Journal of Applied Informatics and Computing (JAIC)
Vol.9, No.3, June 2025, pp. 876~882
e-ISSN: 2548-6861

Optimizing Customer Data Security in Water Meter Data Management Based on RESTful API and Data Encryption Using AES-256 Algorithm

Syahrul Adrianto [1]*, Bambang Agus Herlambang [2]*, Ramadhan Renaldy [3]*
* Informatics, Universitas Persatuan Guru Republik Indonesia Semarang
syahruladrianto444@gmail.com [1], bambangherlambang@upgris.ac.id [2], ramadhanrenaldy@upgris.ac.id [3]

Article Info

Article history:

Received 2025-03-27
Revised 2025-04-24
Accepted 2025-05-04

Keyword:

RESTful API,
Laravel,
Javascript,
AES-256,
Water Meter.

ABSTRACT

Good, accurate and secure data management is certainly one of the main needs for companies that provide public services. This research aims to develop a web application-based information system to manage customer water meter data at a regional water company in Semarang. This system was built using the RESTful API architecture using the PHP programming language framework, namely Laravel and the development of web page displays using the Javascripts framework. The data used is the original database managed by the company every month which is managed using a database management system by meter reader officers. To increase the security of customer data, a cryptographic algorithm is used, namely the Advanced Encryption Standard (AES) algorithm with a 256-bit key length to secure data that is considered sensitive and contains high privacy. This system is intended for meter readers to update customer water meter data per month in an efficient and structured manner. This research uses a Research and Development (R&D) based software development method with system testing using black-box testing method to ensure application functionality and data exposure testing method to ensure data security in the database. The test results show that the system successfully manages customer water meter data in realtime per data sent and secures customer data.

I. PENDAHULUAN

The rapid development of technology certainly increases the company's need to provide an efficient and secure system for managing customer data. The use of computers as well as their development systems is a major requirement in an effort to improve company performance and services[1]. PDAM Tirta Moedal Semarang City is a company that provides clean water services so it requires a system that is able to increase efficiency in processing customer water meter data per month. In this case the company must follow the development of technology to improve performance and service to customers [2].

In previous research, it was said that the REST method can integrate between systems and between databases in inventory data management. REST web services also have better performance and are lightweight and save bandwidth compared to other methods[3]. The use of REST API can increase the efficiency of data exchange and transactions that focus on the backend system on the system[4]. Laravel was chosen because it is a framework that is easy to understand and has a powerful performance among other frameworks that provide various components such as authentication, routing and many others[5]. In the research conducted, an information system was developed with a RESTful API architecture using the PHP (Hypertext Preprocessor) framework, namely Laravel with the development of a website display with several javascript frameworks such as vue.js and next.js. Some studies say that and show that the implementation of Laravel as a REST Server and Vue.js as a REST Client has good interoperability[6].

Confidentiality of data or information is one of the complete services provided by the company which aims to prevent data from being read and opened by unauthorized parties[7]. Customer data security is one form of service provided by the company for every customer who has a business attachment to the company, some important data that is private must be secured with the right strategy, one of which

is by applying cryptographic algorithms that convert customer data into a ciphertext. In several previous studies, the AES algorithm was used to ensure data security in the sales and ordering process of the Community business by changing the data stored in the database into random words that are difficult to understand[8]. Other research also mentions that the AES-256 algorithm is used to help a system design in protecting important data in companies such as field reports and company personal data[9]. With the encryption and decryption process in the aes algorithm, data security is more guaranteed because when the data wants to be accessed, a decryption process must be carried out which of course uses a password that is not understood by unauthorized people[10]. Other research also explains that cryptography using the AES 256 algorithm can secure data in the form of messages in a data communication[11]. This research applies a cryptographic algorithm that can increase security and authenticated privacy[12]. The algorithm is AES-256 (Advanced Encryption Standard) algorithm with 256-bit key length which is used to increase the security of customer data. AES-256 is used because it has a high level of security with an encryption process that converts data into ciphertext or random data that is difficult to read[13]. Therefore, this research not only develops a web-based system, but also integrates a RESTful API architecture designed with authentication and advanced encryption and decryption processes that are not only used in the user authentication process but can be used to secure other sensitive data to ensure the security of data communication.

This research aims to develop a web-based customer water meter data management information system with RESTful API implementation that can improve bandwidth efficiency and save time in the data exchange process[14]. In addition, this research also ensures that the system has optimal performance with good data security. The benefits of making this information system are to increase the security and privacy of customer data in the data management system, besides that the community also gets more knowledge about good water quality and gives the impression of a comfortable and reliable service. This research is also useful to facilitate the management and monitoring of digital water meter data and improve operational efficiency. In addition to being designed to support the activities of meter readers in recording and updating customer data in real-time, this system also has the potential for further development so that it can be accessed by the company's central admin in verifying, quality control, and monitoring the activities of officers in each branch. Not only that, the system also has the potential to be developed into a customer service platform, especially to accommodate complaints or grievances related to water distribution services directly through the website, thus increasing transparency and quality of public services.

II. METHODS

This research uses the Research & Development (R&D) method which has the aim of developing or producing a new information system[15]. Creating a system that is easy to use and secure in managing customer water meter data. The main stages in this method include.

A. Needs Analysis

At this stage of the needs analysis, several actions are taken to identify what needs will be solved, including:

- Identify system requirements based on existing problems in managing PDAM customer data.
- Conduct a literature study related to data security and the application of the AES-256 algorithm in information systems. Previous research shows that the AES-256 algorithm has proven effective in securing sensitive data[16].
- Analyze backend and frontend requirements to ensure optimal RESTful API communication.

B. System Design

1. Using Unified Modeling Language (UML) to describe the flow of the system, including Use Case Diagram, Activity Diagram, and Entity Relationship Diagram (ERD). Unified Modeling Language (UML) is one of the most important modeling methods in the design of information systems[17].

Use Case Diagram is a behavioral model of an information system, which is used to describe the interaction between the user and the system, ensuring that any required functionality is well- defined [17].

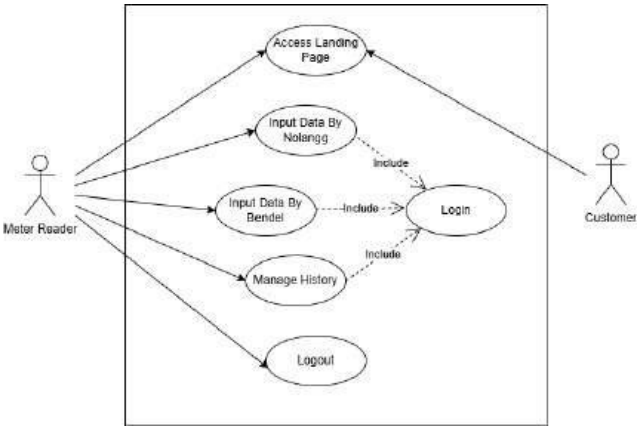

Figure 1. Use Case Diagram

Activity diagram is a diagram whose role is to describe the workflow in the system, including how data is processed from one stage to another, making it easier to understand the business processes that exist in the software [17].

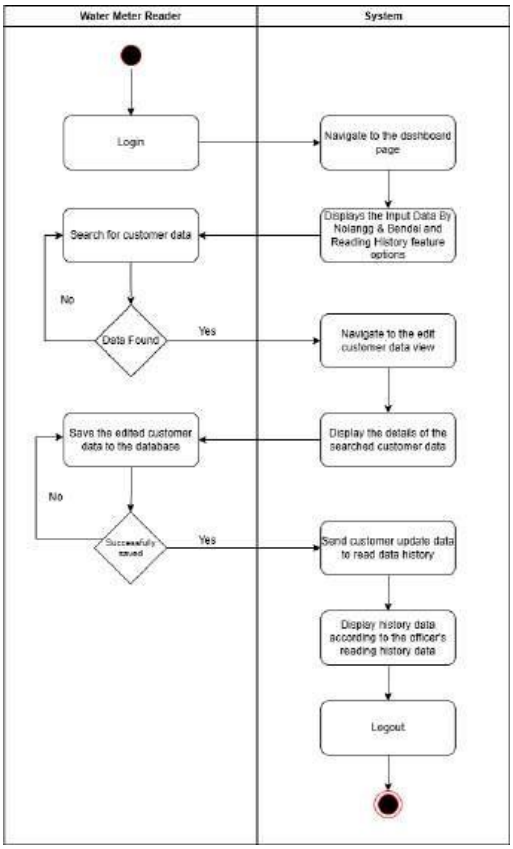

Figure 2. Activity Diagram

Designing RESTful API architecture with Laravel framework. The study shows that Laravel is effective in developing RESTful API for document monitoring system [18]. Design an AES-256 encryption implementation to ensure customer data security. The implementation of AES-256 has been proven to improve data security in various applications [13]. Developed a frontend view using Vue.js to create an interactive and easy-to-use interface. The use of Next.Js as a landing page and Vue.js together with Laravel in the development of RESTful APIs has provided effective results in several studies [6].

C. System Implementation

1. Restful API Development

Representational State Transfer (REST) architecture is an HTTP protocol-based communication approach that allows data exchange between client and server flexibly and efficiently. In this research, RESTful API is used as the main framework in building interactions between the user interface (front-end) developed using a JavaScript framework with backend services developed through Laravel, a PHP framework that supports route management and authentication in a modular manner.

The design of the RESTful API in this system follows the main principles of REST, such as the use of standard HTTP methods (GET, POST, PUT, DELETE) to handle data requests. For example, the GET method is used to retrieve customer data, POST to store the latest meter reading data, PUT to update encrypted customer data, and DELETE to delete data that is no longer needed. Each endpoint has a URI that is hierarchically designed and descriptive, facilitating system integration and documentation.

In addition, the API system also implements JSON Web Token (JWT)- based token authentication, where each successfully logged-in user will get a unique access token that is used for each request to the API. This scheme not only strengthens user authentication, but also enables role- based access control on each available endpoint, where restrictions are made to officers with their respective officer codes and branches, this restriction aims to divide and organize so that the data managed by officers is data that corresponds to the officer's branch only. To ensure data security when interacting with the API, this research applies two layers of security.

First, all communication between client and server uses the HTTPS protocol to prevent data interception by third parties. Second, data categorized as sensitive, such as customer identity and address information, is encrypted using the AES-256 algorithm before being transmitted or stored in the database. This ensures that even if the data is successfully intercepted, the information remains unreadable without a decryption key. Restful API (Representational State Transfer Application Programming Interface) is an architectural standard that enables communication between clients and servers via the HTTP protocol.

In this system, RESTful API is used to manage customer data in an efficient and structured manner. In this system, each resource is accessed through the API endpoints used such as :

a) GET → Retrieve data
b) POST → Adding data
c) PUT/PATCH → Update data
d) DELETE → Delete customer data

Here is the workflow of the RESTful API:

a) *Requests from clients*, in this study, are used in the frontend implementation using a javascript framework, namely vue js, which sends HTTP requests to the server to access and manage customer data. The axios library is used to connect the calling process.

b) *Server Processing*, the backend server used in this research uses the Laravel framework which receives requests and processes interactions with the database according to business needs in customer data management, several models are created to connect relationships and management processes with the database provided, then management processes such as data calls and customer data update processes are configured in the controller.

c) *Response Delivery*, the server sends the response back to the client in json format.

2. AES-256 Algorithm

a) The AES-256 or Advanced Encryption Standard algorithm is a symmetric encryption algorithm that is widely adopted to secure digital data. AES-256 uses a 256 bit long encryption key, which works quickly and efficiently. One

study proved that the AES-256 algorithm has a faster performance than other cryptographic algorithms such as the RSA (Rivest, Shamir, and Adleman) algorithm[19].

The implementation of the AES-256 encryption algorithm in this study was carried out in storing customer address data. Implementation in other studies is done to secure documents using the AES-256 algorithm[16]. Data encryption in this system is applied at the application level, which is before sensitive data is sent through the API and stored in the database. Any private customer data, such as addresses, will be encrypted using the AES-256 algorithm on the client or backend side before being sent to the server, and then stored in the database in the form of cipher text.

On the reverse side, when the data is read or consumed by the client, the decryption process is performed first so that the data can be displayed in a form that can be understood by the user. With this approach, the system not only protects data while "in-transit" (when moving between networks via HTTPS), but also while "at-rest" (when stored in the database), so that data security is maintained even in the event of unauthorized access to the storage system.

b) The implementation of AES-256 in managing customer water meter data involves several main steps including:

- Key Generation, which creates a 256-bit encryption key that will be used for the encryption and decryption process on customer data as shown below. The AES-256 encryption key is not stored directly in the source code, but is managed through Laravel .env environment configuration file. This file is private and not included in the public repository, so it cannot be accessed by outsiders. This method is known as environment-based key management, which is standard practice in securing modern web applications.
- Data Encryption, which is when the original data (plaintext) is split into 128-bit blocks. Each block is then processed through 14 rounds of transformation involving byte substitution, row shifting, column blending, and round key addition to produce the ciphertext.
- Data Decryption, the decryption process uses the same key to return the ciphertext to its original form through the inverse steps of the encryption process.

c) AES-256 Algorithm Encryption Process

The encryption process in the AES-256 algorithm consists of four main stages of byte transformation, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey. The data to be encrypted, referred to as plaintext, is divided into 128-bit blocks. Each plaintext block is then arranged into a 4×4 matrix known as the State Array, where each element of the matrix contains one byte of data. In the AES-256 algorithm, the encryption key used is 256 bits in length. This key is processed through a key expansion stage to generate the round keys required at each stage of encryption. The encryption process is carried out in 14 rounds, where in each round a sequence of transformations is performed in order to enhance data security. A complete illustration of these encryption stages can be seen in Figure 3.

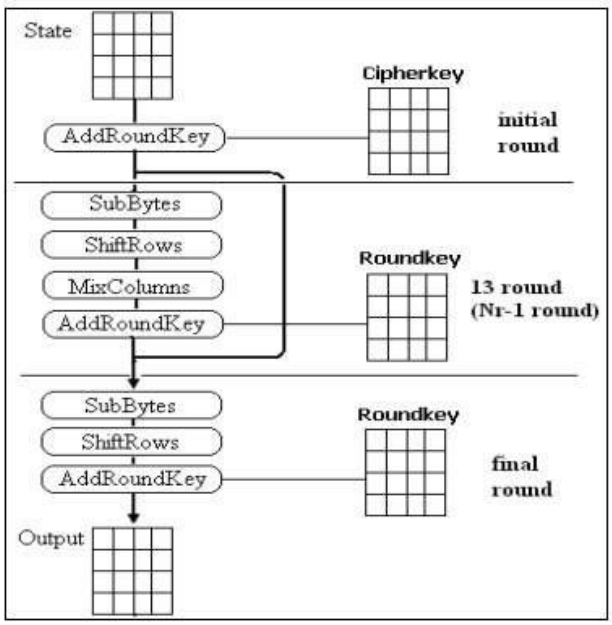

Figure 3. Encryption Process of AES-256 Algorithm[20]

d) AES-256 Algorithm Decryption Process

The decryption process is the opposite of the encryption process. In this process the ciphertext is returned to plaintext using the same round key but using the reverse order. The process is depicted in Figure 4.

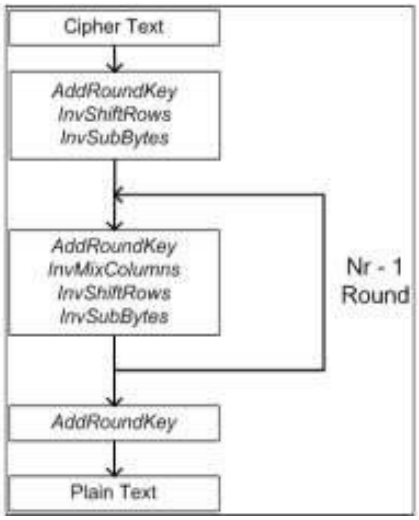

Figure 4. Decryption Process of AES-256 Algorithm[20]

Ciphertext is the result of the previous encryption process, at the beginning of the decryption process, the ciphertext is directly processed at the AddRoundKey stage, where the last key of the key schedule is added to the cipher text with an XOR operation.

3. Website Interface Design Development

Website interface design development or frontend is made using several frameworks in javascript, namely next.js and vue.js. Next.js is only used to create an attractive and responsive landing page display while the water meter data management business process uses Vue.js which is specifically accessed for branch admins only. The data retrieval and authentication process with the backend api uses the axios library.

D. Testing System

Testing in this study uses the BlackBox testing method to ensure system functionality runs as desired. Testing can be seen in tabular form by displaying tests of each feature unit on the website and retrieving fire from the backend, while testing the AES-256 algorithm encryption process on customer data is carried out by the data exposure method which ensures that the data is secured and sent in the database in the form of ciphertext correctly

III. RESULT AND DISCUSSION

A. Data Calling Process Using Restful-API

The data call process in managing customer meter data starts from the officer data authentication process where each officer already has an NPP or officer number and their respective passwords, then when the officer successfully enters the officer's code and password correctly the officer will be directed to the next page and can access other data management features. The following shows the results of response time testing on the RESTful API conducted using Postman.

TABLE I
RESTFUL API RESPONSE TIME TESTING

No.	Endpoint API	Method HTTP	Response Time(s)	Status	Description
1	/api/login	POST	0.501 s	200	Authentication successful
2	/api/customer/search/{nolangg}	GET	1.3 s	200	The data retrieval process is successful
3	/api/edit/{nolangg}	PUT	2 s	200	Data successfully updated
4	/api/history	GET	1.31	200	History data successfully loaded

Based on Table I, the results of response time testing on several main endpoints used in the application, it can be concluded that the system has the ability to respond to requests from clients in an average time of under 2 seconds. The response time value obtained ranges from 510 milliseconds to 2 seconds, which is still in the real-time response time category based on the web application responsiveness standard <1 second for instant interaction. This indicates that the system can support officers operations in the field without significant delays.

The use of AES-256 encryption does not have a significant impact on increasing response time, as the encryption process is executed synchronously and efficiently before the data is sent to the database.

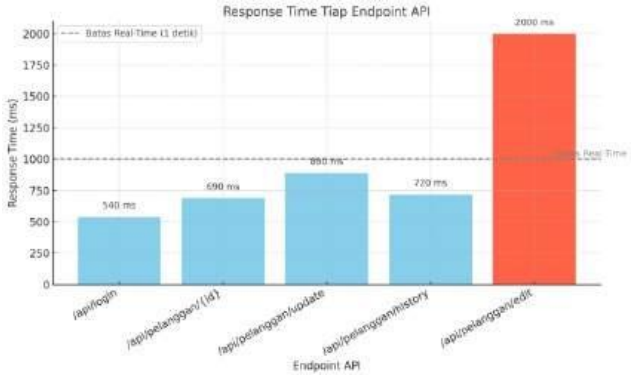

Figure 5. Enpoint API Response Time Bar Chart

Figure 5 is a bar chart depicting the response time of each API endpoint. This graph shows that four of the five endpoints are below the real-time standard limit of 1,000 milliseconds (1 second). One endpoint, /api/customer/edit, shows a response time of 2,000 milliseconds (2 seconds), which is still tolerable in an operational context, although it has passed the instant responsiveness category.

B. AES-256 Algorithm Testing

a) Data Exposure (Sensitive Data Exposure Test)

Testing the AES Algorithm to ensure the security of customer data uses the Data Exposure method or Sensitive Data Exposure Test. Data Exposure aims to ensure that sensitive data such as customer addresses and other private information is not sent or stored in plaintext, either in client-server communication or in database storage. Ensure that the encryption on the secured database is running properly, the check is carried out with the endpoint of editing the api data in postman with json output and ensuring that the data entering the database is encrypted data.

Figure 6. Checking Encryption

Figure 6 displays the json output of the data that has been saved and successfully encrypted the customer address data which in this research is the target of the secured data.

Figure 7. Checking Encryption in the Database

Another check is made to ensure that the data entered into the database as shown in figure 7 is an address data that has been encrypted in the form of ciphertext. With this, sensitive customer data can be more secure.

TABLE II
TESTING ENCRYPTION AND DECRYPTION TIME ON CUSTOMER DATA

No	Input file size (plaintext)	Output file size (ciphertext)	Encryption Time	Decryption Time
1	13 bytes	49 bytes	0.451332 seconds	0.000422 seconds

Table II shows the execution time of encryption and decryption where the data transformation process from plaintext to ciphertext takes 0.451332 seconds, and the decryption process by changing the ciphertext data to plaintext again takes 0.000422 seconds, the results show that the time given is quite fast and efficient in processing the encryption and decryption data performed.

C. System Testing

System testing is carried out using the blackbox testing method which can be seen in the following table.

TABLE II
TESTING INPUT DATA BASED ON CUSTOMER NUMBER

No.	Test Description	Expected Output	Results
1.	Officers perform the login process using their respective codes and passwords	The web application displays loading and the officer is directed to the dashboard page, the login API call for user authentication is successfully called and seen on inspection	Successful
2.	The clerk tries to search for data, and views the details of the customer data to be updated.	The web application displays the details of the data searched and will be updated by the officer through the API that has been set up in the backend.	Successful
3.	Officer saves customer update data	The web application saves customer data to the database with AES-256 algorithm encryption rules by converting officer address data into cipher text to the database.	Successful
4.	Officer accesses read history data	The web application displays data history data that has been managed by officers	Successful

Table II above is the overall test table where the system runs from the first officer logs into the system and manages customer data, where all activities carried out by officers are regulated and limited by the RESTful API architecture which is equipped with data security on customer addresses by the AES-256 algorithm.

V. KESIMPULAN

This research successfully developed a RESTful API-based water meter data management information system with Laravel and Vue.js frameworks that provides increased efficiency and security in managing PDAM Tirta Moedal Semarang City customer data. The application of RESTful API allows flexible data integration between the backend and frontend, so that the process of recording, managing, and monitoring customer data can be done in real-time. In addition, the use of AES-256 algorithm in encrypting customer data is proven to increase the protection of sensitive information, and reduce the risk of data leakage. The Research and Development (R&D) method applied in this research also enables more systematic system development based on scientific evaluation, so that each stage from design to testing can be carried out optimally.

Overall, the developed system is not only a digital solution in managing PDAM customer data, but can also be a model in developing similar systems in other sectors that require high data security. The results of testing using the Black Box Testing method show that the system functions properly according to specifications. The system that has been developed in this research can be expanded in terms of users and service functions. Not only limited to meter readers, further development allows the system to be accessed by the central admin in charge of managing customer data, verifying reports per branch, and monitoring the performance of field officers. In addition, the system can be upgraded into a customer service platform through an online complaint feature that allows the public to submit complaints related to water distribution or technical problems directly, creating a responsive and participatory water service information system.

DAFTAR PUSTAKA

[1] Y. Eka and E. Arviana, "Sistem Informasi Pendapatan Jasa pada Koperasi PDAM Tirta Patriot Bekasi," *J. Tek. Komput. AMIK BSI*, vol. 4, no. 1, pp. 1–8, 2018, [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/2377

[2] E. D. B. Santoso, N. R. Hidayati, and F. Nugrahanti, "Rancang Bangun Sistem Pendukung Keputusan Penilaian Kinerja Karyawan dengan menggunakan Metode AHP Berbasis Desktop pada PDAM Kabupaten MAdiun," Literasi Digit. pada Era Revolusi Ind. 4.0, pp. 66–71, 2018.

[3] M. Farizd, Aditya Kurnia Pratama, and Abdul Rezha Efrat Najaf, "Penerapan Rest Api Sistem Informasi Cinema Catalog Movie Berbasis Desktop Dan Web Service," Pros. Semin. Nas. Teknol. dan Sist. Inf., vol. 3, no. 1, pp. 116–125, 2023, doi: 10.33005/sitasi.v3i1.441.

[4] I. Nurjaman, F. S. Utomo, and N. Hermanto, "Penerapan REST API Laravel sebagai Fondasi Back-end Aplikasi G-MOOC 4D," J. Informatics Interact. Technol., vol. 1, no. 1, pp. 9–18, 2024.

[5] K. Gowell and Suprihadi, "Perancangan Web Service REST API Menggunakan PHP dan Framework Laravel di Tenta Tour Salatiga," J. JTIK (Jurnal Teknol. Inf. dan Komunikasi), vol. 8, no. 1, pp. 49–57, 2024, doi: 10.35870/jtik.v8i1.1269.

[6] H. Fery Herdiyatmoko and Y. Dicka Pratama, "Rest Api Pada Toko Kelontong Untuk Transaksi Penjualan Menggunakan Framework Laravel," Idealis Indones. J. Inf. Syst., vol. 7, no. 1, pp. 118–127, 2024, [Online]. Available: http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/indexHendrikFery Herdiyatmoko%7Chttp://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index%7C

[7] M. Hasanudin, Lasmin, and M. N. Dasaprawira, "Pengujian Aplikasi Tabungan Santri Berbasis Web Dengan Menggunakan Algoritma Kriptografi Advance Encryption Standard (Aes) 256.," JOINICS (Journal Informatics …, vol. 1, no. 1, pp. 11–18, 2022, [Online]. Available: https://jurnal.unugha.ac.id/index.php/jnc/article/view/383

[8] S. E. Damayanti and F. Permana, "Sistem Informasi Pada Usaha Wangi Project Di Limbangan Tengah Dengan Menggunakan Algoritma Linear Search Dan Aes 256," Naratif J. Nas. Riset, Apl. dan Tek. Inform., vol. 6, no. 1, pp. 79–88, 2024, doi: 10.53580/naratif.v6i1.288.

[9] T. D. A. P. Wardhani and Y. Asriningtias, "Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android Menggunakan Algoritma AES-256," *JUSTIN (Jurnal Sist. dan Teknol. Informasi)*, vol. 12, no. 1, pp. 143–154, 2024, doi: 10.26418/justin.v12i1.71449.

[10] T. Bin Tahir, M. A. Hadi Sirad, and M. Rais, "Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel," Patria Artha Technol. J., vol. 4, no. 1, pp. 41–46, 2020, doi: 10.33857/patj.v4i1.326.

[11] K. I. Santoso and R. Habibi, "Kriptografi Pada Aplikasi Komunikasi Data dengan Algoritma AES 256," Pros. Semin. Nas. ILMU Komput. 2014 "Trusted Digit. Identity Intell. Syst., pp. 447–458, 2014, [Online]. Available: https://ilkom.unnes.ac.id/snik/2014/prosiding/

[12] R.M. Hilmy Hernandi and Joko Christian Chandra, "Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya," KRESNA J. Ris. dan Pengabdi. Masy., vol. 4, no. 1, pp. 12–22, 2024, doi: 10.36080/kresna.v4i1.131.

[13] T. D. A. P. Wardhani and Y. Asriningtias, "Implementasi Algoritma AES-256 Dalam Perancangan Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android," INTECOMS J. Inf. Technol. Comput. Sci., vol. 6, no. 2, pp. 1289–1293, 2024, doi: 10.31539/intecoms.v6i2.8027.

[14] B. A. Wicaksono and I. V. Paputungan, "Pengembangan REST API untuk Sistem Pelaporan dan Pengaduan dengan Laravel," J. Portal, vol. 3, no. 2, 2022.

[15] Okpatrioka Okpatrioka, "Research And Development (R&D) Penelitian Yang Inovatif Dalam Pendidikan," Dharma Acariya Nusant. J. Pendidikan, Bhs. dan Budaya, vol. 1, no. 1, pp. 86–100, 2023, doi: 10.47861/jdan.v1i1.154.

[16] A. E. Standard, K. Dokumen, and B. B. Testing, "1,2 1* , 2," no. November 2018, pp. 1044–1052, 2024.

[17] D. W. T. Putra and R. Andriani, "Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD," J. TeknoIf, vol. 7, no. 1, p. 32, 2019, doi: 10.21063/jtif.2019.v7.1.32-39.

[18] S. Kelly and K. Kumar, "RESTful APIs," Unity Netw. Fundam., vol. 2, no. 1, pp. 55–89, 2022, doi: 10.1007/978-1-4842-7358-6_3.

[19] N. Anwar, M. Munawwar, M. Abduh, and N. B. Santosa, "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 3, pp. 783–791, 2018, doi: 10.29207/resti.v2i3.606.

[20] V. Yuniati, G. Indriyanta, and A. Rachmat C., "Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File," *J. Inform.*, vol. 5, no. 1, 2011, doi: 10.21460/inf.2009.51.69.