Jurnal Multidisiplin Sahombu
E-ISSN : 2809-8587
Sean Institute

Design of Personal Data Security Scheme in Digital Public Service System Using AES-128 Cryptographic Algorithm

Fandi Fajar Maulana[1], Eka Jiparolim[2], Eko Nurcahyo[3], Jefry Sunupurwa Asri[4]
[1,2,3,4] Informatics Engineering Study Program, Faculty of Computer Science,
Universitas Esa Unggul

ARTICLE INFO

Keywords:
Cryptography, AES-128, Data Security, Public Services, Data Confidentiality

Email:
fandifajar31@student.esaunggul.ac.id, ekajiparolim123@student.esaunggul.ac.id, ekogandoz321@student.esaunggul.ac.id, jefry.sunupurwa@esaunggul.ac.id

ABSTRACT

Digital transformation in the public service sector has significantly accelerated the efficiency of government administration. However, this digitalization presents significant challenges related to cybersecurity, where the risk of personal data (Personally Identifiable Information) leakage poses a threat that could undermine public trust. This research aims to design a data security scheme in a public service system using the Advanced Encryption Standard (AES) cryptographic algorithm with a 128-bit key length. The research method used is conceptual design with a system development life cycle approach. The analysis results indicate that the AES-128 algorithm was selected due to its proven high performance and adequate level of security for public service needs. This design is recommended for implementation in public service databases to ensure the confidentiality of sensitive citizen data without overloading server performance.

INTRODUCTION

The development of information technology post-pandemic has fundamentally changed the paradigm of public services. The government is now required to provide services that are fast, transparent, and accessible from anywhere through digital platforms. This transformation towards e-government is a strategic step to increase administrative efficiency and minimize physical contact, which previously hampered conventional services (Sisilianingsih et al., 2023). This digitalization includes the management of large-scale population data exchanged via the internet. According to Heeks (2020), digital transformation in the public sector is not only about the application of technology but also involves reforming business processes and institutional capacity to utilize technology optimally. This emphasizes that e-government implementation must be accompanied by changes in organizational culture that support innovation and transparency.

However, the massive digitalization of public services is directly proportional to increased cybersecurity risks. Threats to data confidentiality and integrity pose serious challenges that can hamper the sustainability of this digital transformation. Leaks of personal data (Personally Identifiable Information), such as National Identification Numbers (NIK) and biometric data, not only harm individuals but also undermine public trust in government technology infrastructure (Alfi et al., 2023). According to Whitman & Mattord (2018), data vulnerabilities in public systems can arise from various factors, including weak credential management, outdated software, and insecure network configurations. Therefore, robust data protection mechanisms are required at the database layer before data is stored or transmitted.

One of the most effective data security methods is the application of cryptographic techniques. Among the various available algorithms, the Advanced Encryption Standard (AES) is known as a symmetric encryption standard with a high level of security. Based on performance comparison studies, the AES algorithm has been shown to be more efficient than its predecessors, such as Triple DES, and asymmetric algorithms like RSA. Tests show that AES can perform encryption with an average time of 12 ms, significantly faster than RSA, which can take up to 98 ms. This makes it an ideal solution for public service systems requiring real-time responses (Aswandi et al., 2025). According to Stallings (2017), AES offers advantages not only in speed but also in resistance to various modern cryptanalysis attacks, making it highly suitable for use in critical government information systems.

Furthermore, according to Kaur & Sood (2019), the successful implementation of cryptography in public services also depends on sound key management and integration with strong authentication systems. These best practices ensure data remains secure during storage and transmission, while minimizing the risk of unauthorized access. Previous research has shown that combining AES with additional security protocols, such as TLS/SSL, can provide an effective double layer of protection for public service platforms (Singh et al., 2021).

Based on this background, this study aims to design a data security scheme in a public service system using the AES algorithm with a 128-bit key length (AES-128). The selection of the 128-bit variant is based on considerations of the balance between computational speed and adequate security strength to protect civil administrative data. This research will produce a data security architecture design that can be applied to mitigate the risk of data leakage on public service platforms, while also serving as a reference for the development of more secure and reliable e-government systems in the future.

METHOD

The method used in this research is the System Development Life Cycle (SDLC) with the waterfall model. This model was chosen because it uses a systematic and sequential approach to developing information systems (Wahid, 2020). As explained in the reference, the stages of the waterfall model include requirements, design, implementation, verification, and maintenance. The advantage of this method is that the resulting system tends to be of good quality because its implementation is carried out in stages. Given that the focus of this research is on data security aspects and not on developing a complete application, the research stages are limited to the requirements (needs analysis) and design (schematic design) stages, without delving into the full implementation of the program code.

The research stages are as follows:

1. Requirement Analysis. This stage aims to identify the types of sensitive data in public services that require confidentiality protection. The data that is the primary object of protection is Personally Identifiable Information (PII) of residents, such as National Identification Numbers (NIK) and Full Names. Furthermore, this stage defines non-functional performance requirements, where the cryptographic system must have low latency so that the encryption-decryption process does not

overload the server when handling large data queues. This need for speed is the primary basis for selecting the algorithm type.

2. Literature Review: This stage gathers theoretical references regarding the performance of cryptographic algorithms. The study focuses on a comparative analysis of the symmetric AES-128 algorithm and the standard asymmetric RSA-2048 algorithm. The goal is to empirically demonstrate that the symmetric algorithm is significantly more efficient in terms of data processing speed (computational speed) than the asymmetric algorithm, making it more suitable for public service systems with high transaction volumes.

3. Cryptographic Scheme Design: This stage is the core of the research, where the security system logic flow is designed. The design includes creating a flowchart of the encryption process when users send data (input) and the decryption process when administrators access data (retrieval). The design also includes key management to ensure encryption keys are stored separately from the main database.

4. Simulation and Analysis: The final stage involves conducting manual simulation calculations using dummy data samples. This simulation aims to validate that the input data (plaintext) can be converted into a scrambled format (ciphertext) using the specified key and can be restored to its original form perfectly. Security analysis is also performed to ensure the designed scheme is resistant to basic attack patterns.

RESULTS AND DISCCUSION

Comparative Analysis of Algorithm Performance

The initial stage in designing this security system was determining the most efficient cryptographic algorithm for handling public service data traffic. Based on a literature review comparing the performance of symmetric (AES-128) and asymmetric (RSA-2048) algorithms, significant differences in processing speed (computational time) were found.Table 1 below presents the results of encryption and decryption time tests based on varying data sizes (bytes), as cited in research (Ananda et al., 2025).

Table 1. Comparison of Processing Time of AES-128 vs RSA-2048

Data Size (Byte)	Algorithm	Encryption Time (ms)	Decryption Time (ms)
50	AES-128	0.0217	0.0334
50	RSA-2048	0.7815	1.9138
100	AES-128	0.0143	0.0131
100	RSA-2048	0.7632	2.4004
150	AES-128	0.0138	0.0138
150	RSA-2048	0.8228	2.0711
200	AES-128	0.0165	0.0145
200	RSA-2048	0.7505	2.2495

Based on the data in Table 1, it is clear that AES-128 has a drastic performance advantage over RSA.

- Encryption Speed: For a data size of 50 bytes (the same size as the National ID and Name data), AES only takes 0.0217 milliseconds, while RSA takes 0.7815 milliseconds. This means AES is approximately 36 times faster at locking data.

- Decryption Speed: The performance gap becomes even more pronounced in the decryption process, where RSA takes up to 1.9-2.4 milliseconds, while AES remains stable at 0.01-0.03 milliseconds.

The implications of these findings are crucial for public service systems. Using RSA, the accumulated latency when thousands of citizens simultaneously access the queue will cause server overload. Therefore, using AES-128 is a crucial design decision to ensure data security without sacrificing service speed.

Encryption Scheme Design

Based on the performance analysis results above, a data security scheme was designed that integrates the AES-128 algorithm into the public service data storage flow. The main principle of this design is data segregation, where the system distinguishes between public data (such as queue numbers), which are not encrypted, and private data (such as National Identification Numbers and Names), which require encryption.

The logical flow of the proposed data security process can be seen in Figure 1 below:

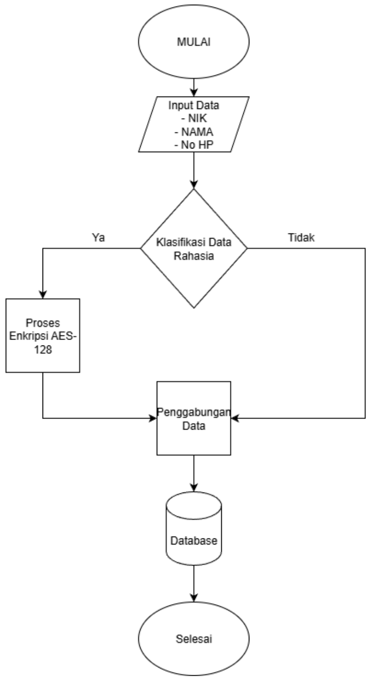

Figure 1. Flowchart of Data Encryption Process Flow

In the above scheme, the encryption process is designed using the Cipher Block Chaining (CBC) operating mode. The use of CBC mode aims to increase security entropy, where each encrypted data block is dependent on the previous block. This ensures that if two residents share the same name, the resulting ciphertext will remain distinct and random, preventing unauthorized parties from analyzing the data pattern. Encryption keys are managed through a separate storage mechanism (key storage) accessible only by the system's authorization module, mitigating the risk of server hacking.

Data Encryption Simulation

To validate the designed scheme, an encryption simulation was conducted using synthetic data samples (dummy data). This simulation was run using the AES-128 algorithm with the CBC operating mode, which adheres to the standard (National Institute of Standards and Technology, 2023). The goal was to verify that plaintext could be converted to ciphertext according to applicable technical specifications.

Table 2 below displays the simulation results for data transformation on sensitive resident attributes.

Table 2. Data Encryption Simulation Results

Atribute	Plaintext	Key enkripsi	Ciphertext (Data Stored in Database)
National Identification Number	3201123456780001	KuncirahasiaKRPT	cMJnszI70r+b2Zz7jU7u4oTvj9nTPm6hHIXO/1CDJsg=
Full Name	Eko Nurcahyo	KuncirahasiaKRPT	7bblUhMT9lgjrAzH2KQA3w==
Telephone Number	082154338766	KuncirahasiaKRPT	1NKUGxZXr9epZxbXx/wdWw==

Based on Table 2, it can be seen that the NIK data, which was originally in the form of the number 3201..., has been successfully converted into a random character sequence cMJnszI7.... In cryptographic principles, this indicates the success of the confusion and diffusion process. Unauthorized parties (such as hackers or rogue admins) will only see gibberish data in the database. Without a valid decryption key (KuncirahasiaKRPT), the data is computationally impossible to return to its original form within a reasonable time, thus ensuring the security of public privacy data.

CONCLUSION

Based on the analysis and design results, it can be concluded that implementing the AES-128 cryptographic algorithm is the right solution for securing data in digital public service systems.

1. In terms of performance, the comparative study results show that AES-128 has a much more efficient encryption-decryption process speed (average 0.02 ms) than asymmetric algorithms such as RSA (0.78 ms). This efficiency is crucial for preventing bottlenecks or data queues on public service servers with high traffic.
2. In terms of security, the proposed scheme has proven effective in protecting the confidentiality of sensitive citizen data (NIK and Name) by converting it into a random format (ciphertext) that cannot be read without a valid key.

This study recommends that government agencies immediately implement the AES-128 encryption standard in their database layers as a preventative measure against the threat of data breaches.

REFERENCE

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional, 6*(2). https://doi.org/10.7454/jkskn.v6i2.10082

Ananda, S., Rusydi, I., Faruqi, M., Ramadhan, M. W., Syahrin, M. N. A., Prayugo, R. P., & Ihsan, M. (2025). Analisis perbandingan algoritma kriptografi AES dan RSA terhadap keamanan dan waktu proses enkripsi data teks: Comparative analysis of AES and RSA cryptographic algorithms on security and processing time of text data encryption. https://jicnusantara.com/index.php/jicn

Arif, Z., & Nurokhman, A. (2023). Analisis perbandingan algoritma kriptografi simetris dan asimetris dalam meningkatkan keamanan sistem informasi: Comparative analysis of symmetric and asymmetric cryptographic algorithms in improving information system security. In *JTSI, 4*(2).

Aswandi, A. S., Nurtanzis Sutoyo, M., & Pradipta, A. (2025). Analisis performa dan keamanan implementasi kriptografi AES untuk penyandian dokumen berbasis web, *8*(1).

Heeks, R. (2020). *Implementing and managing e-government: A global perspective*. Routledge.

Kapoor, B., Pandya, P., & Sherif, J. S. (2011). Cryptography: A security pillar of privacy, integrity and authenticity of data communication. *Kybernetes, 40*(9), 1422–1439. https://doi.org/10.1108/03684921111169468

Kaur, G., & Sood, M. (2019). Cryptography and key management in digital government services: Best practices and challenges. *International Journal of Network Security, 21*(3), 211–223.

National Institute of Standards and Technology. (2023). *Advanced Encryption Standard (AES)*. https://doi.org/10.6028/NIST.FIPS.197-upd1

Singh, P., Sharma, R., & Verma, K. (2021). Securing e-government platforms using AES and TLS protocols. *Journal of Cybersecurity and Digital Trust, 5*(4), 78–92.

Sisilianingsih, S., Purwandari, B., Eitiveni, I., Purwaningsih, M., & Korespondensi, P. (2023). Analisis faktor transformasi digital pelayanan publik pemerintah di era pandemi. https://doi.org/10.25126/jtiik2023107059

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

Wahid, A. A. (2020). Jurnal ilmu-ilmu informatika dan manajemen STMIK Oktober (2020): Analisis metode waterfall untuk pengembangan sistem informasi.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.