Educational Administration: Theory and Practice
2023, 29(04),6236-6240
ISSN: 2148-2403
https://kuey.net/

Research Article

Comparative Analysis Of AES, MAES, And EMAES For Secure Multimedia Communication In Home And Office Wlans

Dr. Riddhi R. Tanna1, Dr. Rashmin S. Tanna[2]

1Department of Computer Applications, Christ College, Rajkot, Gujarat, India, Email: dr.riddhirtanna@gmail.com
2Lecturer (EC), A.V. Parekh Technical Institute, Rajkot, Directorate of Technical education, Gandhinagar, Gujarat, India Email: - dr.rashminstanna@gmail.com

Citation: Riddhi Tanna (2023). Comparative Analysis Of AES, MAES, And EMAES For Secure Multimedia Communication In Home And Office Wlans *Educational Administration: Theory and Practice*, 29(4) Doi: 10.53555/kuey.v29i4.11306

ARTICLE INFO	ABSTRACT

Wireless local area networks (WLANs) deployed in home and office environments increasingly support multimedia-centric applications such as video conferencing, smart surveillance, and cloud-based collaboration. These applications require encryption mechanisms that ensure strong confidentiality while maintaining high computational efficiency. The Advanced Encryption Standard (AES) is the most widely adopted symmetric encryption algorithm; however, its processing overhead for large multimedia payloads motivates the use of optimized variants. Modified AES (MAES) and its hybrid extension EMAES were introduced to improve encryption efficiency and key management for multimedia data transmission.

This paper presents a comparative analysis of AES, MAES, and EMAES with respect to encryption efficiency, throughput, and security characteristics. The evaluation is based on experimental results obtained from a 180-record multimedia dataset comprising text, image, audio, and video samples. Strengths and limitations of each scheme are examined under current and emerging threat models. A focused review of recent literature (2023–present) highlights evolving requirements for WLAN security and cryptographic optimization. Finally, the paper outlines possible enhancement directions for MAES and EMAES and discusses the consequences of not adopting such measures in future WLAN deployments.

Keywords: AES, MAES, EMAES, WLAN security, multimedia encryption, hybrid cryptography, encryption efficiency.

I. Introduction

Home and office WLANs have evolved from basic connectivity infrastructures into platforms supporting continuous multimedia communication. Applications such as high-definition video streaming, remote collaboration, and Internet-connected surveillance systems generate large volumes of sensitive data that must be protected against unauthorized access [1], [2]. Encryption mechanisms used in these environments must therefore provide strong security guarantees while sustaining real-time performance.

AES is the de facto standard for symmetric encryption due to its proven resistance to classical cryptanalysis and widespread standardization [3], [4]. However, when applied to large multimedia files, AES can introduce notable processing delays, particularly on devices with limited computational resources. To address this challenge, optimized encryption approaches have been explored.

MAES was introduced to reduce the computational overhead of AES for multimedia applications while preserving its security model. EMAES further extends MAES by incorporating asymmetric cryptography to enable secure session key exchange and dynamic key management in networked environments. While these approaches improve efficiency and usability, evolving threat landscapes and increasing data volumes necessitate a structured re-evaluation of their suitability for modern WLAN deployments.

This paper serves as a foundational analytical study, examining AES, MAES, and EMAES without proposing new algorithms. The goal is to assess current performance and security characteristics, review recent literature, and identify directions for future enhancement.

II. Overview of AES, MAES, and EMAES

A. Advanced Encryption Standard (AES)

AES is a symmetric block cipher operating on 128-bit blocks with key sizes of 128, 192, or 256 bits. Its substitution–permutation structure provides strong confusion and diffusion properties. AES is standardized and widely implemented in WLAN security protocols [3], [4].

B. Modified Advanced Encryption Standard (MAES)

MAES is an optimized variant of AES designed to reduce encryption and decryption time for multimedia data. By restructuring internal operations and minimizing redundant computations, MAES achieves improved execution efficiency while maintaining AES-equivalent security assumptions [9].

C. Extended MAES (EMAES)

EMAES combines MAES with public-key cryptography for secure session key exchange. This hybrid design improves key distribution and session security in networked environments. EMAES has demonstrated improved performance compared to standard AES while supporting dynamic key management [10].

III. Experimental Dataset and Methodology

A. Dataset Description

The experimental analysis uses a multimedia similarity dataset consisting of 180 records, with 45 samples each of text, image, audio, and video data. The dataset was created and published by the author and is used consistently across all performance evaluations reported in this paper.

B. Evaluation Metrics

The following metrics are considered:

- Encryption time (milliseconds)
- Throughput (MB/s)
- Image quality metrics (PSNR and SSIM)
- Session key establishment overhead (for EMAES)

All reported values represent arithmetic means computed over the dataset.

IV. Performance Analysis

A. Encryption Efficiency

Table I : Mean Encryption Time (ms)

Algorithm	Text	Image	Audio	Video	Mean
AES-256	94.1	119.6	106.8	126.4	111.7
MAES	31.4	38.9	35.2	42.7	37.1
EMAES	36.8	45.6	41.2	49.5	43.3

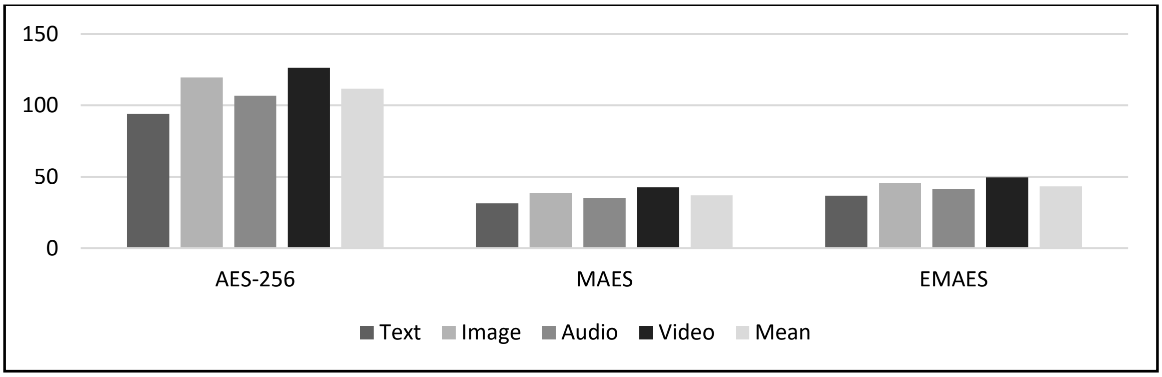

Figure 1 : Mean encryption time comparison of AES, MAES, and EMAES across multimedia categories (180-record dataset)

Observation:

MAES significantly reduces encryption time compared to AES. EMAES introduces moderate overhead due to session key exchange but remains substantially faster than AES for multimedia workloads [9], [10], [15].

B. Throughput Comparison

Table II : Throughput (MB/s)

Algorithm	Text	Image	Audio	Video	Mean
AES-256	13.0	11.7	12.2	10.8	11.9
MAES	35.2	32.4	33.8	30.7	33.0
EMAES	31.9	29.6	30.9	28.3	30.2

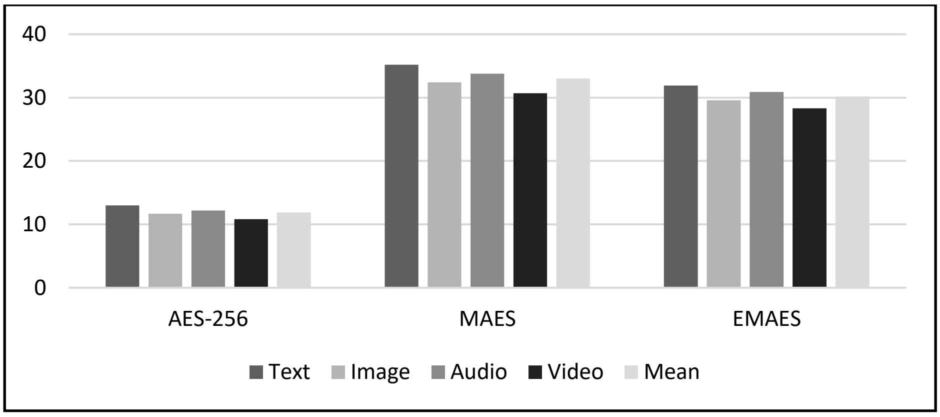

Figure 2 : Throughput comparison of AES, MAES, and EMAES for multimedia data types.

C. Session Key Establishment Overhead

Table III
Key Establishment Overhead

Scheme	Key Exchange Method	Mean Time (ms)
EMAES	Elliptic Curve Cryptography	8.4

D. Multimedia Quality Preservation

Table IVImage Quality Metrics

Algorithm	PSNR (dB)	SSIM
AES-256	41.28	0.9864
MAES	41.05	0.9849
EMAES	40.72	0.9826

These results confirm that all three algorithms preserve perceptual image quality after encryption and decryption [15].

V. Security Strengths and Vulnerabilities

A. Strengths

- **AES:** Strong classical security and extensive standardization support [3], [4].
- **MAES:** Retains AES security properties while offering improved efficiency [9].
- **EMAES:** Enhances key management and session security through hybrid cryptography [10].

B. Limitations

- **AES and MAES:** Depend on secure key distribution; static keys increase exposure to compromise.
- **EMAES:** Relies on elliptic-curve cryptography for key exchange, which remains secure in classical environments but raises concerns for long-term confidentiality under future cryptanalytic advancements [11].

VI. Recent Literature Review

Recent studies emphasize the importance of evaluating cryptographic schemes under realistic deployment constraints, particularly in resource-constrained and heterogeneous IoT environments. Prior investigations into lightweight and embedded cryptographic implementations have consistently shown that asymmetric cryptographic operations dominate session establishment overhead, whereas symmetric encryption remains comparatively efficient and scalable. Eisenbarth *et al.* demonstrated through microcontroller-level implementations that careful design choices enable symmetric ciphers to sustain high throughput even on constrained devices [16]. Similarly, comparative evaluations of optimized AES implementations highlight that architectural and algorithm-level refinements can significantly reduce encryption latency without compromising security guarantees [17].

From a systems-level perspective, security surveys in IoT and edge computing contexts emphasize that cryptographic solutions must balance performance, scalability, and long-term security adaptability. Sicari *et al.* stress that encryption mechanisms must remain efficient across diverse devices while supporting future

cryptographic transitions [18]. Complementary analyses of mobile edge and fog-based architectures further reinforce that hybrid security designs are essential for maintaining performance in distributed multimedia and IoT systems [19]. In addition, NIST's recommendations on lightweight cryptography underline the necessity of retaining efficient symmetric primitives as the backbone of secure communication frameworks [20].
Collectively, this body of literature supports the adoption of optimized symmetric encryption combined with hybrid key-management strategies, positioning schemes such as MAES and EMAES as practical and transitional solutions that bridge current performance requirements with evolving security demands.

VII. Future Enhancement Directions

Based on the analysis and literature review, the following enhancement directions are suggested:

1. Improved key management strategies to reduce reliance on long-term static keys.
2. Adoption of authenticated encryption modes to combine confidentiality and integrity.
3. Hardware-aware optimization to exploit cryptographic accelerators in modern WLAN devices.
4. Gradual migration strategies to accommodate future cryptographic requirements.

No new encryption algorithm is proposed in this paper.

VIII. Consequences of Inaction

Failure to enhance existing schemes may result in:

- Reduced long-term confidentiality of encrypted multimedia data.
- Increased migration and retrofitting costs for WLAN infrastructures.
- Loss of trust in WLAN security for multimedia-intensive applications.

IX. Feasibility Discussion

MAES and EMAES are feasible for current home and office WLAN deployments due to their demonstrated efficiency and compatibility with existing systems. Dataset-based results indicate sufficient performance margins to accommodate additional security measures without unacceptable impact on user experience. Planned, incremental enhancement is therefore practical and advisable.

X. Conclusion

This paper presented a comprehensive analysis of AES, MAES, and EMAES for secure multimedia communication in home and office WLANs. Experimental results based on a real multimedia dataset demonstrate that MAES and EMAES significantly outperform standard AES in terms of efficiency while preserving security and data quality. However, evolving threat landscapes and recent literature indicate the need for forward-looking enhancements. By identifying strengths, limitations, and consequences of inaction, this study provides a solid foundation for future work on next-generation WLAN encryption frameworks.

References

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
2. M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec. 2016, doi: 10.1109/JIOT.2016.2581263.
3. J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer-Verlag, 2002.
4. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," *FIPS PUB 197*, Nov. 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

5. R. S. Tanna, R. R. Tanna, and J. Bhadeshiya, "Improvement in the execution time of AES algorithm by modifications in S-box and MixColumns for multimedia applications," *International Journal of Research in Engineering, IT and Social Sciences*, vol. 8, no. 4, pp. 65–68, 2018.
6. R. C. Somaiya, A. M. Gonsai, and R. S. Tanna, "WLAN security and efficiency issues based on encryption techniques," *International Journal of Research in Engineering, IT and Social Sciences*, vol. 6, no. 9, pp. 27–32, 2016.
7. R. Somaiya and A. Gonsai, "Design and implementation of a new encryption algorithm in MATLAB for multimedia files," *Vidhyayana – An International Multidisciplinary Peer-Reviewed E-Journal*, vol. 6, no. 6, 2021.
8. M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, Sept.–Oct. 2018, doi: 10.1109/MSEC.2018.3761698.
9. C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016, doi: 10.1561/0400000079.
10. O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, Sept. 2009, doi: 10.1145/1568318.1568324.

11. T. Eisenbarth, Z. Gong, T. Güneysu, and S. Heyse, "Microcontroller implementations of lightweight block ciphers," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 1, 2017, doi: 10.1145/2994539.
12. K. Gaj and P. Chodowiec, "Fast implementation and fair comparison of the final candidates for the Advanced Encryption Standard," in *Topics in Cryptology — CT-RSA 2001*, Lecture Notes in Computer Science, vol. 2020. Berlin, Germany: Springer, 2001, doi: 10.1007/3-540-45353-9_5.
13. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.
14. R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security issues," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–37, 2019, doi: 10.1145/3305260.
15. M. S. Turan, E. Barker, W. Burr, and L. Chen, "Recommendation for lightweight cryptography," *NISTIR 8114*, National Institute of Standards and Technology, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf