Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume 3 Nomor 4, Juli 2025
e-ISSN : 3031-8912; p-ISSN : 3031-8904; Hal 350-360
DOI: https://doi.org/10.61132/merkurius.v3i4.1009
Available Online at: https://journal.arteii.or.id/index.php/Merkurius

Implementation of the Advanced Encryption Standard (AES) Cryptographic Algorithm in Library Information Systems for Member Data Security at the Cipanas Presidential Palace

***Putri Maharani[1], Jusmardi[2], Ahmaddul Hadi[3], Melri Deswina[4]**
[1,2]Universitas Negeri Padang, Indonesia

Alamat: Jl. Prof. Dr. Hamka, Air Tawar Bar., Kec. Padang Utara, Kota Padang, Sumatera Barat 25171
Korespondensi penulis: putrimhrrr9@gmail.com

Abstract. *This study aims to develop a data security system for the Pancadaya Waste Bank web-based application by implementing a hybrid cryptography algorithm combining AES and RSA. The main problem identified is the vulnerability of manually recorded and unsecured transaction data. The research applied a qualitative approach through interviews with system users and the Environmental Agency, as well as literature reviews on hybrid cryptography algorithms. The system was developed using the Rapid Application Development (RAD) method and implemented using PHP, MySQL, and the OpenSSL library. The results show that the system successfully encrypts transaction data using AES and secures the AES key with RSA, thereby enhancing data security. Testing with GTmetrix indicates excellent application performance. Furthermore, the system can display and decrypt real-time transaction data in receipt form for both deposit and withdrawal processes. This application provides an innovative solution to data management and transaction security issues in digital-based waste bank systems.*

Keywords: *AES, Hybrid Cryptography, RSA, Waste Bank, Web Application*

Abstrak. Penelitian ini bertujuan untuk mengembangkan sistem keamanan data transaksi pada aplikasi Bank Sampah Pancadaya berbasis web melalui implementasi algoritma kriptografi hybrid yang menggabungkan AES dan RSA. Permasalahan utama yang ditemukan adalah lemahnya sistem pencatatan dan keamanan data transaksi nasabah yang masih bersifat manual. Metode penelitian menggunakan pendekatan kualitatif dengan teknik wawancara kepada pengelola dan Dinas Lingkungan Hidup, serta studi literatur terkait algoritma kriptografi hybrid. Pengembangan sistem dilakukan dengan metode Rapid Application Development (RAD) dan diimplementasikan menggunakan PHP, MySQL, dan pustaka OpenSSL. Hasil implementasi menunjukkan bahwa sistem mampu mengenkripsi data transaksi dengan AES dan mengamankan kunci AES menggunakan RSA, sehingga meningkatkan lapisan keamanan data. Pengujian menggunakan GTmetrix menunjukkan performa aplikasi yang sangat baik. Sistem ini juga mampu menampilkan dan mendekripsi data transaksi secara real-time dalam bentuk nota, baik untuk transaksi setor maupun tarik saldo. Dengan demikian, aplikasi ini memberikan solusi inovatif terhadap persoalan pengelolaan data dan keamanan transaksi dalam sistem bank sampah berbasis digital.

Kata kunci: AES, Aplikasi Web, Bank Sampah, Kriptografi Hybrid, RSA

1. INTRODUCTION

Libraries are essential sources of information that support education, research, and decision-making activities. In government institutions such as the Cipanas Presidential Palace, the library serves as a valuable reference center, especially for historical collections that aid leaders in understanding the socio-political and cultural context influencing policy decisions.Previously, the library system relied on barcode-based records managed manually via Microsoft Excel. This approach presents several limitations, including the risk of data loss or manipulation, inadequate information security, and inefficiencies in searching and managing collections. The use of Excel as a database does not provide robust security features, making

Received: Mei 31, 2025 Revised: Juni 17, 2025 Accepted: Juli 28, 2025
Published: Juli 30, 2025

sensitive data vulnerable to unauthorized access or loss due to technical or human error.A fundamental issue is the lack of an official web-based or digital application for the library which restricts access to physical locations within the office. This limitation also affects reading interest among staff, as access to the library collection is only available on-site. In the digital era, increasing reading interest is challenging without a system that facilitates flexible and secure information access

Fig 1. Cipanas Palace Library System (2018-2024)

In the context of government institutions, digital system management must comply with strict regulations to ensure data security and system integrity. Therefore, the development of a library system at the Cipanas Presidential Palace must adopt an innovative approach to ensure that information resources are optimally utilized for strategic decision-making.The development of information technology has penetrated various sectors, including libraries. In environments with limited access, such as the Cipanas Presidential Palace, an information system-based library is a solution that facilitates staff access to literature and information sources. However, data security remains a critical aspect, especially for systems storing sensitive information such as NIK and phone numbers. Data breaches, hacking, or unauthorized access can lead to serious consequences, including privacy violations and identity misuse.

As a national strategic institution, the Presidential Palace has a significant responsibility to maintain the confidentiality and security of all data, including library member data. The library information system must be designed with a high level of security to ensure that sensitive data is not easily accessible to unauthorized parties. Encryption algorithms, particularly AES, are widely recognized as efficient and secure solutions for protecting sensitive data.

2. RESEARCH METHODOLOGY

This research adopts a descriptive and qualitative approach using the **Waterfall model** as the software development methodology. The Waterfall model consists of sequential phases that guide the development process in a structured manner. This method was chosen because

it is well-suited for systems with clearly defined requirements, such as the development of a secure library information system. The following are the stages carried out in this research:

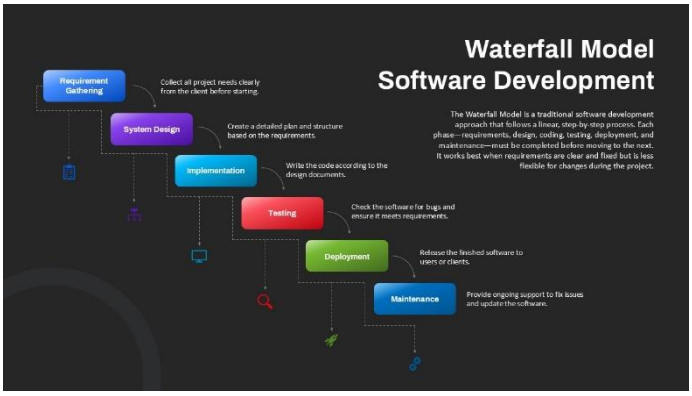


Fig 2. Waterfall method

1. Requirement Analysis

   In this stage, data collection was conducted through observation and interviews with staff at the Cipanas Presidential Palace to understand the problems with the current manual library system. The focus was placed on identifying data vulnerabilities, especially in managing sensitive member information such as National Identification Numbers (NIK) and phone numbers.

2. System Design

   The design phase includes creating diagrams using Unified Modeling Language (UML), such as Use Case Diagrams, Class Diagrams, Activity Diagrams, and Entity-Relationship Diagrams (ERD). These diagrams illustrate system behavior, data structures, and user interaction with the system. The AES encryption algorithm was integrated at this stage for securing member data.

3. Implementation

   The system was developed using PHP programming language and the Laravel framework, with MySQL as the database management system. Laravel's built-in AES-128 encryption feature was used to encrypt sensitive data before storage. Features such as member registration, book management, borrowing, and returning were implemented.

4. Testing

   System testing was carried out to validate functionality and encryption effectiveness. Manual validation and inspection through Laravel Tinker were performed to ensure encrypted data could be accurately decrypted. This phase confirmed that data input, display, and update processes work properly and that encryption effectively protects member data.

5. Deployment and Maintenance

   The final system was deployed for use within the internal network of the Cipanas Presidential Palace. Feedback from initial users (admin) was collected to assess usability and security. Maintenance procedures were outlined to address future updates and encryption expansion.

This structured methodology ensures that the system is not only functional and easy to use but also provides robust data protection aligned with national information security standards. The implementation of AES within the library system provides a significant advancement in maintaining the confidentiality and integrity of member data.

1. Software Requirements Analysis

a. Visual Studio Code

   Visual Studio Code text is a text editor that is used to create application programs automatically to make it easier for programmers to type editor code..

b. XAMPP

   Xampp is a free software package consisting of Apache, MySQL (or MariaDB), PHP, and Perl, which is used to run a local web server on a computer. XAMPP provides an easy-to-use development environment for web developers to create and test web applications without having to upload them to an actual web server.

c. MySql

   MySQL is a software and database creation system that is open source to run on all forms. MySQL is one type of database server as a source and data processing for building web applications.

d. PhpMyAdmin

   PhpMyAdmin is a web server that is used to manage the database of web programs that have been created where the program must be in accordance with the database.

2. Hardware Requirements Analysis The hardware needed for the development of this blood donor application is as follows:

a. DESKTOP-EXPERTCOM

b. Intel(R) Core(TM) i5-3230M CPU @

   2.60GHz 2.60 GHz

c. RAM 4 GB

Developing the user interface, and integrating various system components to ensure that all planned functions can run properly.

After the application has been developed, the next step is to test the application to ensure that all features function as expected and meet user needs. This testing includes various types of testing, such as functional testing, integration testing, and user testing, which aims to get direct feedback regarding their experience when using the application.

3. RESULTS AND DISCUSSION

In this discussion section, the author explains what we will find on the library information system website, the menus and the steps for operating them.

SYSTEM DESIGN

The design of this web-based application using the Unified Modeling Language (UML) as a modeling language as follows:

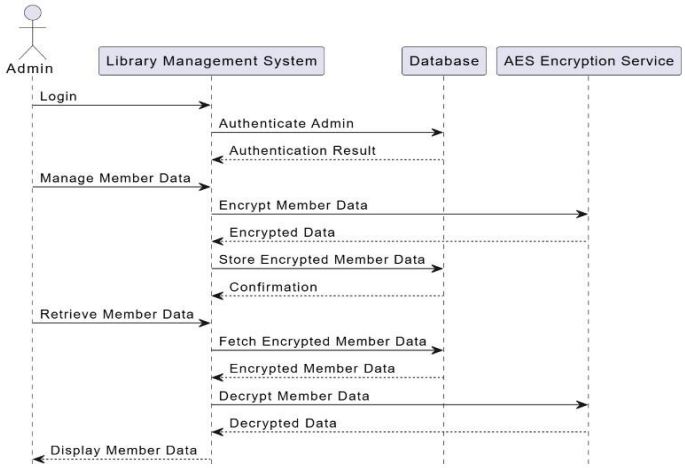


Fig 3. flowmap

This flowmap of the library information system demonstrates the proposed workflow for optimizing library management processes and strengthening the security and accessibility of member data through the implementation of the AES cryptographic algorithm at the Cipanas Presidential Palace.

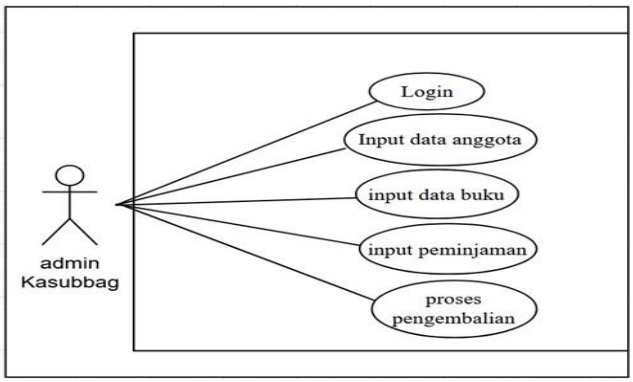


Fig 4. Use Case Diagram

The use case diagram above depicts the functions and activities accessible only to the admin, as the system is designed with pre-registered admin accounts and does not allow user self-registration.

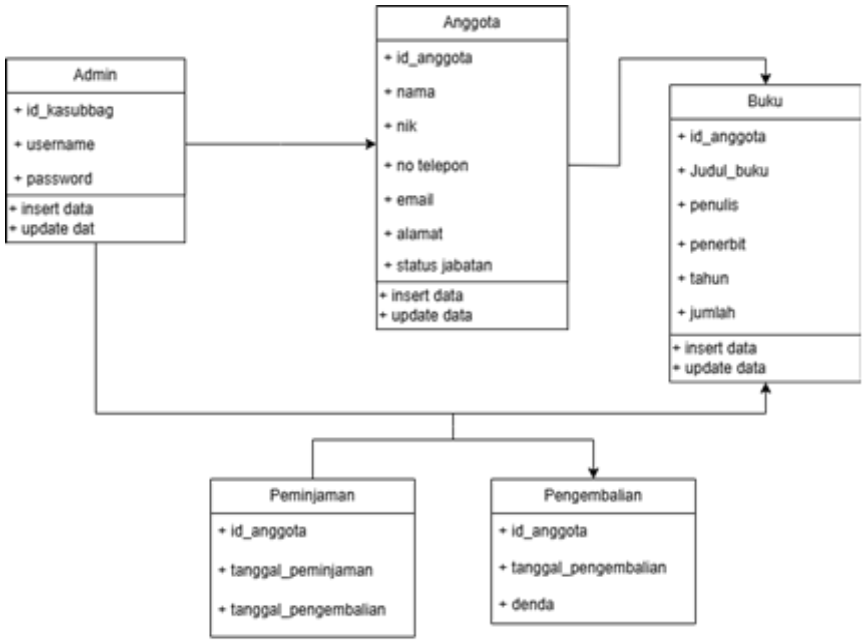


Fig 5. Class Diagram

This Class Diagram describes the system structure in terms of defining the classes that will be created to build a library information system website

Figure 6 shows a database structure consisting of several interconnected tables to support the functionality of the library information system. These tables represent the main entities involved in managing the library information system, as well as other related processes. The system implementation stage is the stage of changing the previously designed system into a system that can be run on various platforms or hardware.

Fig 6. ERD

A. Login Page

Fig 7. Login Page

In the design of the Login menu page display, there are three features including the login button, username input and password input in the application. This page serves to enter the system by entering the username and password that has been registered.

B. Admin Dashboard Page

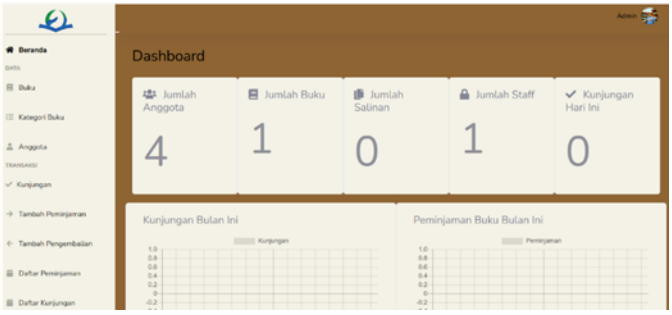


Fig 8. Dashboard Page

The admin dashboard is the main display that appears after logging into the application or website. The dashboard serves as a control center where users can easily view important information and access key features. The dashboard contains eight menus: Books, Book Categories, Members, Visits, Add Borrowing, Add Returning, Borrowing List, and Visiting List.

C. Book Page

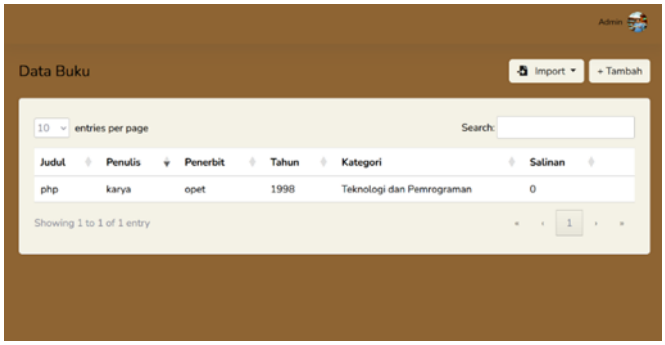


Fig 9. Book Page

The Book page in the library information system serves as the central interface for managing the collection of books available in the library. This page provides both administrators and authorized users with access to detailed information about each book, including the title, author, publisher, publication year, category, and availability status.

D. Member Page

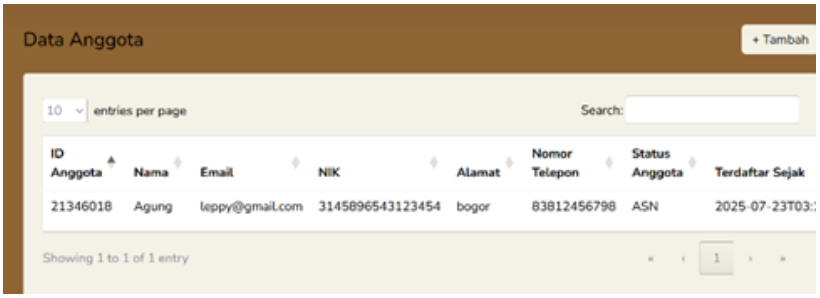


Fig 10. Member Page

The Member page functions as a core feature of the library information system that manages the personal data of registered library members. This page enables administrators to view, add, edit, and delete member records in an organized and secure manner. Each member's data includes information such as full name, username, email, class, phone number, address, and crucial identity fields such as Member ID and National Identity Number (NIK). To ensure data confidentiality and prevent unauthorized access, the system implements Advanced Encryption Standard (AES) to encrypt the Member ID and NIK before storing them in the database. Decryption is applied only when the data needs to be displayed to authorized users.

E. Visit Page

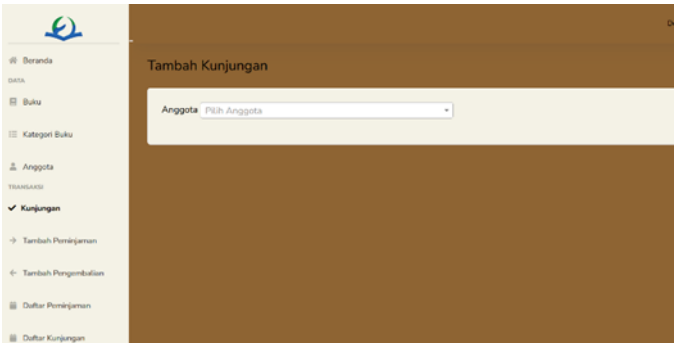
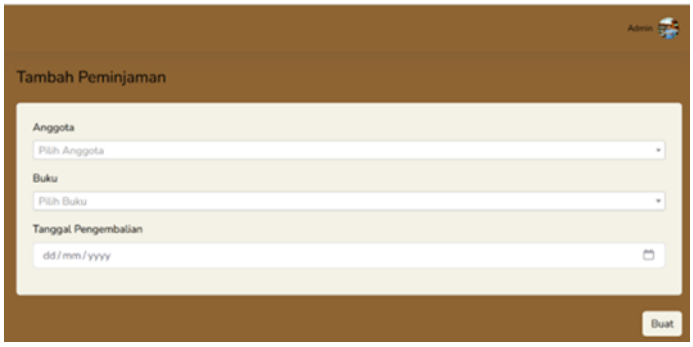


Fig 11. Visit Page

The Visit page is a supporting feature of the library information system that records and displays member visit activities within the library. This page is primarily used by administrators to monitor user engagement, track the frequency of visits, and maintain attendance logs for analysis and reporting purposes.

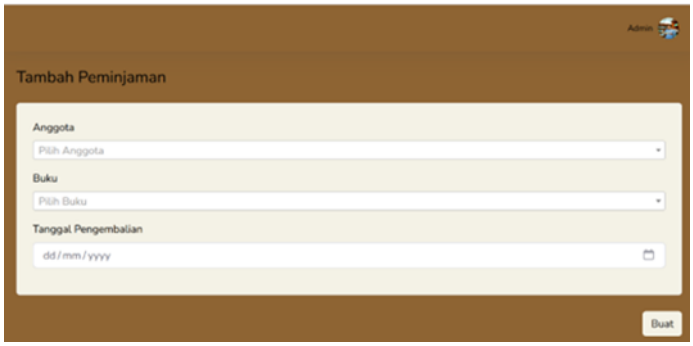
F. Book Borrowing Page



12. Book Borrowing Page

The Book Borrowing page is a vital feature of the library information system that facilitates the lending process between the library and its members. This page allows administrators to manage borrowing transactions in a structured and efficient manner. Each borrowing record contains important information such as the borrower's name, book title, borrow date, due date, and the status of the loan.

G. Book Return Page



13. Book Return Page

SYSTEM TESTING

System testing was conducted to evaluate both the functionality and security aspects of the developed library information system, particularly focusing on the implementation of the **Advanced Encryption Standard (AES)** for member data protection. The goal was to ensure that the system behaves according to its intended specifications and successfully protects sensitive data from unauthorized access.

Fig 14. Data Security Testing

Based on the results of testing conducted through manual functional validation and database inspection, it can be concluded that the system performs reliably, with all tested features functioning as expected. Data input, display, and update operations related to library members, book records, and transactions were executed successfully without errors. More importantly, the system showed significant improvements in data security with the implementation of the AES encryption algorithm. Sensitive information such as Member ID and National Identity Number (NIK) was stored in encrypted format using Laravel's built-in AES-128 encryption method, and decryption occurred only within the authorized system context. Manual verification through Laravel Tinker confirmed that encrypted values could be decrypted accurately, ensuring data integrity and confidentiality. Compared to conventional manual data handling, this application offers major advantages, particularly in protecting member privacy and minimizing data exposure risks. Additionally, the centralized and encrypted database design reduces the possibility of unauthorized access or data tampering. This demonstrates that the developed system not only enhances data management efficiency but also meets modern standards of information security, making it a robust digital solution for the library operations at Istana Kepresidenan Cipanas.

TABLE 1 COMPARISON OF MANUAL LIBRARY MANAGEMENT AND ENCRYPTED LIBRARY INFORMATION

No	Feature Tested	Test Scenario	Expected Result
1	Add New Member	Submit registration form with valid input	Data is saved and encrypted in the database
2	View Member List	Access member list from the dashboard	Data is decrypted and displayed in readable format
3	Edit Member Data	Modify member information through the system	Updated data is re-encrypted and stored successfully
4	Delete Member	Remove member from the system	Data is deleted from the database

From the table above, it can be concluded that the Blood Donor App is significantly superior to the manual method used by PMI Pesisir Selatan. The app increases time efficiency through process automation, facilitates online access to information, and supports real-time collaboration between officers and donors.

4. CONCLUSIONS

The conclusion of this research is that the implementation of the Advanced Encryption Standard (AES) algorithm within the library information system has successfully enhanced data security, particularly for protecting member-related information such as Member ID and

National Identification Number (NIK). The developed system facilitates administrative operations such as managing books, categories, members, borrowings, returns, and visit logs in a more structured and secure manner.

With the integration of AES encryption, the confidentiality and integrity of sensitive member data are better preserved, minimizing the risk of data breaches or unauthorized access. This innovation not only strengthens information security but also improves the trustworthiness of the system used at Istana Kepresidenan Cipanas.

In terms of functionality, the system offers a user-friendly interface for administrators to perform daily operations, while maintaining high standards of data protection. The addition of features like encrypted member registration and secure data display also supports compliance with modern information privacy practices.

For future development, it is recommended to expand the encryption coverage to other modules, such as borrowing history or visit logs, and to implement role-based access control (RBAC) for more granular user management. Furthermore, integrating automated data backup and exploring the use of blockchain or biometric authentication could provide additional layers of security and reliability in future iterations of the system.

Through continuous improvement, this AES-based library information system can become a robust digital asset in supporting administrative efficiency and safeguarding personal data in institutional environments

REFERENCES

Kurniawan, D. (2018). *Implementasi algoritma AES untuk keamanan data* (Skripsi Sarjana, Universitas XYZ).

Laravel. (2023). *Laravel documentation*. https://laravel.com/docs

National Institute of Standards and Technology (NIST). (2001). *Announcing the advanced encryption standard (AES)* (FIPS PUB 197). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

phpMyAdmin. (2023). *phpMyAdmin documentation*. https://www.phpmyadmin.net/docs/

Rezy, F., & Ikasari, D. (2023). Penerapan sistem informasi berbasis web untuk efisiensi pengelolaan inventori. *Jurnal BIIKMA*, *5*(2), 112–119.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Jakarta: PT Indeks.

SweetAlert2. (2023). *Beautiful, responsive, customizable pop-up library*. https://sweetalert2.github.io/

Wibowo, H. (2016). *Perancangan sistem informasi perpustakaan berbasis web* (Skripsi Sarjana, Universitas ABC).