https://doi.org/10.32815/jitika.1229

Volume 20, Issue 1, 2026

Jurnal Ilmiah Teknologi Informasi Asia

Journal Homepage: https://jurnal.asia.ac.id/index.php/jitika

Article

Implementation of AES-256 encryption for data security on the Desa Cantik administration services website

Febiola, Kasmawi *, Nurmi Hidayasari

Teknik Informatika, Politeknik Negeri Bengkalis, Bengkalis, 28711, Indonesia

***Abstract*—Data security in village administration service systems is a critical concern, as these systems manage sensitive personal information such as full names, National Identity Numbers (NIK), Family Card (KK) numbers, addresses, and supporting documents. Many existing village administration systems store such data without adequate protection, increasing the risk of data leakage, identity theft, and unauthorized access. This study implements the Advanced Encryption Standard (AES-256) algorithm to enhance data security in a village administration services website. The research methodology includes system requirements analysis, system design, AES-256 implementation for personal data and document encryption, and functional and performance evaluation. The system automatically encrypts all sensitive data before storing it in the database and decrypts it only for authorized administrators. In addition, the system supports secure processing of statistical Excel files to facilitate the Desa CANTIK program. Experimental results show that the proposed system provides strong data protection with minimal performance overhead, averaging less than 120 ms for encrypting and decrypting 5 MB files, while maintaining acceptable CPU and memory usage. These results indicate that AES-256 can be effectively integrated into village administration services to improve data security without compromising system efficiency.**

Keywords*—*aes-256; data security; village administration services; encryption; desa cantik program

1. Introduction

The rapid advancement of information technology has significantly transformed public administration, particularly through the adoption of web-based systems that simplify document management and service delivery. In village governance, digital administration services have improved accessibility, transparency, and efficiency by enabling citizens to submit requests and access information online. However, alongside these benefits, digital transformation has also increased exposure to cyber threats, including data leakage, unauthorized modification, and information tampering. These risks pose serious challenges to the integrity and trustworthiness of digital public service systems.

Village administration services routinely manage highly sensitive personal data, such as full names, National Identity Numbers (NIK), Family Card (KK) numbers, residential addresses, and population documents. In many cases, such data are stored without adequate protection mechanisms, making them vulnerable to unauthorized access. This condition significantly heightens the risk of identity theft, digital fraud, and misuse of personal information. As digital services expand at the village level, insufficient data security measures can

* Corresponding author.
E-mail Address: *kasmawi@polbeng.ac.id (Kasmawi)*

Author E-mail(s): F (*ffebiola99@gmail.com*), K (*kasmawi@polbeng.ac.id*), NH (nurmihidayasari@polbeng.ac.id)
Digital Object Identifier 10.32815/jitika.1229
Manuscript submitted 10 December 2025; revised 19 January 2026; accepted 19 January 2026.
ISSN: 2580-8397(O), 0852-730X(P).

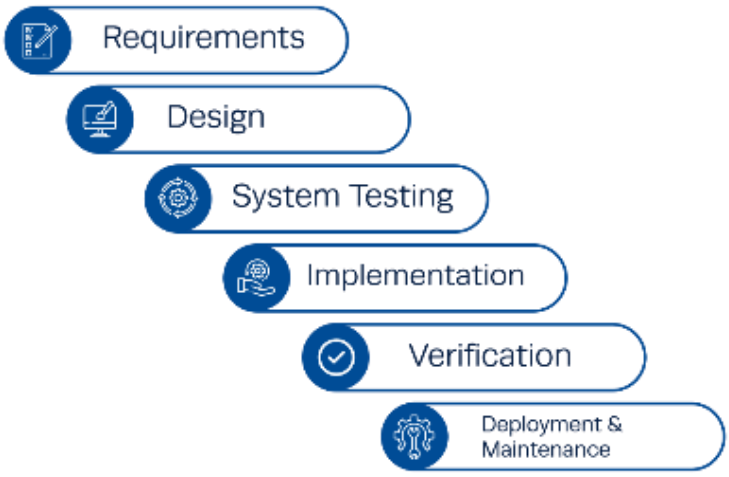

Fig. 1. Waterfall Method

undermine public trust and compromise the credibility of e-government initiatives.

The shift toward web-based village administration systems has been widely adopted across Indonesia, demonstrating tangible improvements in public service delivery. Several studies report that the implementation of village information systems reduces administrative bottlenecks, minimizes physical document accumulation, and allows citizens to independently access services online (Chanifah & Widiyarta, 2024; Mohamad et al., 2024; Zainudin et al., 2022). Moreover, digitalization initiatives have been shown to enhance transparency and responsiveness in village governance, although they remain constrained by uneven digital literacy and infrastructure readiness in certain regions (Anugrah et al., 2023; Yuliana & Natalia, 2025).

Despite these positive outcomes, the digitalization of public services introduces substantial data security risks. Public sector systems are attractive targets for cybercriminals due to the large volume of confidential data they store. Data breaches, privacy violations, and infrastructural vulnerabilities have been identified as major threats in digital public service environments, particularly at the local government level, where technical and financial resources are often limited (Aprilia et al., 2025; Sari et al., 2024). Additionally, human factors such as insufficient cybersecurity awareness and a lack of security culture among administrators further exacerbate these risks.

To mitigate such threats, cryptography has emerged as a fundamental approach to securing sensitive information. Cryptography enables data to be transformed into unreadable formats, ensuring confidentiality and preventing unauthorized access during storage and transmission (Swari et al., 2023). Among various cryptographic techniques, symmetric encryption algorithms are widely favored for their efficiency in protecting large volumes of data within information systems. The adoption of robust encryption methods is therefore essential for safeguarding personal data in village administration services.

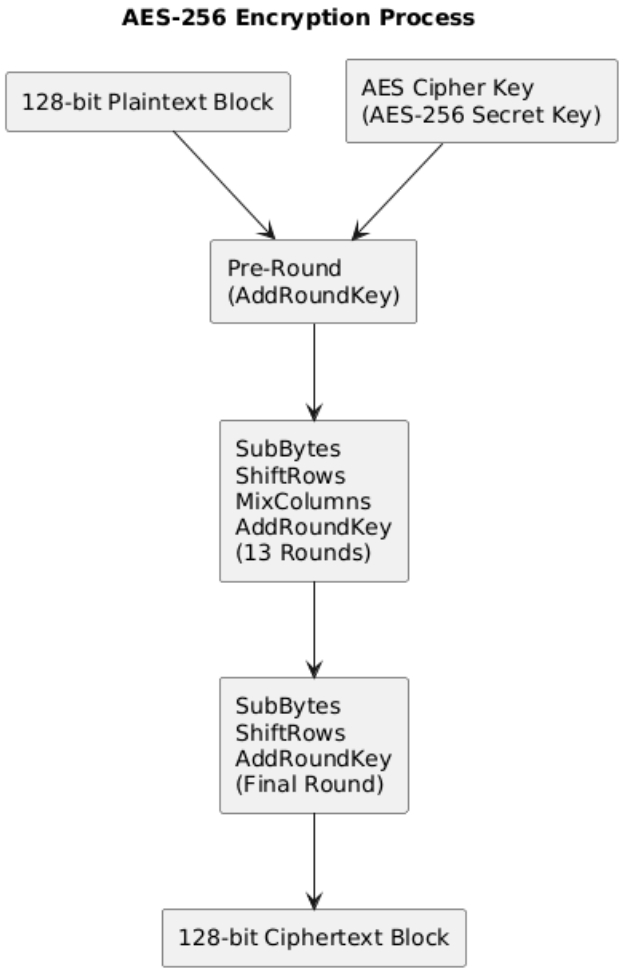

Fig. 2. Encryption Process

Advanced Encryption Standard with a 256-bit key length (AES-256) is widely recognized as one of the most secure and reliable encryption algorithms in modern cryptography. AES-256 offers strong resistance against brute-force, differential, and linear cryptanalysis attacks, making it particularly suitable

for protecting highly sensitive data (Adam & Romli, 2024; Azhari et al., 2022). In addition to its high security level, AES-256 demonstrates computational efficiency and flexibility, enabling its implementation across various platforms, including web-based systems, without significantly degrading system performance (Putra et al., 2024; Ugwunna et al., 2024).

The implementation of AES-256 encryption in village administration services is also closely aligned with the Desa CANTIK (Desa Cinta Statistik) program, which emphasizes accurate, secure, and data-driven village development. As a designated Desa CANTIK, Air Putih Village is expected to manage community data responsibly and utilize statistical information effectively to support development planning (Kamala, 2025). Therefore, strengthening data security through AES-256 encryption not only protects citizens' personal information but also supports the objectives of Desa CANTIK by ensuring data integrity, confidentiality, and reliability within the village administration service system.

2. Method

The method used to design website administration services employs the Advanced Encryption Standard (AES). The website was developed using a waterfall or waterfall model. The waterfall model is a classic, systematic, and sequential approach to the progression of a system through analysis, design, coding, testing, and maintenance. This model is often used in software engineering and other development projects. The stages that can be carried out in this development method consist of several stages and can be seen in Fig. 1 (Damayanti & Yulianingsih, 2024).

2.1. AES-256 (Advanced Encryption Standard)

AES, or (Advanced Encryption Standard), is a symmetric key encryption standard that can be used to secure data, developed by Belgian cryptographers Joan Daemen and Vincent Rijmen (Firdaus & Santika, 2022). AES 256 encryption carries out a 14-round coding process (Fig. 2) consisting of the addroundkey, bytesub, shiftrows, and mixcolumn processes. However, before entering the first round, the password and plaintext are processed by the AES key scheduler, which is part of the PreRound stage. After going through the key schedule, the encryption process continues until rounds 1 to 13 with processes named SubBytes, ShiftRows, MixColumn, and AddRoundKey. In the last round, namely round 14, no MixColumns is performed; only SubBytes, ShiftRows, and AddRoundKey are used. The final result of the entire encryption process is called the ciphertext (Indrayani et al., 2025).

The encryption process begins with a 128-bit plaintext block and a 256-bit secret key. After the key expansion phase (Pre-Round), the algorithm performs 13 standard rounds consisting of SubBytes, ShiftRows, MixColumns, and AddRoundKey operations. The final round excludes the MixColumns step. The output of the process is a 128-bit ciphertext block.

2.2. System Requirements Design

System requirements play a crucial role in the development of the system to be created. By understanding user needs and existing problems, researchers can design and implement the system, thereby generating solutions to meet those needs. At this stage, system requirements are generated based on the analysis of the current system and system documentation (Arianto et al., 2023). The system requirements design that has been created can be seen in Table 1.

Table 1. System Requirements

No	Analysis Results	Output
1	System	The system can display service application forms, encrypt personal data and documents (AES-256), decrypt data by the admin, upload and process statistical Excel files, display a summary of population data, and manage service data (view, delete, and download).
2	Users	Users can complete administrative service forms, upload supporting documents, and view the status of their service requests. All submitted data will be automatically encrypted.
3	Village Admin	Admins can access decrypted data, verify submissions, download documents, upload Excel files for statistics, and view automated summary results.

2.3. System Flow Analysis

In the village administration service system design, all personal data and documents uploaded by the community must be encrypted using AES-256 before being stored in the database (Fig. 3). The system accepts files in common formats such as PDF, JPG, PNG, and other supporting documents. Once received, the system immediately runs the encryption process and stores the ciphertext in the database to prevent unauthorized parties from reading it. On the admin side, the system automatically decrypts the data when the admin opens the service request details. In addition to administrative services, the system design also includes a village statistical data processing flow, where the admin can upload an Excel file containing population data. The system then processes the file and generates an automatic summary based on specific categories such as gender, population, and age group. Analysis of this system's flow helps ensure that the encryption, data storage, and statistical processing processes are structured, secure, and meet the needs of village services.

Fig. 3 illustrates the sequence diagram of the AES-256 encryption implementation in the village administration service system. The diagram shows step-by-step interactions among the user's browser, the Laravel controller, the AES encryption service, and the database, including data submission, encryption, storage, decryption, and statistical data processing.

2.4. Key Management System (KMS)

The security of the AES-256 implementation in this system relies on a centralized Key Management System (KMS). The encryption key is generated using Laravel's built-in secure random generator (random_bytes) and stored in an encrypted environment variable (.env) on the server. The key should never be hard-coded in the application's source code. Access to the key is restricted through server-level permission controls. Periodic key rotation is planned by re-encrypting sensitive records

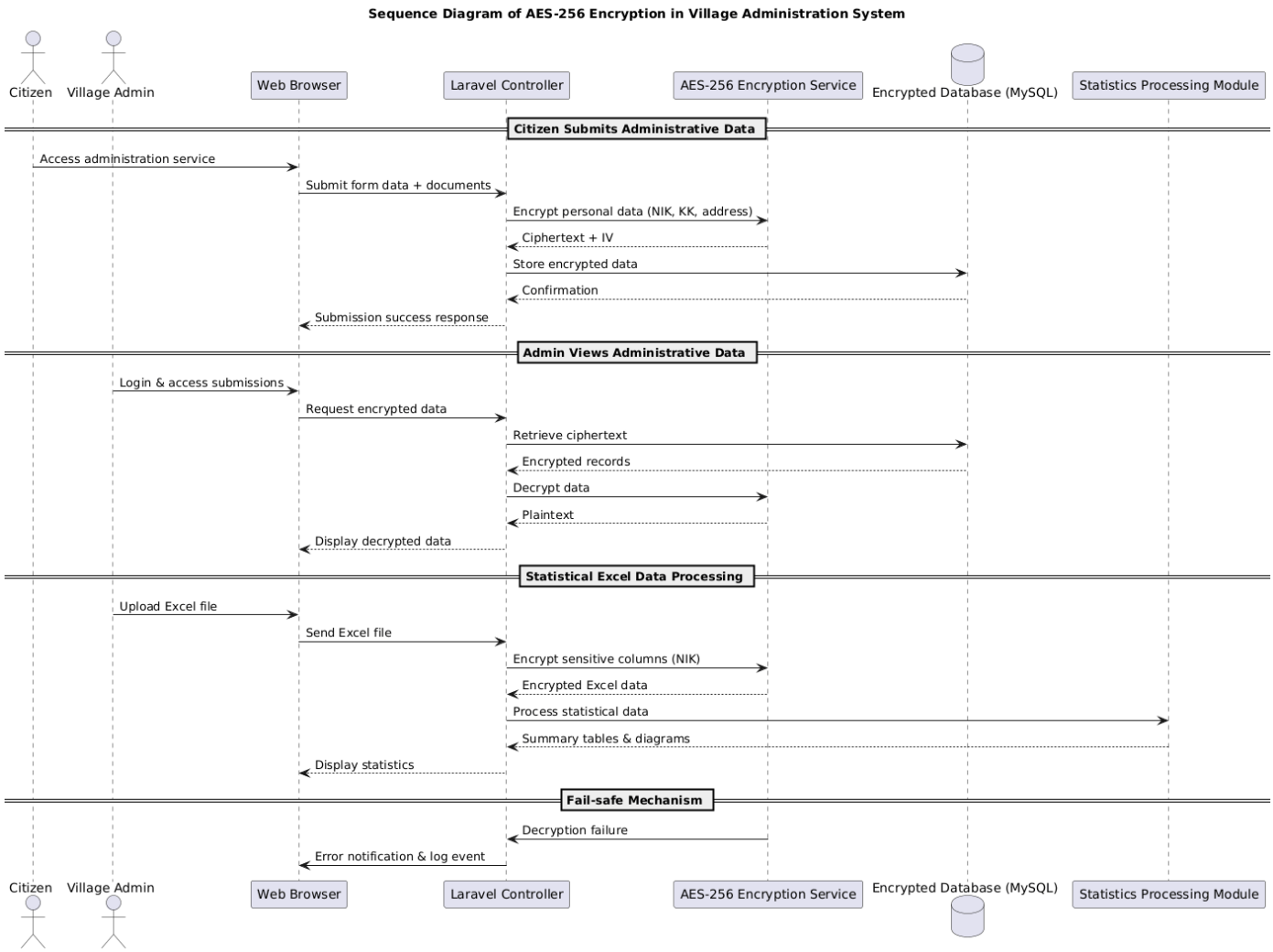

Fig. 3. Sequence Diagram of AES-256 Encryption Process

during scheduled maintenance to minimize key exposure risks.

2.5. Deployment Environment

The system is deployed on a Linux-based server using Apache web server and PHP 8.x. Encrypted data backups are performed daily using automated cron jobs. Database migrations are handled using Laravel migration tools to ensure encrypted fields remain intact without altering ciphertext values.

3. Results

This research produces an administrative service application using the AES-256 (Advanced Encryption Standard) algorithm. This application is website-based and can be accessed from desktop or mobile devices. The programming language used is Laravel with MySQL as its database. Laravel is a PHP framework for creating web-based applications (Sansprayada & Suteja, 2019). The following is an implementation of the design results that have been made previously:

Fig. 4 shows the main dashboard page of the Air Putih Village application. This page is the initial display presented to users when they open the website.

Fig. 5 shows the implementation of the Letter Submission page in the Air Putih Village administrative services application. This page provides a digital form for residents to submit various types of letters online. The form contains several data fields, including the applicant's identity, address, occupation, purpose of use, and supporting document uploads.

Fig. 7 shows the implementation of the letter data management page in the administration services application. On this page, administrators can digitally view the entire list of letters submitted by the public. The data is displayed in tabular form, simplifying the review and management of each letter submission.

Fig. 6 shows the implementation of the Letter Submission Details page in the administration services application. This page is used by the admin to view complete information about a selected letter submission. All data entered by the applicant during submission is displayed in a structured manner, making it easier for the admin to check, verify, and follow up on the letter-creation process.

Fig. 9 shows an implementation of the Air Putih Village Statistics page in the village administration services application. This page presents population data for Air Putih

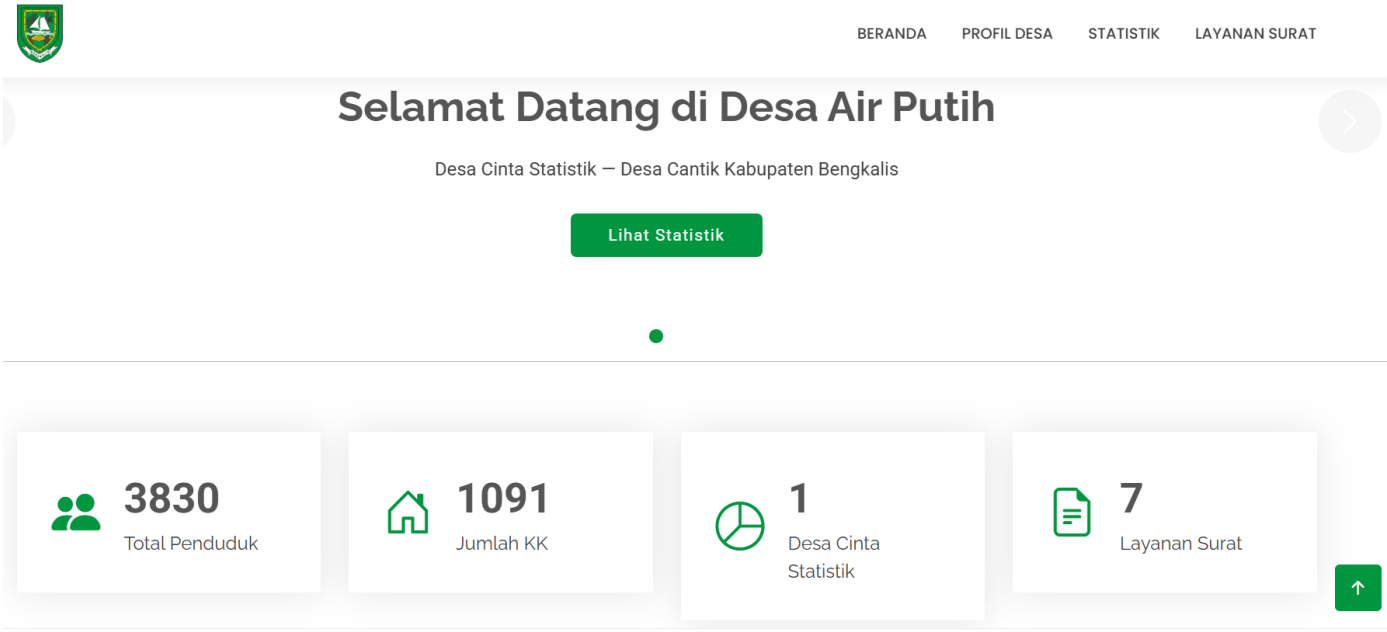

Fig. 4. Page dashboard

Fig. 5. Letter submission page

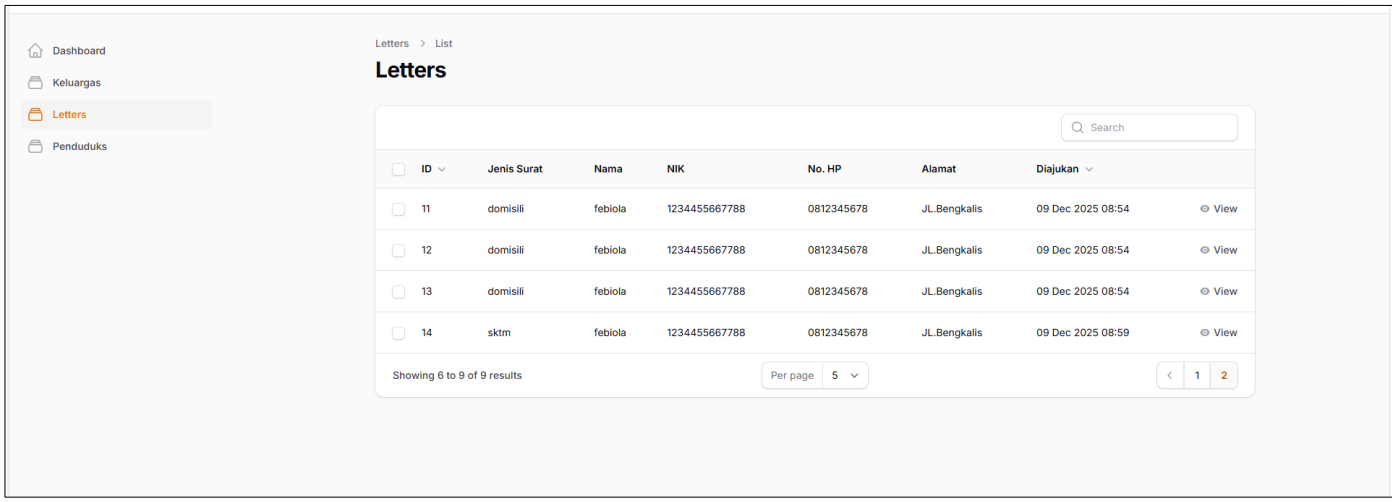

Fig. 7. Admin page

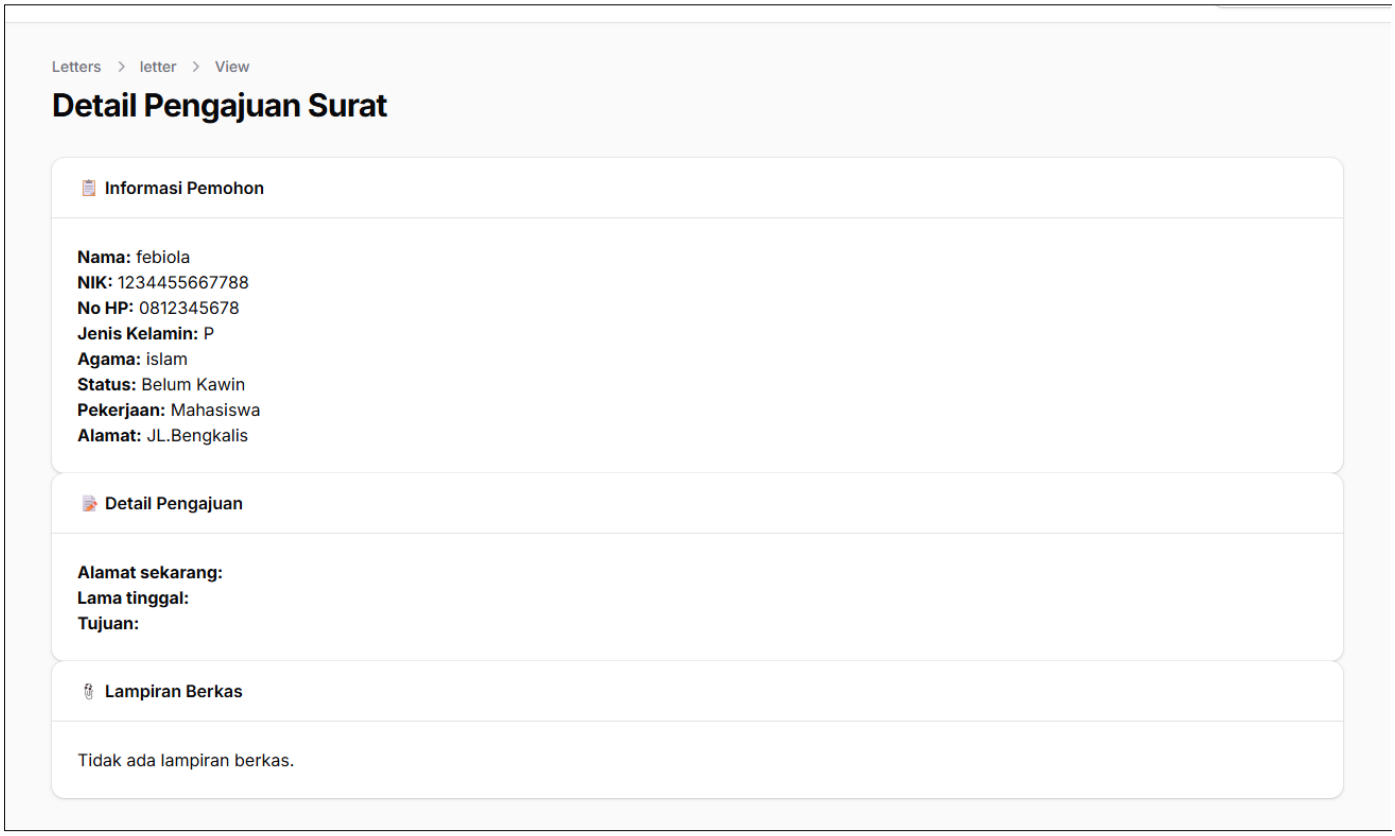

Fig. 6. Letter Submission Details page

Village in visual form to facilitate easier and more interactive demographic information. This statistical information is sourced from a collaboration between the village and Statistics Indonesia (BPS), ensuring accurate and accountable data.

Fig. 8 Shows the results of data encryption in the database, where personal data such as National Identification Number (NIK) and addresses are encrypted using the AES-256 algorithm. The data displayed in the database column is ciphertext (encrypted text) that unauthorized parties cannot read without a decryption process. By storing data in this encrypted form, sensitive public information is protected against leakage, theft, or misuse, while ensuring optimal server-side security.

3.1. Security and Integrity of Statistical Excel Data

In the Desa CANTIK program, data accuracy and integrity are critical, as the processed data are used for reporting and coordination with the Central Statistics Agency (BPS). To ensure data integrity during the transition process, the system automatically encrypts Excel files uploaded by village

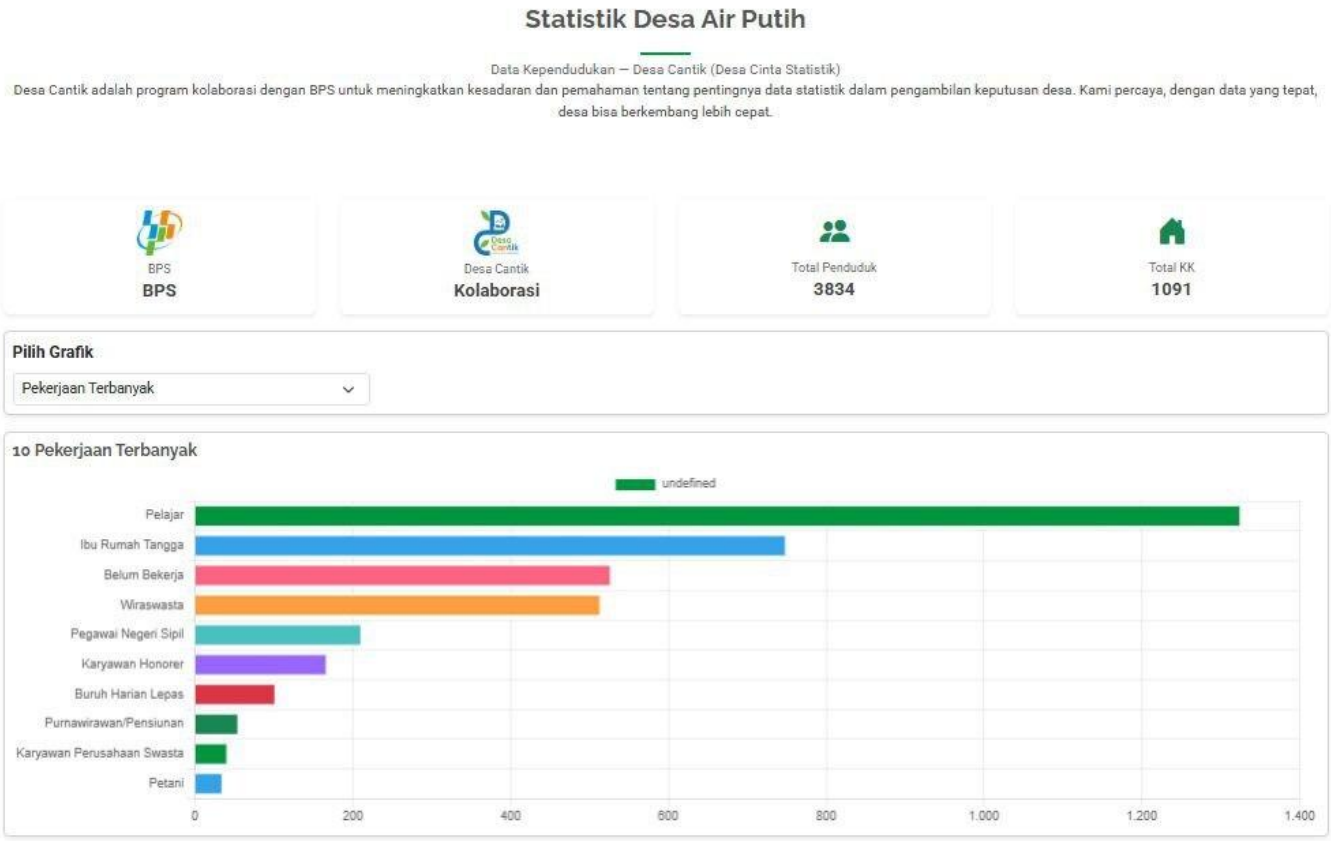

Fig. 9. Statistics page

	id	type	name	nik	phone	tempat_lahir	tanggal_lahir	jenis_kelamin
Edit Copy Delete	1	sktm	febiola	PlJTf0DtTxlzYXteQN66ZkxnaWh4MXdYeEU3VzMwYndpUC9vMm...	riakHntLArbjNgRPUy62gVVQcE5hZHdHWGNWQ2t1Vm5wT1BTVn...	Bengkalis	2002-08-03	L
Edit Copy Delete	2	domisili	pebiola	s6Z68EEzqu54CGkr3RUWP3lLUGNpSUpJQkNlalU4a0Jqam9yTm...	8moKzVwJsj099HyTyHUbnno0bGYyRjVFRFFrRGUvVVhlakFFSm...	Bengkalis	2000-01-28	P
Edit Copy Delete	3	sktm	Harada	h7etJRw+0TDmY4vc4SaTxUMrbHQwYlllRm1mVWdjTTILL0tKWn...	KFLM8wK5BPKz0iEaRJR1YytwNGRtV0hQRXV6RGJrTHJVRDZYVV...	air putih	1992-06-20	P
Edit Copy Delete	4	pengantar_ktpkk	dadang	0PNz2qQE7yh58tam5ixXOmxOdnVKai9GVWhMSUJJZUdLRkJBeX...	EiNJDib56qjTqZYovQ6Uk1IPR0IBYXBBSTJqNW1Kd0tkSGdscl...	Jangkang	2001-03-18	L

Fig. 8. AES-256 encryption result

administrators immediately after upload. Sensitive attributes, such as National Identity Numbers (NIK), are encrypted using the AES-256 algorithm before the file is stored or processed.

The encryption process is performed without modifying the data structure or statistical values contained in the Excel file. Only identifier fields are encrypted, while numerical and categorical data used for statistical calculations remain unchanged. This approach ensures that encryption does not affect statistical aggregation results, such as population counts, gender distributions, and age-group analyses.

In addition, access to encrypted Excel files is restricted to authorized administrators. Decryption is only performed temporarily during internal processing, and the results are immediately converted into aggregated statistical tables and visual diagrams. This mechanism ensures that statistical data remains accurate, consistent, and protected from unauthorized modification throughout the data transfer and processing stages.

3.2. User Interface Design and Training for Village Officials

Implementing an encrypted village administration system requires consideration of the users who will operate it, particularly village officials with varying levels of computer literacy. To minimize operational errors, the system is designed with a simple and intuitive user interface. Encryption and decryption are executed automatically at the system level, so administrators do not need to perform any manual cryptographic operations.

The user interface provides clear form labels, structured data tables, and visual indicators for upload status and processing results. Validation mechanisms are applied during data input and file upload to prevent incorrect or incomplete submissions. Error messages are presented in a concise and understandable

format to guide users in resolving issues.

In addition to interface design, basic training sessions were conducted for village administrators to introduce secure data-handling workflows, system navigation, and error-recovery procedures. These measures help ensure that encrypted data management can be performed effectively and securely, even by users without advanced technical backgrounds.

3.3. Application Security Audit

In addition to data encryption, application-level security is a critical component of the system implementation. A security audit was conducted to evaluate common web application vulnerabilities, including SQL injection, cross-site scripting (XSS), and unauthorized access.

The system uses Laravel's built-in Object-Relational Mapping (ORM) to prevent SQL injection attacks by ensuring that database queries are parameterized rather than constructed directly from user input. Cross-site scripting (XSS) attacks are mitigated through automatic output escaping and input validation mechanisms provided by the framework

Furthermore, Cross-Site Request Forgery (CSRF) protection is enforced using Laravel's CSRF tokens for all form submissions. Role-based access control is implemented to restrict sensitive operations, such as data decryption and document downloads, to authorized administrators only. These security measures complement AES-256 encryption, resulting in a holistic, layered security architecture.

3.4. AES-256 Implementation in Laravel Controller

The AES-256 encryption mechanism is implemented at the controller level to ensure that sensitive data is encrypted before being stored in the database. The system uses a symmetric encryption approach with a 256-bit secret key. The encryption key is securely stored as an environment variable on the server and is never hard-coded into the application source code, as detailed in Algorithm 1.

For each encryption process, a random Initialization Vector (IV) is generated to prevent identical plaintext values from producing the same ciphertext. The system applies Cipher Block Chaining (CBC) mode with PKCS7 padding to handle data blocks that are not aligned with the AES block size. The following pseudocode illustrates the AES-256 encryption workflow applied to sensitive data before it is stored in the database. This process ensures that all sensitive data is encrypted before storage and can be decrypted only by authorized administrators.

Algorithm 1: AES-256 Encryption Process.

Input: Plaintext data, SecretKey (256-bit).
Output: Ciphertext

```
Generate a random Initialization Vector (IV)
Apply PKCS7 padding to the plaintext
Encrypt the plaintext using AES-256 in CBC mode
Combine IV and Ciphertext
Store the encrypted data in the database
Return Ciphertext
```

Table 2. AES-256 Security Test Results

No	National ID (NIK)	Address	Test results
1.	T7RtOV88ENhlHOzaPC41AlltVTR4UlFsbDlKMDhoM2NCSWEvMXdpM3ZKdXdzdlFaaTdlZEkxdFJlb 2M9	i94WBbmFiMi92IniNwtBakdDc1EreDI5OEpHeVQvbFhKTnRNWXc9PQ==	Not successful
2.	4mu/aTGM576KRTsfOr7nLDkrZkE0d3dJM1dZcTYxT1p2VHczY2JJSU9jZUU1dHpKR2dlWDRtUFFqe XM9	G+xtNTsXGTUGHRHGQjyKJnVRS2pDaWZ3aXNXdTU1NWtlbU9wQnc9PQ==	Not successful
3.	ohLhK0EiDCNPJ4adYhaUUjVnL2lvaXB0RHh3bWxmcGJQWllVMFF2NG1hRndSUUR0cnV0Q1dwbk0 1Tjg9	3J7Ij9z+JyTHPbuoVB2SsG9DTjFQLytZK2Z4OTYxNnh1R3UxUkE9PQ==	Not successful
4.	I99k/vRsDhdBKZ87rR3jNjR4RVVma1I2a0h0bDhyVW1KTHA1Nit0NXBRYldlOUVwTXJkUW41Ukpu WnM9	SspKSWo4M3IHUau1vluAZ0VkcUNIcnNLSWxKNEw3UEVld1hHU1E9PQ==	Not successful
5.	whkV10bEOzAf17krLL3PemdhYyt5MFNRNE51cHZGSTBjdUVUQXZ6OXNUWE9iWkdTWkxQNFJ5VXV0Y2c9	g/UA8Vm9CS1Fl7kVqt2oPWZvQWc1MjA1ejJhK2E1N2Q0aEozc2c9PQ==	Not successful
6.	eTsUX9doRR6QSgW2nUtU9UlYc1p2UUgzQzVnZzcwTlRESGoyaE1XaTVZdnJhNmhWW5WSjdxMVdLOHc9	CQKYyVbppb06EzPh22YK0nBLMmE0TlRUK2hGK0NsZnRac2NTR2c9PQ==	Not successful
7.	KLcHZf1Ael0kGdXrewt4JVV3YWpURXdJWmNDc0xWK05ZZ29yZytCdGFvVHJrdEhlOXd2cW1OYS9O bUU9	z0NaBNx3iQg3lzAEPGI7kXFVbXFPQTd1eTgyQjdwd0RWWlJ2WlE9PQ==	Not successful

3.5. System Scalability and Large File Handling

The village administration service system is designed to handle high-volume administrative requests and large document uploads efficiently. To prevent server overload during peak usage, the system applies request validation, file size limitations, and optimized encryption workflows.

Document uploads, including high-resolution scans of Family Cards and identity documents with a maximum size of 5 MB, are processed using a streaming-based encryption approach. This method reduces memory consumption by encrypting files in manageable blocks rather than loading entire files into memory at once.

In addition, encryption is performed asynchronously to avoid blocking user requests. This ensures that multiple users can submit administrative requests simultaneously without significant delays. Performance monitoring during testing shows that the system remains responsive under concurrent access conditions, demonstrating its scalability and suitability for real-world village administration environments.

3.6. Fail-Safe Mechanisms and Error Handling

In practical system deployments, encryption and decryption processes may fail due to corrupted files, incomplete uploads, or

invalid cryptographic parameters. To address these scenarios, the system incorporates fail-safe mechanisms and structured error handling to maintain data integrity and system stability.

During decryption, the system verifies the integrity of the encrypted data and the availability of the corresponding Initialization Vector (IV). If decryption fails, the system immediately halts the process, prevents data from being displayed, and records the event in a server-side error log for administrative review. This approach ensures that corrupted or manipulated data cannot be mistakenly processed or exposed.

For file uploads, validation checks are performed to verify file format, size limits, and completeness before encryption is initiated. If a corrupted or unsupported file is detected, the system rejects the upload and notifies the user to submit a valid document. These fail-safe mechanisms ensure that the system remains reliable and secure, even in the presence of user errors or unexpected system conditions.

3.7. AES-256 Security Test Results

The 7-community data from the NIK and the address are used to test the strength of the AES-256 encryption. The results are tested against the Bruteforce Key attack simulation using the Cryptool tool, as in Table 2.

3.8. Performance Evaluation of AES-256 Encryption

The performance evaluation shows that the AES-256 encryption and decryption processes introduce minimal overhead to the system (Table 3). For small files (100 KB), encryption time is below 20 ms, while for larger files (5 MB), processing time remains under 120 ms. CPU and memory usage increase proportionally with file size but remain within acceptable limits for web-based village administration services. These results confirm that AES-256 can be implemented without significant performance degradation.

Table 3. Performance Evaluation of AES-256 Encryption

File Size	Encryption Time (ms)	Decryption Time (ms)	CPU Usage (%)	Memory Usage (MB)
100 KB	14	13	3	8
1 MB	41	39	7	16
5 MB	118	115	12	32

4. Discussion

The findings of this study indicate that implementing AES-256 encryption effectively enhances data security on the Desa CANTIK administration services website. All sensitive personal data is securely encrypted prior to storage, preventing unauthorized access even in the event of a database compromise. This result is consistent with previous studies that emphasize AES-256's robustness in protecting confidential public-sector data. Adam & Roml (2024) demonstrated that AES-256 provides strong confidentiality guarantees for sensitive personnel documents, while Azhari et al (2022) confirmed its resistance to brute-force and cryptanalytic attacks in government-related information systems. These similarities reinforce the suitability of AES-256 for securing village-level administrative data.

In terms of system performance, this study recorded an average encryption and decryption time of approximately 120 ms for files up to 5 MB. This processing time is considered acceptable for village administration services, where transactions are typically asynchronous and do not require real-time responses. Comparable results were reported by Ugwunna et al (2024), who found that AES-256 encryption in web-based systems introduces minimal latency that does not significantly affect user experience. Likewise, Putra et al (2024) reported encryption delays within the 150 ms range for similar file sizes, indicating that the performance observed in this study is slightly more efficient than several prior implementations. These comparisons suggest that AES-256 can be deployed in resource-limited environments without compromising system responsiveness.

However, some studies present contrasting perspectives regarding the performance implications of AES-256. Research by Mabruri & Alamsyah (2020) noted that AES-256 may introduce noticeable latency in mobile-based applications when compared to AES-128, particularly under constrained computational resources. Similarly, Boura et al (2023) highlighted that higher key lengths, while offering stronger security, inevitably increase computational complexity. The relatively stable performance observed in this study can be attributed to the moderate workload of village administration systems and the use of server-based processing rather than mobile-only environments, which mitigates the performance drawbacks identified in earlier research.

The adoption of a random Initialization Vector (IV) further strengthens the security model by ensuring that identical plaintext inputs yield different ciphertext outputs. This approach aligns with best practices recommended in cryptographic research and standards. Halimi et al (2024) demonstrated that combining AES with randomized parameters significantly reduces vulnerability to pattern-based attacks. Nevertheless, several studies acknowledge the trade-off between security and performance when using random IVs. Subedar & Ashwini (2020) observed that randomized IV generation slightly increases encryption and decryption time due to additional processing and storage overhead. This finding supports the results of the present study, which showed that data retrieval operations were marginally slower, particularly during search and comparison.

Despite its strengths, this study has limitations that align with concerns raised in prior research. Key management remains a critical factor in the overall security of AES-256–based systems, as emphasized by Baso & Anriani (2024) and Goel et al (2024). Improper key storage or rotation could undermine even the strongest encryption algorithms. Additionally, the performance evaluation in this study was conducted under limited concurrent access conditions, similar to the scope limitations reported by Pooja (2025). Future studies should examine system scalability under higher user loads and explore hybrid encryption or indexing strategies to mitigate the performance impact introduced by random IV usage.

5. Conclusion

This study demonstrates that implementing AES-256 encryption in the village administration service system effectively improves the security of community data. All

personal data entered through the service form, including name, address, National Identity Number (NIK), Family Card (KK) number, and supporting documents, is successfully encrypted before being stored in the database, preventing unauthorized access. Furthermore, the Excel file upload process for statistical data also includes an encryption mechanism, which automatically converts sensitive elements, such as the NIK in the population table, into ciphertext, ensuring their security even in the event of unauthorized access to the storage. This implementation demonstrates that AES-256 maintains the confidentiality and integrity of data without reducing system performance. Overall, the system developed not only improves the security of village administration services but also supports the maintenance of statistical data that is more protected and in accordance with information security principles.

Data Availability

All data generated or examined during this research are presented in this paper.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Authors' Contributions

Febiola conducted the system implementation and drafted the initial manuscript. Kasmawi supervised the research process and contributed to the system design and manuscript revision. Nurmi Hidayasari contributed to the security analysis and manuscript refinement. All authors reviewed and approved the final version of the manuscript.

References

Adam, P., & Romli, M. A. (2024). Implementasi Sistem Keamanan Dokumen Kepegawaian Menggunakan Metode Aes-256 Dan Vigenere Chiper. *Jurnal Komputer Dan Teknologi*, *2*(2), 20–26. https://doi.org/10.58290/jukomtek.v2i2.166

Anugrah, S. D., Ardiansyah, M. R. N., Rahmawati, D. A., Aniq, A. H., Kholisa, Y. N., Rahmadani, A. N., Maharani, S. A., Wardani, A. A. A. M. C., Prasojo, Y. R., & Wahyudi, K. E. (2023). Mewujudkan Digitalisasi Pelayanan Pemerintah Dalam Upaya Mencapai Desa Digital Di Desa Banjarsari Kabupaten Probolinggo. *JPHM-Widyakarya*, *1*(4), 149–163.https://doi.org/10.59581/jphm-widyakarya.v1i4.2029

Aprilia, K., Maghfira, R. S., Aji, R. P., & Saputra, D. I. S. (2025). Analisis RIsiko Keamanan Teknologi Infromasi Pada Instansi Pemerintahan Purbalingga. *Journal of Practical Computer Science*, *5*(2). https://doi.org/10.37366/jpcs.v5i2.5960

Arianto, B., Kurniadi, H., & Kurniasari, I. (2023). Implementasi Pengarsipan Elektronik Menggunakan Enkripsi Dan Dekripsi Dengan Metode {AES} Di {Uniska}. *Jurnal Fasilkom*, *13*(2), 259–268. https://doi.org/10.37859/jf.v13i02.5060

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Baso, F., & Anriani L, N. (2024). Implementasi Teknik Kriptografi dengan Metode {AES} 256 untuk Keamanan File. *Information Technology Education Journal*, *3*(3), 84–87. https://doi.org/10.59562/intec.v3i3.5525

Boura, C., Derbez, P., & Funk, M. (2023). Related-Key Differential Analysis of the AES. *Iacr Transactions on Symmetric Cryptology*, *2023*(4), 215–243. https://doi.org/10.46586/tosc.v2023.i4.215-243

Chanifah, S., & Widiyarta, A. (2024). The Effectiveness of the "Desa SIAP" Website in Improving Public Services in Leran Village, Manyar District, Gresik Regency. *Jurnal Ilmiah Ilmu Administrasi Publik*, *14*(2), 509. https://doi.org/10.26858/jiap.v14i2.66522

Damayanti, N. R., & Yulianingsih, E. (2024). Design Aplikasi Catatan Daily Berbasis {Android} Menggunakan Metode {Waterfall}. *Journal of Information Technology Ampera*, *5*(1), 2121–2774. https://doi.org/10.51519/journalita.v5i1.469

Firdaus, R., & Santika, R. R. (2022). Penerapan Algoritma {AES}-128 Untuk Enkripsi Dokumen Di {PT Caveo Biometric Security}. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Universitas Budi Luhur*, 111–120.

Goel, A., Baliyan, H., Tyagi, S., & Bansal, N. (2024). End to End Encryption of Chat Using Advanced Encryption Standard-256. *International Journal of Science and Research Archive*, *12*(1), 2018–2025. https://doi.org/10.30574/ijsra.2024.12.1.0923

Halimi, A. D., Tholib, A., & Yaqin, M. A. A. (2024). Optimasi Keamanan Data Penerimaan Mahasiswa Menggunakan Aes-256, Sha-256, Dan Base64. *Justify Jurnal Sistem Informasi Ibrahimy*, *3*(1), 38–45. https://doi.org/10.35316/justify.v3i1.5107

Indrayani, R., Ferdiansyah, P., & Koprawi, M. (2025). Analisis Penggunaan Kriptografi Metode {AES} 256 Bit pada Pengamanan File dengan Berbagai Format. *Digital Transformation Technology*, *4*(2), 1245–1251. https://doi.org/10.47709/digitech.v4i2.5457

Kamala, S. (2025). *Penjelasan Program Desa Cinta Statistik 01 Penjelasan Umum*.

Mabruri, A. S., & Alamsyah, A. (2020). Data Security System of Text Messaging Based on Android Mobile Devices Using Advanced Encrytion Standard Dynamic S-Box. *Journal of Soft Computing Exploration*, *1*(1). https://doi.org/10.52465/joscex.v1i1.10

Mohamad, Y., Bonok, Z., & Abdussamad, S. (2024). Digital Transformation: Tabumela Village Government Administration Management Through a Web-Based System. *Ejppm*, *2*(2), 52–62. https://doi.org/10.37905/ejppm.v2i2.25

Pooja, T. (2025). Design of Advanced Encryption Standard Using Verilog HDL. *Interantional Journal of Scientific Research in Engineering and Management*, *09*(01), 1–9. https://doi.org/10.55041/ijsrem39724

Putra, J. S., Ardianto, R., & Purwono, P. (2024). Tinjauan Terhadap Implementasi Advanced Encryption Standard 256 Dalam Keamanan Data. *Device Journal of Information System Computer Science and Information Technology*, *5*(2), 335–355. https://doi.org/10.46576/device.v5i2.4621

Sari, J. A., Yuliani, I., Akadira, T., Sunarya, A., & Ating, R. (2024). Data Security and Individual Privacy From the Perspective of Public Administration. *Ilomata International Journal of Social Science*, *5*(3), 818–830. https://doi.org/10.61194/ijss.v5i3.1297

Subedar, Z., & Ashwini, A. (2020). Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication. *International Journal of Mathematical Sciences and Computing*, *6*(4), 35–41. https://doi.org/10.5815/ijmsc.2020.04.04

Swari, M. H. P., Maulana, H., Handika, I. P. S., & Satwika, I. K. S. (2023). Implementasi {AES} 256 Untuk Pengamanan Data Pada {Supply Chain Management} {BUMDes} Sarining Winangun Kukuh. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *6*(1), 12–19. https://doi.org/10.31598/jurnalresistor.v6i1.1332

Ugwunna, C. O., Okimba, P. E., Alabi, O., Orji, E. E., Olowofeso, E. O., & Ayomide, S. O. (2024). Advanced Encryption Standard (Aes) Implementation Efficiency Using Java and NODE.JS Platforms. *Fudma Journal of Sciences*, *8*(6), 42–49. https://doi.org/10.33003/fjs-2024-0806-2832

Yuliana, R. A., & Natalia, N. (2025). Transformasi Digital Desa

Ponggok: Tantangan Dan Potensi Menuju Desa Pintar Yang Berkelanjutan. *Academia Jurnal Inovasi Riset Akademik*, *5*(2), 90–97. https://doi.org/10.51878/academia.v5i2.4977

Zainudin, Z., Ilaalloh, F., Hermanto, D., Wijayanti, R., Affaf, M., Liesdiany, M., Faulina, R., & Salam, A. (2022). Pelatihan Penggunaan Aplikasi Administrasi Kependudukan Berbasis Website Bagi Perangkat Desa Tlangoh. *Sasambo Jurnal Abdimas (Journal of Community Service)*, *4*(4), 611–617. https://doi.org/10.36312/sasambo.v4i4.860

Febiola is currently pursuing a Bachelor of Applied Informatics Engineering degree in Information Systems Security at Bengkalis State Polytechnic, Indonesia. Her academic interests focus on data security, cryptographic implementation, and secure web-based information systems, particularly for public and community services. She has conducted research on the application of the AES-256 encryption standard to protect sensitive personal and statistical data in village administration systems. Her work emphasizes practical system implementation, data confidentiality, and the integration of security mechanisms into real-world administrative applications. service systems, including the AES-256 encryption standard, developing secure web applications, and maintaining structured and protected village statistical data.

Kasmawi is a lecturer and Head of the Informatics Engineering Department at Bengkalis State Polytechnic. He specializes in information systems development, data security, and the implementation of digital solutions for education and public services. He is active in community service, collaboration with schools (vocational high schools), research and application development supervision, and student training. He is involved in research and scientific publications, including mobile/web applications, information systems for MSMEs, and digital services.

Nurmi Hidayasari is a lecturer in the Department of Informatics Engineering, Bengkalis State Polytechnic, Indonesia. She currently specializes in information security and related topics. She is also currently writing a book on information security with a research team from the Applied Undergraduate Program in Information Systems Security. For the past three months, she has served as the Program Coordinator, focusing on strengthening the quality of learning, research, and scientific development in the field of information systems security.