap Penanganan Covid-19 Menggunakan Data Twitter," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 4, pp. 820–826, 2021, doi: 10.29207/resti.v5i4.3146.
[6] K. I. Listyoningrum, D. Y. Fenida, and N. Hamidi, "Inovasi Berkelanjutan dalam Bisnis: Manfaatkan Flowchart untuk Mengoptimalkan Nilai Limbah Perusahaan," *J. Inf. Pengabdi. Masy.*, vol. 1, no. 4, pp. 100–112, 2023, doi: 10.47861/jipm-nalanda.v1i4.552.