Jurnal Multidisiplin Sahombu
E-ISSN : 2809-8587

A Comparative Analysis of the Advanced Encryption Standard (AES) 128-, 192-, and 256-Bit Algorithms in Digital Data Security

Putra Daffa Dwiyansah[1], Fiqri Fathurrohman[2], Nakhwah Alfikry[3], Jefry Sunupurwa Asri[4]

[1,2,3,4] Universitas Esa Unggul

ARTICLE INFO

Keywords:
Algorithm, Advanced Encryption Standard (AES), Digital Security

ABSTRACT

Data security is a crucial aspect of modern information systems as digital data exchange via the internet increases. One widely used solution to protect data confidentiality and integrity is the Advanced Encryption Standard (AES) cryptographic algorithm, which has three main variants based on key length: AES-128, AES-192, and AES-256. This study aims to analyze and compare the security characteristics and performance of these three AES variants based on a literature review of five relevant national journals. The research method used is a literature review with an analysis and synthesis approach to previous research results. The results show a consistent trade-off between security level and computational efficiency. AES-128 excels in speed and resource efficiency, making it suitable for devices with computing limitations. AES-192 offers a balance between performance and security, while AES-256 provides the highest level of security at the expense of increased processing time and resource usage. The conclusion of this study emphasizes that the selection of an AES variant must be tailored to system requirements and data sensitivity levels, and opens up opportunities for further research related to optimizing AES implementation, particularly in modern web application environments.

Email:
ptradaffa45@student.esaunggul.ac.id,
fiqrifaturrohman36@student.esaunggul.ac.id,
nakwahalfikry@student.esaunggul.ac.id
, jefry.sunupurwa@esaunggul.ac.id

INTRODUCTION

Data security is a fundamental aspect of modern information system management. With the rapid development of digital technology, data exchange via the internet has become increasingly widespread, both in business and government contexts, as well as in personal communications. This situation indirectly increases the risk of data leaks, manipulation, and theft by unauthorized parties. Therefore, there is a need for a security system capable of ensuring data confidentiality and integrity from external threats. In this context, cryptography is one of the most important and relevant solutions for securing information in the digital world (Wachid Hidayatulloh et al., 2023).

Cryptography plays a role in converting original data (plaintext) into a coded form (ciphertext) through an encryption process, so that the message can only be restored to its original form by those possessing the decryption key. Thus, cryptography not only maintains data confidentiality but also ensures integrity and authentication in electronic communications. Various cryptographic

algorithms have been developed to meet data security needs, ranging from classic algorithms such as DES (Data Encryption Standard) to modern algorithms such as AES (Advanced Encryption Standard), which is currently the global standard (Wachid Hidayatulloh et al., 2023).

AES was developed by Vincent Rijmen and Joan Daemen, initially known as Rijndael, and was later approved as an encryption standard by the National Institute of Standards and Technology (NIST) in 2001. AES was designed to replace DES, which was no longer considered secure against brute-force attacks. This algorithm uses a 128-bit block structure with three main variants based on key length: AES-128, AES-192, and AES-256, where the number indicates the key length in bits (128, 192, and 256). Each variant has a different number of encryption rounds: AES-128 has 10 rounds, AES-192 has 12 rounds, and AES-256 has 14 rounds (Tampubolon, Isnanto, & Sinuraya, 2014).

Research in Indonesia demonstrates various implementations and analyses of AES in the context of digital data security. Kusyanti & Amron (2018) examined the application of AES to an Android-based Short Message Service (SMS) encryption system and found that AES-128 performed the fastest. Santoso & Rahman (2022) developed an Android-based document encryption application using AES-128 and demonstrated that this algorithm is highly efficient for mobile devices with limited resources. Meanwhile, research conducted by Indrayani, Ferdiansyah, & Koprawi (2025) demonstrated the superiority of AES-256 in maintaining the integrity of various digital file types such as text, images, and videos, although the encryption time required was relatively longer than other variants.

In general, the results of these studies indicate a trade-off between security and computational efficiency among the three AES variants. AES-128 excels in terms of speed and efficiency, AES-192 provides a balance between speed and encryption strength, while AES-256 offers the highest security but at the expense of increased processing time.

The purpose of this literature review is to analyze and compare the performance and security of the three AES variants, while identifying their advantages, disadvantages, and potential applications in modern information systems. This study is expected to provide a more comprehensive understanding of the relationship between key length, number of rounds, and algorithm efficiency, thus providing a guideline for selecting an AES variant that best suits the needs and characteristics of a particular application.

METHOD

This research employed a literature review with a descriptive-analytical approach and qualitative synthesis. Literature review was chosen because it provides a comprehensive understanding of conceptual developments, empirical findings, and research trends in a specific field. According to Creswell (2014), literature review serves to integrate and evaluate previous research findings to build a strong theoretical foundation relevant to the topic being studied.

The descriptive-analytical approach is used to systematically describe the characteristics, methods, and results of previous research, while qualitative synthesis aims to combine various findings into meaningful conclusions. Hart (2018) explains that synthesis in literature review not only summarizes previous research but also interprets, compares, and relates research results to discover patterns and conceptual relationships.

The research phase began with the collection of literature sources in the form of national journals discussing the Advanced Encryption Standard (AES) algorithm and its application in digital

data security. Journal selection criteria included topic relevance, a focus on AES-128, AES-192, and AES-256 variants, and a relationship to system performance and security aspects. This selection process aligns with Kitchenham & Charters (2007), who emphasize the importance of clear inclusion and exclusion criteria in literature reviews to ensure systematic and scientifically sound analysis.

Five selected national journals were then analyzed in depth to identify the research objectives, methods used, implementation context, and reported test results. The analysis was conducted comparatively, focusing on key length, number of encryption rounds, processing time, resource efficiency, and resulting security level. According to Webster & Watson (2002), comparative analysis in a literature review is crucial for uncovering similarities, differences, and understudied research gaps.

Next, a synthesis process was conducted to identify common patterns, similarities, and differences in findings across studies. This process aims to produce a more integrated understanding of the relationship between AES key length, security level, and computational efficiency. Snyder (2019) states that a sound literature synthesis can provide new conceptual contributions and serve as a strong foundation for further research. The final results of this analysis and synthesis process are used to formulate conclusions regarding the characteristics of each AES variant and their potential applications in modern information systems.

RESULTS AND DISCCUSION

RESULTS

Hidayatulloh et al. (2023) — Understanding Advanced Encryption Standard (AES) as a Cryptographic Algorithm for Securing Data, Journal of Digital Transformation Technology (Digitech)

Research conducted by Wachid Hidayatulloh et al. (2023) focuses on the introduction and conceptual analysis of the Advanced Encryption Standard (AES) algorithm as one of the most widely used modern cryptographic methods. This study comprehensively explains the internal structure of AES, consisting of four main processes: SubBytes, ShiftRows, MixColumns, and AddRoundKey, and how these mechanisms create a multi-layered, impenetrable security layer.

The authors assert that AES is superior to previous algorithms such as DES (Data Encryption Standard), both in terms of efficiency and resistance to brute-force attacks. With its very large key space and mathematical complexity based on substitution and permutation, AES is categorized as a secure algorithm for use in modern systems such as IoT, encrypted databases, and cloud services.

However, this research is theoretical in nature and does not yet include empirical analysis of encryption time performance or resource consumption. Nevertheless, Hidayatulloh et al. (2023) provide a strong foundation for understanding the working mechanism of AES and the importance of key length selection (128, 192, and 256 bits) in determining system security.

Kusyanti & Amron (2018) — Comparative Analysis of Advanced Encryption Standard Algorithms for Short Message Service (SMS) Encryption on Android, Journal of Information Technology and Computer Science Development (J-PTIIK), Brawijaya University

Research conducted by Kusyanti and Amron (2018) explicitly compared the performance of three AES variants: AES-128, AES-192, and AES-256, in the context of short message (SMS)

encryption on the Android platform. The main focus of this study was to measure encryption and decryption times and the level of memory efficiency on mobile devices with limited specifications.

Test results show that AES-128 has the fastest and most efficient execution time due to the fewer rounds (10) compared to AES-192 (12 rounds) and AES-256 (14 rounds). Meanwhile, AES-256 provides the highest level of security, with complexity increasing with key length, but requires up to 25–30% longer processing time than AES-128.

This study also emphasizes that the choice of AES variant must be tailored to the system's needs. For mobile applications requiring high efficiency, AES-128 is the ideal choice, while for systems with high security requirements such as banking or confidential communications, AES-256 is preferred (Kusyanti & Amron, 2018).

Santoso & Rahman (2022) — Analysis and Design of an Android-Based Document Encryption and Decryption System Using the Advanced Encryption Standard – 128 Method, Jurnal Logika Media Teknologi (JLMT)

Research conducted by Teguh Budi Santoso and Fildan Hadika Rahman (2022) focuses on the development of an Android-based document encryption and decryption system using AES-128. The goal of this research is to ensure the security of digital documents without compromising mobile device performance.

Test results show that AES-128 is capable of encrypting various types of document files quickly and efficiently without altering the structure or size of the original files after decryption. In terms of memory and power consumption, this algorithm is considered very lightweight and stable for application on low- to mid-range devices.

However, this study did not directly compare AES-192 and AES-256, so the primary focus remains on the efficiency of AES-128. Nevertheless, Santoso & Rahman (2022) concluded that AES-128 is the most practical variant for encryption implementation on mobile systems that require high speed and stability.

Tampubolon et al. (2014) — Implementation and Analysis of the Advanced Encryption Standard (AES) Algorithm on Three Key Length Variations for Multimedia Files

The study by Tampubolon, Isnanto, and Sinuraya (2014) aimed to implement and compare the performance of AES-128, AES-192, and AES-256 in the encryption process for multimedia files, including video, images, and text. Testing was conducted by measuring the encryption and decryption speeds and security levels of each variant.

Experimental results showed that AES-128 had the fastest processing time and lowest CPU consumption, while AES-256 required longer computation time but offered a significantly higher level of security. AES-192 fell in the middle, balancing performance and security.

This study also highlighted that increasing the number of encryption rounds directly increases the level of security, but decreases time efficiency. Therefore, Tampubolon et al. (2014) emphasized the importance of balancing performance and security when selecting an AES variant and recommended the use of AES hardware acceleration as a future optimization solution.

Indrayani, Ferdiansyah, & Koprawi (2025) — Analysis of the Use of AES-256 Bit Cryptography Methods for Securing Files in Various Formats, Digital Transformation Technology, 4(2)

Recent research by Indrayani, Ferdiansyah, and Koprawi (2025) examined the application of AES-256 to secure digital files in various formats, such as text, images, audio, and video. The main focus of this research was to evaluate the effectiveness of AES-256 in maintaining integrity, file size consistency, and resistance to data modification.

The results showed that AES-256 was able to maintain the intact data structure after decryption without losing file quality. However, encryption and decryption times were longer than AES-128 and AES-192, especially for large files.

The authors emphasized that AES-256 is ideal for systems that require high levels of security, such as sensitive data storage in the cloud, government systems, and financial applications. However, for systems with limited resources, algorithm optimization is necessary to avoid performance overhead (Indrayani et al., 2025).

DISCUSSION

Analysis and Synthesis

From the five studies reviewed, a consistent pattern emerges in the relationship between AES key length, security level, and processing efficiency. In general, the longer the key used, the significantly increased security level, but also the longer the encryption and decryption time.

First, AES-128 is considered the most computationally efficient because it uses only 10 rounds of encryption. Research by Santoso & Rahman (2022) shows that AES-128 is capable of delivering high speeds with minimal resource consumption, making it an ideal choice for mobile devices or real-time applications. Similar results were confirmed by Kusyanti & Amron (2018), who found that AES-128 had the fastest execution time compared to AES-192 and AES-256 in tests on the Android platform. However, its main weakness is its smaller key space compared to AES-256, making it less optimal for resisting attacks with high computational power in the long term.

Second, AES-192 occupies a middle ground in terms of performance and security. As explained by Kusyanti & Amron (2018) and Tampubolon, Isnanto, & Sinuraya (2014), AES-192 provides a better level of security than AES-128 without significantly decreasing performance. However, this variant is rarely used in real-world implementations because its differences from AES-256 are insignificant, while the processing overhead remains high.

Third, AES-256 provides the highest level of security due to its 14 rounds and large key length. Research by Indrayani, Ferdiansyah, & Koprawi (2025) shows that AES-256 is effective in maintaining data integrity even across large files and various formats, making it well-suited for systems with high security requirements such as database encryption, cloud storage, and government communications. However, this research also emphasizes that increased security comes at the cost of longer processing times and greater resource consumption.

Furthermore, several studies highlight that AES performance is significantly affected by hardware specifications and the size of the data being processed. Kusyanti & Amron (2018) note that on devices with low processors, the time difference between AES-128 and AES-256 can reach several seconds per file. In contrast, Tampubolon et al. (2014) explained that modern devices supporting AES-NI (Advanced Encryption Standard New Instructions) can significantly minimize this time difference.

Several research gaps that remain open for further study include:

- Limited research on energy consumption and memory usage of each AES variant across various platforms.

• Few studies have examined the effect of hardware acceleration (such as AES-NI or GPU encryption) on the efficiency of the three variants.
• Lack of analysis of the resilience of AES implementations to practical attacks such as side-channel attacks and timing attacks.

Overall, the synthesis results show that AES remains the most relevant and robust symmetric cryptography algorithm to date, with each variant having its own advantages depending on the context of use.
• AES-128 excels in efficiency,
• AES-192 offers balance and performance.
• AES-256 excels in long-term security strength.

Research Directions and Opportunities

Based on the results of a literature review of various previous studies, it can be identified that each AES variant has different performance and security characteristics, and there is no implementation standard that specifically optimizes its use on modern web platforms. Therefore, future research can focus on the adaptive implementation of the AES algorithm, particularly AES-256, in framework-based web application environments such as Laravel and Filament.

Future research is expected to not only test the encryption and decryption capabilities of AES in the context of data security, but also assess its impact on system performance, computational efficiency, and energy consumption. Several important aspects that can be focused on in further research development include:

1. Analysis of AES-256 performance on encryption speed and server load.

Testing is needed to determine the extent to which AES-256 implementation affects web application response times, especially under high user load conditions. This is important because AES-256 has the highest number of encryption rounds (14 rounds), which theoretically can significantly improve processing time compared to AES-128 and AES-192.

2. Implementation of field-level encryption in a Laravel database.

This approach allows each sensitive column in a database table (such as personal data, addresses, or ID numbers) to be encrypted using AES-256 before being stored, then decrypted only when needed. This makes the system more resilient to data leaks caused by direct database access. Further research can evaluate the efficiency of this technique compared to middleware-based global encryption.

3. Comparison of the efficiency of three AES variants (128, 192, and 256) in the context of web applications.

Although AES-256 theoretically offers the highest security, not all web applications require that level of security. Therefore, empirical testing is necessary to compare encryption time, CPU usage, throughput, and memory consumption of the three variants on servers with different specifications.

4. Measurement of additional parameters such as CPU usage, throughput, and energy consumption.

Energy consumption is a critical factor, especially for cloud-based and edge computing systems. Future research can analyze the relationship between AES key size and energy efficiency to determine which variant is most optimal in the context of green computing.

Furthermore, research can be expanded by integrating AES with additional security algorithms, such as steganography or digital signatures, to create a double layer of security. This aligns with research by Santoso & Rahman (2022), which emphasizes the importance of efficiency in mobile systems, and the findings of Indrayani, Ferdiansyah, & Koprawi (2025), which demonstrate the importance of high levels of security in cloud-based file storage systems.

With this approach, further research is expected to make a significant empirical contribution to the development of AES-based data security in modern web application environments, while also serving as a technical reference for implementing security based on software frameworks such as Laravel, Django, or Node.js.

CONCLUSION

Based on a review of five national journals, it can be concluded that the AES algorithm has three main variants: AES-128, AES-192, and AES-256. Each has distinct security and performance characteristics, requiring its use to be tailored to system requirements. AES-128 excels in processing speed and resource efficiency, making it highly suitable for systems with computing constraints, such as mobile devices and real-time applications. Research shows that this variant is capable of fast encryption and decryption, maintains file structure, and requires relatively little memory, making it effective for Android-based environments and other lightweight systems.

AES-192 occupies a middle ground, offering a balance between performance and security. This variant provides stronger protection than AES-128 without significantly increasing processing time. However, AES-192 is relatively rarely used in practice because its security improvements are not significant compared to AES-256, while processing complexity remains. Therefore, many implementations simply choose AES-256 for high-security applications.

AES-256 is the variant with the highest level of security because it uses a 256-bit key length and 14 rounds of encryption. The results show that AES-256 is highly effective in maintaining data integrity in various file formats such as text, images, audio, and video without compromising the quality of the decrypted results. However, this superior security comes at the cost of longer encryption and decryption times and higher processor resource consumption, especially on devices with limited computing capabilities.

Overall, the analyzed literature shows a consistent trade-off between security and performance across the three AES variants. AES-128 emphasizes efficiency and speed, AES-192 offers a balance between security and performance, while AES-256 focuses on long-term security strength. These differences in characteristics emphasize that the selection of an AES variant must consider the specific needs of the system and the sensitivity of the data being protected. This study also opens up opportunities for further research, particularly in optimizing AES-256 implementations in modern web frameworks, comparative testing of time efficiency and resource consumption across various server specifications, and integrating AES with additional security mechanisms to improve performance without compromising security.

REFERENCE

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage Publications.

Hart, C. (2018). *Doing a literature review: Releasing the research imagination* (2nd ed.). London: Sage Publications.

Hidayatulloh, N. W., Tahir, M., Amalia, H., Basyar, N. A., Prianggara, A. F., & Yasin, M. (2023). Mengenal *Advanced Encryption Standard* (AES) sebagai algoritma kriptografi dalam mengamankan data. *Digital Transformation Technology (Digitech)*, 3(1), 1–10. https://jurnal.itscience.org/index.php/digitech/article/view/2293

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://jurnal.itscience.org/index.php/digitech/article/view/5457

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. EBSE Technical Report, EBSE-2007-01.

Kusyanti, A., & Amron, K. (2018). Analisis perbandingan algoritma *Advanced Encryption Standard* untuk enkripsi *Short Message Service* (SMS) pada Android. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2(10), 4281–4289. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2893/1112

Santoso, T. B., & Rahman, F. H. (2022). Analisa dan perancangan sistem enkripsi dan dekripsi dokumen berbasis Android menggunakan metode *Advanced Encryption Standard*–128 (Studi kasus: PT. Kelab 21 Retail). *Jurnal Logika dan Manajemen Teknologi (JLMT)*, 2(1), 45–53. https://ojs-teknik.usni.ac.id/index.php/jlmt/article/view/197

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.

Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W. (2014). Implementasi dan analisis algoritma *Advanced Encryption Standard* (AES) pada tiga variasi panjang kunci untuk berkas multimedia. *Jurnal Transient*, 3(4), 567–574. https://ejournal3.undip.ac.id/index.php/transient/article/view/10581

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), xiii–xxiii.