Jurnal Krisnadana (Jurnal Komputer, Sistem Kendali & Jaringan)
Vol 4, Issue 3, Mei 2025 , pp. 122-130
https://doi.org/10.58982/krisnadana.v4i3.836

E-ISSN: 2808-3563
P-ISSN: 2808-3520

Implementation of AES Encryption for Data Security on Web-Based Information Systems in Fafinesu A Village

Fransiskus A. Naimnule[1*], Fransiska A.L Hanoe[2], Maria N. Banusu[3], Maria O. Mano[4]

[1*,2,3,4]Program Studi Teknologi Informasi, Universitas Timor
[1*]naimnulea@gmail.com, [2]hanoefransiska@gmail.com, [3]novibanusu@gmail.com, [4]ocymano@gmail.com

ARTICLE INFO

Article history:
Received 10 April 2025
Accepted 21 Mei 2025
Published 13 Juni 2025

Keywords:
Data security;
AES encryption;
Village information system;
Web-based system

ABSTRACT

The advancement of information technology has driven many institutions, including village governments, to adopt web-based information systems to enhance the efficiency and accuracy of public services. However, the use of digital information systems also presents serious challenges in terms of data security, especially for personal and sensitive information. A major concern is the risk of data breaches or unauthorized access through hacking or misuse of the system. This study aims to implement the Advanced Encryption Standard (AES) algorithm as a data protection mechanism within the web-based information system of Fafinesu A Village. AES was selected due to its proven reliability and efficiency as a symmetric encryption algorithm with a high level of security. The research stages include identifying sensitive data that needs protection, designing encryption and decryption schemes, integrating the AES module into a Laravel-based web system, and evaluating the encryption results and system performance impact. The implementation results show that all sensitive data stored in the database was successfully encrypted and can only be decrypted using a valid key within the system. Performance testing indicates that the AES integration does not significantly affect system speed. From the user's perspective, the encryption implementation increases trust in the system due to the higher level of data confidentiality and protection. This study provides a practical contribution to improving information security standards in village government environments and can serve as a model for the development of secure, modern, and trustworthy village information systems.

1. Introduction

In today's digital era, information technology has become the backbone of government administration, including at the village level. Village government as the frontline in public services has the responsibility to provide accurate, fast, and easily accessible information to the community. Therefore, the use of web-based information systems is an unavoidable

necessity. This system can assist in managing population data, archiving correspondence, document services, and reporting village government activities more effectively.

But behind this convenience, new threats related to information security have also emerged. Web-based information systems are highly vulnerable to various forms of cyber attacks, such as SQL Injection, brute-force attacks, sniffing, and data manipulation. If not equipped with adequate security mechanisms, important data such as resident identities, village decrees, and financial documents can be easily accessed or stolen by irresponsible parties. This has the potential to cause great losses both in terms of administration and public trust in the digital village government system.

One of the most important aspects of maintaining information system security is the protection of sensitive data. In the context of village government, data such as the Population Identification Number (NIK), address, letter request history, and financial reports are confidential and should only be accessed by authorized parties. If this data is leaked to the public, not only will the privacy of citizens be compromised, but also the credibility of the village government will be questioned. Therefore, it is imperative to implement security methods that protect the confidentiality, integrity, and availability of the data.

One method that is widely used in maintaining data confidentiality is through encryption. Encryption is a technique in cryptography that converts the original information into an unreadable form without a specific key. Thus, even if the data is successfully accessed illegally, its contents remain incomprehensible without the decryption process. Encryption has proven to be one of the most powerful layers of protection against cyberattacks. Using the right encryption algorithm can provide assurance that data will remain safe, even if the network or server is compromised.

The main contributions of this research are: 1) designing and implementing AES-256 encryption directly on the Laravel-based village information system; 2) evaluating the impact of system performance after encryption integration; and 3) providing a data security implementation model that can be replicated in other villages as part of the national village digitization program.

In this research, the algorithm used is Advanced Encryption Standard (AES). AES is a symmetric cryptography algorithm developed as an encryption standard by the National Institute of Standards and Technology (NIST) of the United States. AES was chosen because it has high efficiency in the encryption and decryption process and a very strong security level. In addition, AES has been widely used in various national and international information security systems, making it a reliable solution to be applied at the village information system scale.

This research was specifically conducted on the information system of Fafinesu A Village, which began to adopt digital systems for data management and public services. This information system has not previously implemented encryption technology in the data storage process, so there is great potential for data leakage if there is a security gap. Through this research, it is expected that the implementation of AES can close the gap and make the village information system more secure, structured, and reliable.

By implementing AES encryption in the village information system, this research not only aims to improve technical security, but also provides an example of simple technology implementation that can be adapted by other villages. It is hoped that the results of this research can support the village digitalization program launched by the central government,

as well as encourage awareness of the importance of data security in today's information age.

2. Method

This research uses a software engineering method approach with the aim of designing and implementing an encryption-based security system on the village information system. This approach was chosen because the main focus of the research was to build a technological solution to a real problem, namely the lack of data protection on the information system of Fafinesu Village A. The stages in this research were organized systematically starting from needs analysis, system design, development, testing, to evaluation of encryption implementation.

This research uses a software engineering method approach with the aim of designing and implementing an encryption-based security system on the village information system. This approach was chosen because the main focus of the research was to build a technological solution to a real problem, namely the lack of data protection on the information system of Fafinesu Village A. The stages in this research were organized systematically starting from needs analysis, system design, development, testing, to evaluation of encryption implementation.

Data sources came from Fafinesu A Village's information system used to manage resident data, document requests, and financial reports. Data collection was conducted using two main techniques: 1) Direct observation of the information system that is running. 2) Interviews with system operators and village officials involved in data management.

Table 1. Encrypted data types

Data Type	Description
NIK	Population Identification Number
Full Name	Personal Identity Information
Address	Resident's domicile address
Mail Request History	Village administration service data

Data Processing

a. Once the data is classified, the processing is done in several technical stages:
b. Encryption uses the AES-256-CBC algorithm through Laravel Crypt which utilizes OpenSSL. This process runs on the server side.
c. Storage: The encrypted data is stored in a MySQL database.
d. Decryption: When an authorized user accesses the system, the data is automatically decrypted by the system.
e. Key Management: Encryption keys are securely stored in an .env configuration file that can only be accessed by the server system.

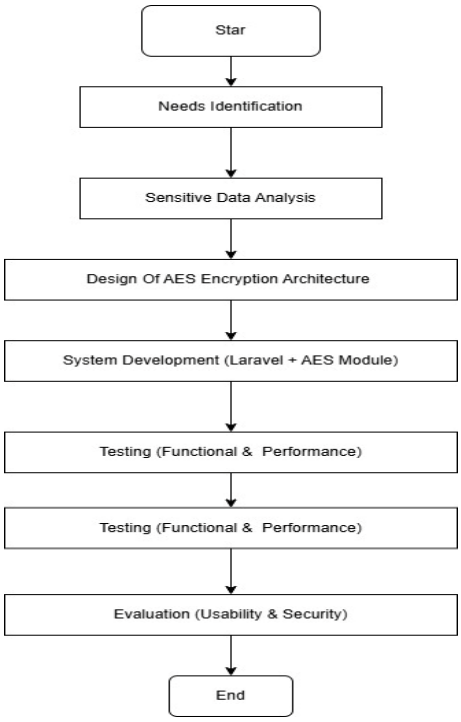

Figure 1. Flowchart of the research flow

In the initial stage, a data needs analysis was conducted to determine the type of information that needed to be protected. Sensitive data included population data (NIK, full name, address), letter request data, and official documents from the village government. The analysis was conducted through direct observation of the old system and interviews with village operators in charge of managing data. The results of this analysis became the basis for determining the point of encryption implementation in the system flow.

The next stage is the design of the security system which includes mapping the encryption and decryption flow, selecting the key storage place, and planning integration with the web system. The algorithm used is Advanced Encryption Standard (AES) with a key length of 256 bits because it is considered to have a high level of security and stable performance. Encryption is done on the server side especially when the data is stored in the database. The decryption process is done when the data is read by users who have access rights.

In the development of the system, the Laravel framework was used as the basis for the web system. Laravel was chosen because it has a Model-View-Controller (MVC) architectural structure that facilitates the integration of security modules in a separate and structured manner. For the implementation of AES encryption, the OpenSSL library and Laravel's built-in encryption feature (Crypt facade) are used which utilizes symmetric encryption with the AES-256-CBC method. The encryption key is securely stored in the .env configuration file, which can only be accessed by the server through specific permissions.

System testingThe testing process was carried out in two main aspects, namely first, testing the functionality of encryption and decryption; second, testing the performance of

the system after the application of encryption. The tests were carried out using dummy data and scenarios that reflect actual usage, such as filling out demographic data forms and requesting letters. The test results show that the data stored in the database is already in encrypted form (not directly readable), and when accessed by authorized users, the data is successfully displayed normally. In addition to functionality testing, performance testing was also conducted to see the effect of encryption implementation on system response time. This test was conducted using a benchmark method using tools such as Laravel Telescope and Debugbar to record the execution time of the data storage and retrieval process. The test results show that the addition of the encryption process only provides a very small time increase (less than 100ms), so it does not interfere with user comfort in using the system.

During the evaluation process, follow-up interviews were conducted with village operators to determine whether the system changes provided a better user experience. Operators stated that the system remained easy to use and did not require additional training, as the user interface had not changed. Confidence in the security of the system increased as operators realized that data was now protected with modern encryption technology.

Overall, the methodology applied in this research combines a technical approach and a participatory approach. The technical approach is carried out through software development, while the participatory approach is carried out by involving the end users of the system in the design and evaluation process. This aims to ensure that the solution is not only technically safe, but also suits the real needs in the field and is easy to operate by village officials.

3. Results and Discussions

The application of the AES-256 algorithm with Laravel Crypt integration in the context of village government information systems is an approach that has not been described in much detail in Indonesian academic literature. This approach offers a practical solution and can be adopted by other information systems at the village level without requiring large technical resources, thus bridging the gap between modern data security technology and its application in rural areas.

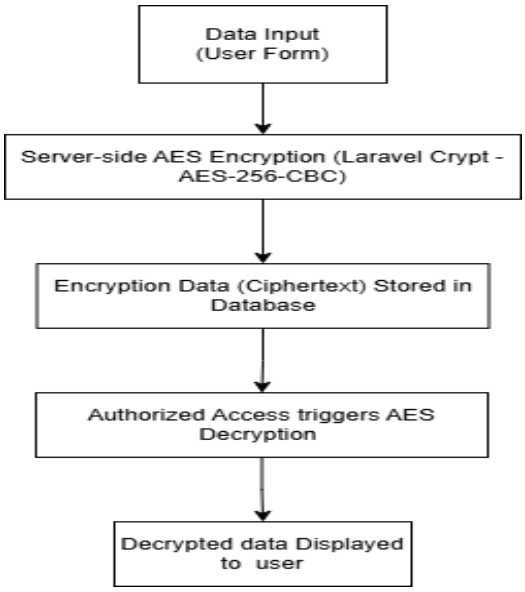

Figure 2. Flowchart of Research Flow

1 Data Input: The user enters data through a form on the web system interface.
2 Encryption Process: Data is sent to the server and automatically encrypted using AES-256 algorithm with CBC mode via Laravel Crypt utilizing OpenSSL library. The key is securely stored in the .env configuration file.
3 Storage: Encrypted data (ciphertext) is stored inside a MySQL database. Without the encryption key, this data cannot be read or understood.
4 Decryption: When data needs to be accessed by authorized users, an automatic decryption process is executed before the data is displayed on the user interface.
5 Output: The user only sees the original data (plaintext) without realizing the encryption-decryption process taking place behind the scenes.

System Implementation

System implementation is done by encrypting sensitive data using the AES-256 algorithm in a Laravel-based village information system. The encryption process takes place when the data is stored, and automatic decryption is performed when the data is accessed by authorized users, thus maintaining the confidentiality and security of the information.

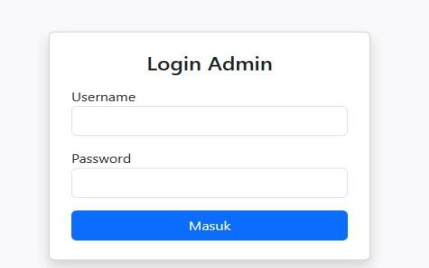

Figure 3. Admin Login Form

The admin login form is used to authenticate users before accessing the system. This form consists of username and password fields, as well as a "Login" button to verify credentials. If the data is valid, the user is directed to the system dashboard. This form is the first layer of information system security.

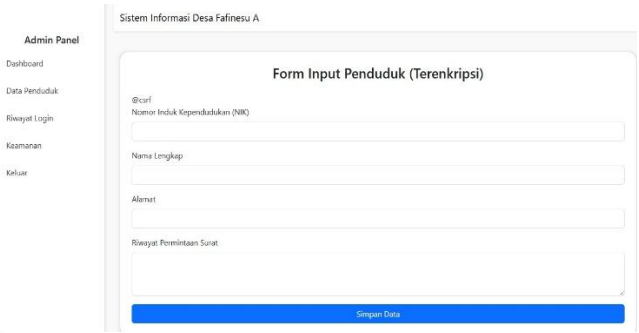

Figure 4. Resident Data Input Form (Encrypted)

This form is used to enter resident data into the system, which includes NIK, full name, address, and mail request history. The entered data will be encrypted before being saved to the database in order to maintain the confidentiality of the information and improve the security of the system.

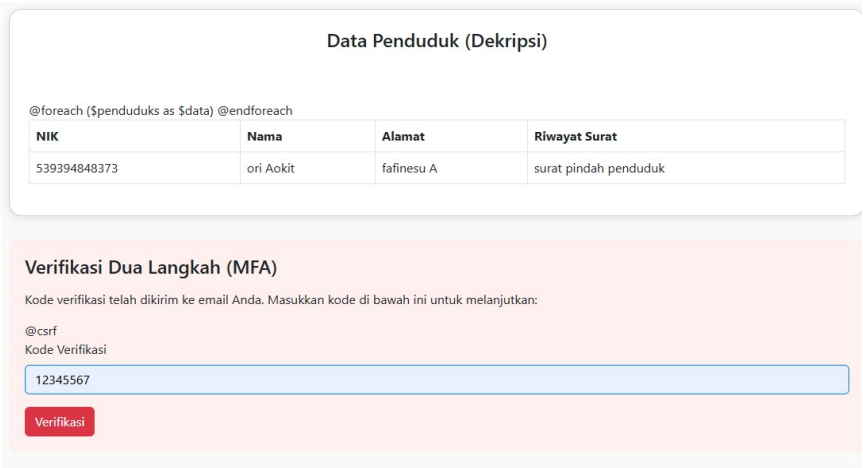

Figure 5. Resident data that has been successfully inputted

This figure shows the system interface that displays the decrypted resident data as well as the two-step verification (Multi-Factor Authentication/MFA) feature. Resident data such as NIK, name, address, and mail history are displayed using the @foreach loop. Before accessing the data, users are required to enter a verification code sent to email as an additional form of security, with CSRF protection to prevent security attacks.

4. Conclusion

This research has successfully implemented encryption using the Advanced Encryption Standard (AES) algorithm on a web-based information system in Fafinesu A Village, with the main objective of improving data security. The implementation results show that the application of AES encryption can effectively protect sensitive data stored in the village information system, such as population data and village administration documents. By using a 256 bit encryption key, data stored in the database cannot be read directly by unauthorized parties, even if the database is successfully accessed by outsiders. This successful implementation also increased user confidence in the system without requiring major changes to the interface or work processes. The participatory approach that involved village operators in the evaluation of the system contributed to the successful adoption of this technology in the field. For future research, it is recommended to develop the system with additional security features such as multi-factor authentication (MFA), biometric integration, and performance testing in large-scale scenarios. This is important to ensure that the system can operate reliably and securely under more complex and data-intensive usage conditions. This research shows that advanced encryption technologies such as AES can be well adapted in the context of village governance, providing strong data protection and supporting the village digitization agenda in a sustainable manner.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2017.
[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer-Verlag, 2002.
[3] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*, 16th ed., Pearson, 2020.
[4] R. Munir, *Kriptografi: Teori dan Praktik Modern*, Bandung: Informatika, 2019.
[5] Kementerian Komunikasi dan Informatika Republik Indonesia, "Pedoman Transformasi Digital Desa," 2021. [Online]. Available: https://kominfo.go.id/
[6] National Institute of Standards and Technology (NIST), "FIPS PUB 197: Advanced Encryption Standard (AES)," 2001.
[7] H. Kurniawan, "Pengembangan Sistem Informasi Desa Berbasis Web untuk Mendukung Transparansi Pemerintahan," *Jurnal Teknologi Informasi*, vol. 11, no. 2, pp. 100-110, 2020.
[8] A. Setiawan and R. Fadillah, "Implementasi Keamanan Data Menggunakan Algoritma AES pada Aplikasi Surat Menyurat," *Jurnal Informatika dan Komputer*, vol. 7, no. 1, pp. 15–22, 2021.
[9] E. D. Priyanto and S. Handayani, "Pengaruh Penerapan Data Enkripsi terhadap Kinerja Sistem Informasi Berbasis Web," *Jurnal Keamanan Informasi*, vol. 5, no. 1, pp. 22–30, 2022.

[10] A. Alasmary, A. Alhaidari, and M. Zohdy, "A Review on Data Encryption Techniques in Cloud Computing," *IEEE Access*, vol. 8, pp. 44312–44329, 2020.
[11] M. Kumar and P. K. Singh, "A Secure Data Transmission Scheme Using AES in IoT," *Procedia Computer Science*, vol. 167, pp. 1810–1819, 2020.
[12] A. Ahmad et al., "Performance Analysis of AES Variants in Securing Web Applications," *Journal of Information Security and Applications*, vol. 63, p. 103028, 2022.
[13] J. Wu, Y. Zhang, and Q. Li, "An Efficient AES-based Secure Scheme for E-Government Data," *International Journal of Information Management*, vol. 64, p. 102452, 2022.
[14] L. Singh and R. Dutta, "Lightweight Encryption Techniques for IoT Devices: A Comparative Study," *Computer Networks*, vol. 182, p. 107495, 2020.
[15] M. F. Firdhous, "A Survey on the Use of Encryption Algorithms in Securing E-Government Systems," *ICTACT Journal on Communication Technology*, vol. 12, no. 1, pp. 2416–2422, Mar. 2021.