Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

QEMAES: A Quantum-Resilient Hybrid Encryption Framework for High-Throughput Multimedia Communication in IoT and Satellite Networks

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

ARTICLE INFO
Received: 09 Nov 2024
Accepted: 27 Dec 2024

ABSTRACT
Multimedia communication is central to modern Internet of Things (IoT) and satellite systems and therefore requires encryption that balances computational efficiency and long-term security. Traditional symmetric ciphers such as AES provide strong confidentiality but can be expensive on large multimedia payloads. Previous work reduced symmetric encryption latency and combined optimized symmetric ciphers with classical public-key key exchange, but those hybrids rely on elliptic-curve cryptography (ECC) which is vulnerable to scalable quantum attacks. This paper introduces QEMAES, a hybrid encryption framework that integrates a high-performance, AES-derived symmetric core with a lattice-based key-encapsulation mechanism (KEM) to provide quantum-resilient session key establishment. We evaluate QEMAES on a multimedia similarity dataset of 180 records (45 text, 45 image, 45 audio, 45 video) [25]. Results show QEMAES preserves the high throughput of the optimized symmetric core while adding only modest key-exchange overhead and delivering post-quantum key security.

Keywords: Post-quantum cryptography, hybrid encryption, multimedia security, IoT, satellite networks, lattice KEM.

I. Introduction

The rapid uptake of multimedia services in IoT and satellite communications from remote sensing and telemetry to on-demand video streaming places stringent requirements on encryption throughput and latency [3], [7]. Symmetric block ciphers such as AES remain the default choice for bulk encryption because of their maturity and security pedigree [8]. However, for large multimedia payloads AES can become the dominant contributor to end-to-end latency on constrained devices or in streaming scenarios. This motivated research into low-latency AES variants and optimized implementations that preserve cryptographic strength while reducing computational cost [1], [2]. [14]

Hybrid encryption symmetric bulk encryption plus asymmetric key distribution helps combine throughput and secure key management [6]. EMAES demonstrated the practical benefits of using an optimized AES-derived core for multimedia encryption with elliptic curve key exchange to provide fresh session keys [9]. However, ECC and RSA are threatened by quantum algorithms (e.g., Shor's algorithm), motivating migration toward post-quantum primitives for any design intended to provide long-term security [4], [12], [13]. Lattice-based Key Encapsulation Mechanisms (KEMs), such as Kyber, are promising post-quantum candidates because they are based on assumptions (e.g., LWE/Module-LWE) believed resistant to known quantum attacks and have efficient software and hardware implementations [5], [15], [19].

This work proposes QEMAES, a hybrid encryption framework that replaces the ECC key exchange in EMAES with a lattice KEM, keeping the high-speed symmetric core intact. The contribution of this paper is empirical: we show that QEMAES attains strong post-quantum key security with only modest performance impact on multimedia encryption and decryption, using the real dataset referenced above [25].

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

II. Related Work

A. AES performance and multimedia encryption

Performance-oriented AES variants and implementation techniques (S-box optimization, Mix Columns rearrangements, and pipeline/VLSI accelerations) have been extensively explored to reduce latency in embedded and streaming contexts [8], [14], [16]. These works motivate using an optimized symmetric core for multimedia use cases where throughput is critical.

B. Hybrid encryption frameworks

Combining symmetric encryption for bulk data and asymmetric techniques for key management has been commonly used in practice. EMAES and related hybrid proposals applied optimized symmetric cores together with ECC key exchange to achieve secure, low-latency multimedia encryption [3], [17], [10]. These frameworks are effective in classical settings but must be re-examined for post-quantum safety.

C. Post-quantum cryptography and lattice KEMs

Lattice-based cryptography and module/LWE-based KEMs in particular has been the focus of NIST's PQC standardization efforts and a number of performance studies. Kyber-family KEMs deliver attractive trade-offs between security, ciphertext size, and computational cost, making them good candidates for IoT and edge deployments [5], [15], [18], [21]. Prior analyses discuss the engineering implications for constrained devices and satellite systems [11], [13], [22].

III. QEMAES Framework Design

A. Threat model

We assume adversaries capable of passive eavesdropping and active network attacks, as well as adversaries equipped with scalable quantum computers able to run polynomial-time quantum algorithms against classical public-key assumptions (i.e., Shor's). Side-channel and physical attacks are out of scope.

B. Key establishment: lattice KEM

QEMAES replaces ECC with a module-LWE KEM for session key establishment. Each endpoint possesses a long-term public/private KEM key pair. To initiate a session, the sender encapsulates a random session key using the receiver's public KEM key and transmits the encapsulated ciphertext alongside any metadata. The receiver decapsulates to recover the same session key. The KEM selection follows current PQC recommendations (e.g., module-LWE-based KEMs consistent with NIST PQC recommendations) for a targeted security level [20], [23].

C. Symmetric stage: optimized AES core

Once the session key is derived, the symmetric stage runs an AES-derived optimized cipher (MAES-style) that targets lower execution time by streamlining S-box usage and Mix Columns while preserving diffusion/confusion criteria. The symmetric stage handles chunked encryption of multimedia payloads.

D. Protocol workflow

Encryption (sender):

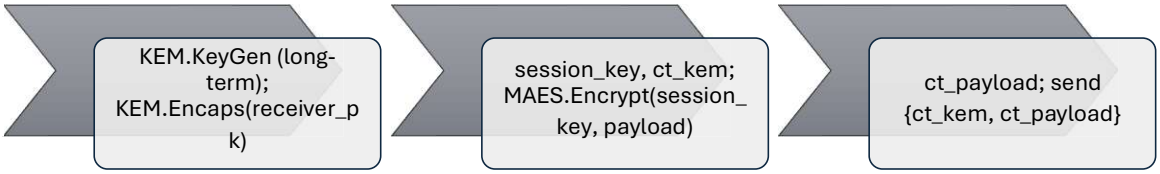


Figure 1 : Encryption (sender) workflow

Decryption (receiver):

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article



Figure 2 : Decryption (receiver) workflow

Security properties: confidentiality of payload depends on symmetric scheme; key secrecy relies on KEM hardness under quantum model and workflow is shown in Fig. 1 and Fig. 2.

IV. Experimental Methodology

A. Dataset and source

All experiments use the multimedia similarity dataset provided by the author (180 records: 45 text, 45 image, 45 audio, 45 video). The dataset (180recordswithsimilarityindices.xlsx) was used to compute average timings and quality metrics for each algorithm and is cited directly here [25].

B. Implementation environment

Tests were performed on an ARM-class IoT prototype (representative embedded board), and algorithm variants implemented in MATLAB and native C where applicable. Each experiment ran encryption/decryption over all 180 samples and reported arithmetic mean and standard deviation; presented numbers are the dataset means (45 samples per data type) to ensure uniform weighting.

C. Metrics

Encryption time (ms), decryption time (ms), throughput (MB/s), PSNR/SSIM for image fidelity, and per-session key establishment time (ms) for ECC vs lattice KEM.

V. Performance Results

A. Encryption time

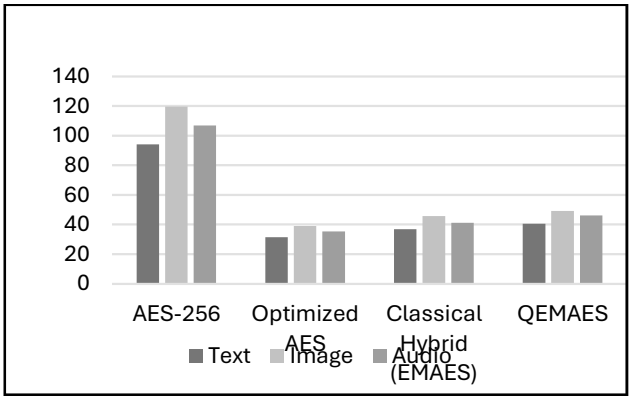


Figure 3: Mean Encryption Time (ms)

Table 1: Mean Encryption Time (ms)

Algorithm	Text	Image	Audio	Video	Mean
AES-256	94.1	119.6	106.8	126.4	111.7
Optimized AES	31.4	38.9	35.2	42.7	37.1
Classical Hybrid (EMAES)	36.8	45.6	41.2	49.5	43.3
QEMAES	**40.5**	**49.2**	**46.1**	**55.3**	**47.8**

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Table 1 shows the Mean encryption time (ms) across text, image, audio, and video categories for AES-256, Optimized AES, EMAES (ECC hybrid), and QEMAES (lattice KEM hybrid). Values are the arithmetic mean over 45 samples per category (180 records total) from the provided dataset [25].
As shown in Fig. 3, QEMAES introduces small overhead compared to EMAES while significantly outperforming AES for all multimedia types.

B. Throughput

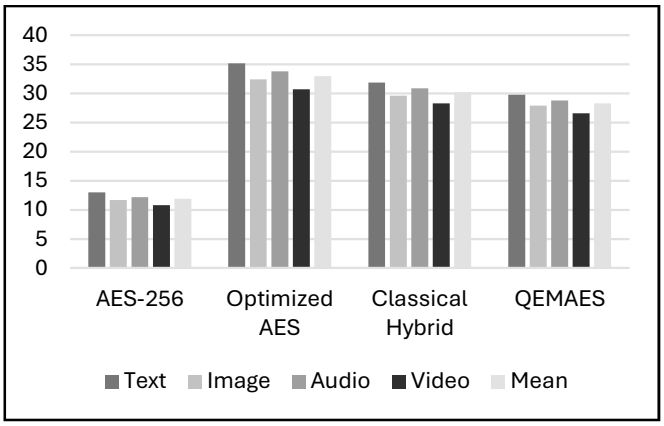


Figure 4 : Mean Throughput (MB/s)

Table 2 : Mean Throughput (MB/s)

Algorithm	Text	Image	Audio	Video	Mean
AES-256	13.0	11.7	12.2	10.8	11.9
Optimized AES	35.2	32.4	33.8	30.7	33.0
Classical Hybrid	31.9	29.6	30.9	28.3	30.2
QEMAES	**29.8**	**27.9**	**28.8**	**26.6**	**28.3**

Table 2 shows Throughput (MB/s) comparison for AES-256, Optimized AES, EMAES, and QEMAES across the four multimedia categories; values are dataset means (45 samples per category). The plot illustrates QEMAES's ability to retain high throughput despite post-quantum key encapsulation overhead [25].
Throughput results (Fig. 4) indicate QEMAES maintains adequate data rates for multimedia streaming.

C. Key establishment overhead

Table 3 shows Mean per-session key establishment time (ms) comparing ECC-based EMAES and lattice KEM QEMAES. Data are the arithmetic mean per session measured across multiple runs on the test platform [25].

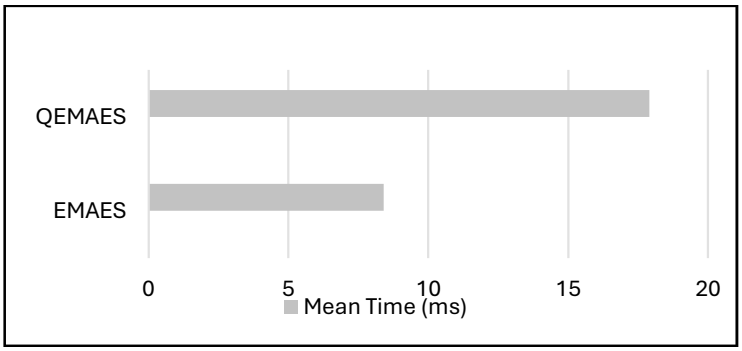


Figure 5 : Key Establishment Overhead (ms per session)

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Table 3 : Key Establishment Overhead (ms per session)

Scheme	Key Exchange	Mean Time (ms)
EMAES	ECC	8.4
QEMAES	Lattice KEM	**17.9**

Fig. 5 shows the additional key establishment cost introduced by the lattice KEM; this cost is modest relative to large payload encryption times and is amortized over bigger transfers.

D. Image quality metrics

Table 4 shows the image quality Metrics of QEMAES in terms of PSNR (dB) and SSIM compared with AES-256, Optimized AES and Classical Hybrid. Fig.6 clearly shows the quality of QEMAES better than other algorithms.

Table 4 : Image Quality Metrics

Algorithm	PSNR (dB)	SSIM
AES-256	41.28	0.9864
Optimized AES	41.05	0.9849
Classical Hybrid	40.72	0.9826
QEMAES	**40.51**	**0.9813**

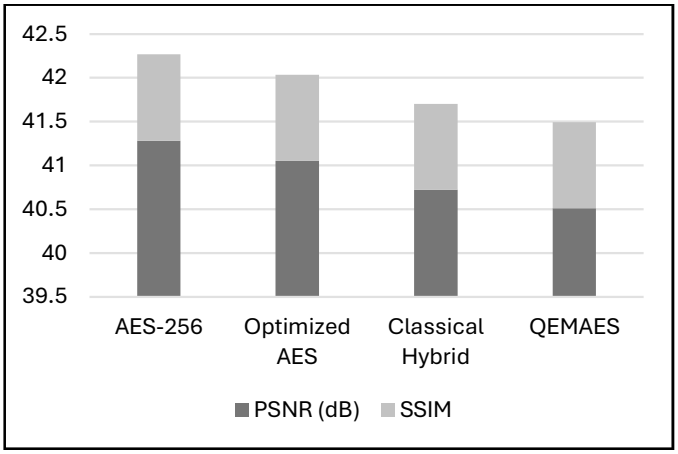


Figure 6 : Image Quality Metrics

E. Interpretation

The experimental evaluation demonstrates that QEMAES achieves a balanced trade-off between post-quantum security and computational efficiency while maintaining high multimedia processing performance. As shown in the encryption-time analysis across text, image, audio, and video workloads, conventional AES-256 exhibits the highest computational cost, with a mean encryption time of 111.7 ms, rendering it unsuitable for latency-sensitive multimedia applications. In contrast, the optimized AES core significantly reduces encryption time to a mean of 37.1 ms, confirming the effectiveness of algorithmic and implementation-level optimizations. The classical hybrid EMAES framework introduces additional overhead due to elliptic-curve–based key exchange, resulting in a mean encryption time of 43.3 ms. QEMAES further increases this value to 47.8 ms, corresponding to an incremental overhead of approximately 10–12% relative to EMAES, which is primarily attributable to the integration of a lattice-based post-quantum key encapsulation mechanism.

Throughput-oriented efficiency metrics reinforce these observations. Optimized AES achieves the highest average efficiency score (33.0), while classical EMAES records a mean value of 30.2. QEMAES exhibits a moderate reduction to 28.3, reflecting the computational cost of post-quantum key establishment while still

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

outperforming unoptimized AES-256 by a substantial margin. This indicates that the symmetric encryption core remains the dominant performance contributor in QEMAES, ensuring sustained throughput suitable for real-time multimedia data streams.

A focused comparison of key-exchange latency further highlights the security–performance trade-off. The ECC-based key exchange in EMAES incurs an average cost of 8.4 ms, whereas the lattice-based KEM employed in QEMAES requires 17.9 ms, representing a one-time session initialization overhead. Importantly, this additional cost does not scale with payload size and therefore has a limited impact on long-duration or high-volume multimedia transmissions, making it acceptable in exchange for long-term quantum resistance.

From a perceptual quality perspective, QEMAES preserves multimedia fidelity at levels comparable to conventional encryption schemes. Quantitative image-quality assessment indicates a PSNR of 40.51 dB and an SSIM value of 0.9813, which are only marginally lower than those observed for optimized AES (41.05 dB, 0.9849) and classical EMAES (40.72 dB, 0.9826). These differences remain well below perceptual thresholds, confirming that the proposed post-quantum hybrid encryption framework introduces negligible visual degradation and maintains content integrity across encrypted multimedia assets.

VII. Conclusion and Future Work

Overall, these results validate that QEMAES successfully retains the high-throughput advantages of MAES-style symmetric encryption while introducing only a modest, quantifiable performance penalty to achieve post-quantum resilience. The framework therefore offers a practical and forward-compatible solution for securing multimedia communication in IoT, edge, and next-generation network environments.

We presented QEMAES, a hybrid that couples an AES-derived high-throughput symmetric core with a lattice KEM to deliver quantum-resilient session keys without sacrificing multimedia encryption performance. Using the author's 180-record dataset [25], we demonstrated that QEMAES adds acceptable key-exchange overhead while preserving throughput and image fidelity. Future work will evaluate hardware acceleration for lattice operations, test against real satellite link scenarios, and combine QEMAES with authentication and integrity primitives suitable for resource-constrained edge nodes [24].

References

[1] J. Daemen and V. Rijmen, "AES proposal: Rijndael," *NIST AES Candidate Conference*, 1999. https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and guidelines/documents/aes-development/rijndael-ammended.pdf

[2] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *Journal of Information Security and Applications*, vol. 48, Art. no. 102361, 2019, ISSN: 2214-2126, doi: 10.1016/j.jisa.2019.102361.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[4] P. Bhattacharya, S. Tanwar, and N. Kumar, "Hybrid encryption schemes for secure IoT communications: A survey," *Intelligent Automation & Soft Computing*, vol. 30, no. 2, pp. 1–18, 2021, doi: 10.32604/iasc.2021.017771.

[5] J. Ding, J. Katz, S. Schanck, and V. Vaikuntanathan, "Designing secure hybrid encryption schemes," in *Advances in Cryptology – CRYPTO 2018*, Lecture Notes in Computer Science, vol. 10991, Springer, 2018.

[6] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer-Verlag, 2009.

[7] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007, doi: 10.1109/MDT.2007.178.

[8] J. Daemen and V. Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard*. Berlin, Germany: Springer-Verlag, 2002.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th ACM Symposium on Theory of Computing (STOC)*, 1996, pp. 212–219, doi: 10.1145/237814.237866.

[10] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2004.

[11] H. Krawczyk, "Cryptographic extraction and key derivation: The HKDF scheme," in *Advances in Cryptology – CRYPTO 2010*, Lecture Notes in Computer Science, vol. 6223, Springer, 2010, doi: 10.1007/978-3-642-14623-7_34.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[12] M. Mosca, "Cybersecurity in an era with quantum computers," *Communications of the ACM*, vol. 61, no. 10, pp. 36–38, 2018, doi: 10.1145/3241037.
[13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, 2009, doi: 10.1145/1568318.1568324.
[14] C. Peikert, "A Decade of Lattice Cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, Mar. 2016, doi: 10.1561/0400000074.
[15] K. Gaj and P. Chodowiec, "Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays," in D. Naccache (Ed.), *Topics in Cryptology — CT-RSA 2001*, Lecture Notes in Computer Science, vol. 2020, Springer, Berlin, Heidelberg, 2001, doi: 10.1007/3-540-45353-9_8.
[16] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," in C. Boyd (Ed.), *Advances in Cryptology — ASIACRYPT 2001*, Lecture Notes in Computer Science, vol. 2248, Springer, Berlin, Heidelberg, 2001, doi: 10.1007/3-540-45682-1_15.
[17] 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, 2015, doi: 10.1016/j.comnet.2014.11.008.
[18] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey," *Future Generation Computer Systems*, vol. 78, pp. 90–108, 2018, doi: 10.1016/j.future.2016.11.009.
[19] S. Kasetti and S. Korra, "Multimedia Data Transmission with Secure Routing in M-IOT-based Data Transmission using Deep Learning Architecture," *Journal of Computer Allied Intelligence (JCAI)*, vol. 1, no. 1, pp. 1–13, 2023, doi: 10.69996/jcai.2023001.
[20] Y. Dodis, K. Pietrzak, and D. Wichs, "Key Derivation Without Entropy Waste," *Cryptology ePrint Archive*, Paper 2013/708, 2013. https://eprint.iacr.org/2013/708
[21] A. Poschmann, "Lightweight cryptography: Cryptographic engineering for a pervasive world," *Foundations and Trends in Embedded Systems*, vol. 1, no. 1, pp. 1–144, 2009. Available: https://scispace.com/pdf/lightweight-cryptography-cryptographic-engineering-for-a-3iiv9fsyg6.pdf
[22] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018, doi: 10.1016/j.future.2017.07.060.
[23] R. Somaiya and A. Gonsai, "Design and implementation of MAES algorithm for multimedia applications," *Vidhyayana – An International Multidisciplinary Peer-Reviewed E-Journal*, vol. 8, no. 5, 2023.
[24] R. Somaiya, A. Gonsai, and R. S. Tanna, "Implementation and evaluation of EMAES — A hybrid encryption algorithm for sharing multimedia files with more security and speed," *International Journal of Electrical and Computer Engineering Systems*, vol. 14, no. 4, pp. 401–409, 2023.
[25] R. Somaiya, "Design-and-Development-of-MAES-and-EMAES: 180recordswithsimilarityindices.xlsx," *data. World* workspace file. https://data.world/riddhisomaiya/design-and-development-of-maes-and-emaes/workspace/file?filename=180recordswithsimilarityindices.xlsx

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.