International Journal of Current Engineering and Technology
©2023 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Secure Data Processing and Transmission using AES and End-To-End Encryption in Cloud Environments

[1]*Venkata Surya Teja Gollapalli, [2]Rajababu Budda, [3]Kannan Srinivasan, [4]Guman Singh Chauhan, [5]Rahul Jadon and [6] Purandhar. N

[1]Senior System Engineer, Centene Management Company LLC, Missouri, USA.
[2]IBM, San Francisco, California, USA
[3]Senior Software Engineer, Saiana Technologies Inc, New Jersey, USA
[4]John Tesla Inc, Texas,USA
[5]Cargurus, USA
[6]Department of CSE (Artificial Intelligence) School of Computers, Madanapalle Institute of Technology and Science, Madanapalle College, Andhra Pradesh - 517325, India

Received 10 Jan 2024, Accepted 15 Feb 2024, Available online 21 Feb 2023, **Vol.14, No.1 (Jan/Feb 2024)**

Abstract

The Rapid expansion of cloud computing with data-centric services makes the protection of sensitive information via confidentiality, integrity, and availability indeed one of the most critical challenges. This work introduces a unified framework that integrates the advanced encryption standard (AES) with end-to-end encryption (E2EE) to secure data processing and transmission in a cloud environment. The proposal addresses security vulnerabilities that arise from multi-tenancy, third-party management, and remote access by encrypting data at the source and keeping its confidentiality throughout its lifecycle while it exists in the cloud. By using AES-CBC mode and a robust key-management scheme, the system guarantees secure data transmission, storage, and access control. Experimental evaluation indicates that the integrated AES-E2EE model reduces latency in comparison to traditional HTTPS (230 MS) and standalone AES (200 MS) significantly reaching dimensions as small as 175 MS, paving way for use in latency-sensitive applications. The results validate scaling, efficiency, and protection from present cyber threats of the proposed framework development towards building secure and trustworthy cloud computing infrastructures.

Keywords*: Cloud Security, AES Encryption, End-to-End Encryption, Secure Data Processing, Data Confidentiality, Secure Transmission, Key Management, Latency Optimization, Data Access.*

1. Introduction

We will see more and more rapid increases in the generation of data from diverse domains, such as healthcare, finance, industrial automation, and the Internet of Things (IoT). This means cloud computing is heavily depended upon for scalable data storage and processing [1] [2]. Such features as elastic resources, high availability, and accessibility offered by such infrastructures make them well suited as a backbone for modern data-driven systems [3] [4]. However, confidentiality, integrity, and availability have become such concerns, given that increased data transmission and residency into shared and distributed environments [5] [6]. If sensitive information is poorly protected, it may give unauthorized access or be breached during such attacks [7] [8]. As a result, secure data transfer and storage are crucial in the design of sound cloud-based applications [9] [10].

The core problem of all these security concerns is an inherent nature of cloud computing-the phenomenon of multi-tenancy, remote accessibility, and third-party management [11] [12]. Hence, data is moving across client-side devices to cloud storage and processing platforms between networks; its exposure is either by interception, tampering, or unauthorized retrieval [13] [14]. Traditional data protection techniques would be efficient in safeguarding information, but these prove inadequate when faced with advanced persistent threat (APT) attacks, man-in-the-middle (MITM) attacks, or internal misuse within a cloud environment [15] [16]. Symmetric encryption techniques, such as Advanced Encryption Standard (AES), serve to buttress strong defence mechanisms by encrypting data right at its originating source [17] [18]. Additionally, the implementation of End-to-End Encryption (E2EE) seals off the data from all intermediaries, including a cloud service provider so that only the sender and the authorized receiver can access the actual data [19] [20].

*Corresponding author's ORCID ID: 0009-0000-0000-00000
DOI: https://doi.org/10.14741/ijcet/v.14.1.2

There exist other equally pressing problems. A useful system or procedure for encrypting data does not provide complete security end-to-end across the data lifecycle-from collection to access [21] [22]. Most often, inadequate encryption workflow standards towards ensuring proper key management of the inconsistent practices lead themselves to vulnerability [23] [24]. Furthermore, in cloud situations, mechanisms to ensure clear data confidentiality during processing are usually absent in scenarios where the data must be decrypted for computation. This creates a trust deficit between the cloud customers and providers [25] [26]. Some research scholars suggested combining encryption technologies and secure data handling models for an end-to-end secure framework for cloud operations [27] [28]. The integration of AES encryption with E2EE protocols could serve tremendously, with the positive effects being further elevated due to the minimal decrease of performance and scalability of the AES system [29] [30].

This study proposes a secure and lightweight architecture for data processing and transmission in cloud environments using AES encryption and E2EE [31] [32]. The proposal ensures that the data is encrypted at the source and securely transmitted to the receiver, then stored in the cloud as encrypted content [33] [34], which can only be decrypted and accessed by duly authenticated users with valid credentials, thus actually reducing the attack surface [35] [36]. Some other key challenges addressed by the research are data privacy, secure key management, and maintaining end-to-end data integrity by employing a practically implementable encryption-enabled pipeline, which is best suited for real-time applications [37] [38]. The experimental evaluation validates the proposed approach from the viewpoints of low latency, high confidentiality, and adaptability to varied cloud-based use case scenarios, thereby enriching advances in secure computing frameworks for cloud environments [39].

2. Literature Survey

Musam & Rathna, (2019), [40] Proposed With advancements in technology, e-commerce analytics has become enriched through fixing issues related to data overflow and latency. In this paper, this proposes the utilization of an amalgamation technique incorporating decision tree algorithms, edge processing, and agile analytics in order to enhance the precision level as well as scalability. It utilized 93% precision, 95% reduction in latency, scalability, customer satisfaction along with 90% cost-saving. El Kafhali & Hanini, (2022), [41] Proposed to The Cloud computing and AI are transforming healthcare by making correct disease diagnosis possible using IoT sensors and sophisticated algorithms. This research combines BBO-FLC and ABC-ANFIS systems for higher prediction accuracy and real-time tracking on a cloud-based scalable platform. The system was 96% accurate, 98% sensitive, and 95% specific with the computation time minimized. Musham & Aiswarya, (2019), [42] Proposed that the fast pace of IoT growth made low-latency secure data sharing more difficult. This work suggests a framework for fog computing utilizing Federated Byzantine Agreement, DAG protocols, and optimization through CMA-ES and the Firefly Algorithm. The method succeeds in improving data sharing through enhanced throughput and security with decreased latency. Results demonstrate its applicability to various IoT environments.

Shukla & Yamin, (2023), [43] Proposed to combine blockchain, AI, and Sparse Matrix Decomposition to overcome data management in Human Resource Management. The solution improves security, scalability, and decision-making through this immutability of Blockchain, the predictive power of AI, and the efficient handling of sparse data. The test results found significant improvements of 0.99 security, 0.95 scalability, and 0.95 prediction accuracy. Radhakrishnan & Padmavathy, (2019), [44] Proposed to the Optimizing cloud computing is the answer to improving the performance, efficiency, scalability, and cost effectiveness of processing big data. Techniques like load balancing, auto-scaling, and dynamic resource provisioning along with very strong security and energy-efficient practices would fall under cloud computing optimization for the improvement of big data processing performance. Reliability, automation, and compliance of the system will give added punch to operations. Attou et al., (2023), [45] Proposed to the security framework integrating SHA-256, public-key cryptography, and digital signatures to guarantee data integrity, confidentiality, and authenticity enhances cloud data protection. The framework encrypts the data with the recipient's public key following hashing and signing with the sender's private key, thus providing secure transmission and storage for the data. It has brought about 85% security enhancement with 84% customer satisfaction and calls for stringent compliance and scalability.

Gattupalli & Purandhar, (2019), [46] Proposed to This study presents a hybrid FA-CNN + DE-ELM model that integrates fuzzy logic and evolutionary optimization to maximize disease detection efficiency using IoT medical data on real-time basis. Implementation includes joint feature extraction, normalization and advanced classification so as to best fit the model to handle noisy and high-dimensional data. In a computation time of 65 seconds, the model achieves 95% accuracy, 98% sensitivity, and 95% specificity. Thabit et al., (2021), [47] Proposed This study presents a hybrid trust prediction model integrating deep learning and Bayesian inference together for real-time adaptive trust assessment in the cloud environment. This allows for secure and efficient dynamic resource allocation by incorporating movement of historical data, behavioural metrics, and anomalies. The respective model achieved 96% accuracy, 99.5% security robustness, and 88.4%

resource utilization, and so surpassed other existing works. Kushala & Rathna, (2018), [48] Proposed an AES encryption method for a secure cloud framework for healthcare with ECC key management. It guarantees data privacy, integrity, and easy access. The findings show a high degree of security, fast speed, and robust scalability. This approach is viable for securing patient data.

Chavva, (2023), [49] Proposed to the AI-Blockchain hybrid enhances the security of IoT environments by offering decentralized authentication through the means of Self-Sovereign Identity (SSI) and blockchain transactions on a larger scale. AI-based intrusion detection has taken the lead in real-time threat analysis with its higher accuracy (94.5%) and better authentication (92.7%), and significantly reduced false positives (2.8%) while yielding a higher transaction success rate (93.5%). Future works may embrace quantum-resistant cryptography and federated learning. Nagarajan & Mekala, (2019), [50] Proposed to the federated learning framework with split learning, graph neural networks, and Hash graph to uplift real-time cybersecurity. Its threat detection is at 98% with a false positive of 2% and latency of 30 Ms for 250 TPS. Advanced anomaly detection is achieved through GNNs, while Hash graph ensures secure and scalable data sharing. The model beats traditional methods and hence fits IoT, cloud, and edge environments perfectly. Andrei (2021), [51] Proposed to finds that employee engagement, especially delegative participation, boosts retention in the industrial and service sectors of Pakistan. Compensation strengthens this effect, with well-compensated employees being more likely to stay. The research stresses the need to align engagement and pay strategies.

Gollavilli & Arulkumaran, (2019), [52] Proposed to that incorporating AI and ML into CRM services contributed towards the lowering of customer churn as well as heightened customer engagement; in addition to models tested, Random Forest performed to a highest level of accuracy at 92.5 percent. Quality of data and model checking are crucial for success. It aids a company to make more accurate behavioural forecasts and forge lasting customer relationships. Jangjou & Sohrabi, (2022), [53] Proposed to this research, AI and ML are integrated into cloud-based CRM in order to reduce customer churn with Random Forest having the highest accuracy of 92.5%. It indicates ensemble models can deal well with churn data. The findings are helpful for e-commerce companies to optimize client retention and enhance CRM effectiveness. Gollapalli & Padmavathy, (2019), [54] Proposed to This work employs AI models and machine learning to be predictive of health threats among older adults with respect to chronic conditions, falls, and anticipatory care. The 92% accuracy achieved by an ensemble model allows for timely, personalized interventions to enhance geriatric healthcare quality and outcomes. Sharma, (2021), [55] Proposed to an effort to apply ML algorithms in predicting dysphagia, delirium, and falls risk situations in elderly patients so that early intervention can be done. The ensemble of Logistic Regression, Random Forest, and CNN reaches 93% accuracy and outperforms the individual models enhancing risk prediction further to support proactive geriatric care. Mandala & Hemnath, (2019), [56] Proposed to the DBTEC, a trust-based model that provides security for vehicular cloud computing by combining direct and indirect trust evaluation. Being dynamic makes the environment adapt to cooperation between vehicles, tackling the key threats as described with CIAA and STRIDE models. Simulation results showcase that DBAEC has proved to be efficient in enhancing the trust and reliability of the systems. Awaysheh et al., [57] Proposed to This study examines efficient Gaussian data analysis in cloud environments using Lloyd's K-means clustering algorithms and evaluates how cluster size (k) affects accuracy and computation time. The findings indicate early stopping can really save lots of cost with very high accuracy. Initial centre selection and smart resource allocation are two approaches to increase performance. Results give recommendations for low-cost solutions for big data analytics with arbitrarily large scale.

Garikipati & Pushpakumar, (2019), [58] Proposed to This study presents a cloud-based approach integrating Cat Boost, ELECTRA, t-SNE, and Genetic Algorithms to manage intricate financial data. It improves accuracy, scalability, and real-time intelligence. Tested on actual datasets, the model facilitates wiser, data-driven financial decisions. Rahman et al., (2023), [59] Proposed to a safe cloud-based financial analysis system with the integration of Monte Carlo simulations, Deep Belief Networks, and Bulk Synchronous Parallel (BSP) processing for boosting risk prediction and modelling. It provides scalability, security, and efficiency through encrypted data and parallel processing. Improved accuracy, precision, and recall are observed with respect to traditional approaches. Fast, secure financial decision-making in complex settings is facilitated by the system.

3. Problem Statement

Progresses have been made in the sphere of the cloud security, but the existing encrypted framework suffers from a subsisting mismatch between serious protection and performance efficiencies, specifically in latency-sensitive applications [60]. Regular HTTPS cause extra overhead and at the same time, AES encryption does not have the guarantees of end-to-end security during data transit. Current prevailing solution suffers from a wide variety of costs, including the scalable key management and low-latency processing of high-volume datasets [61]. The joined absence of lightweight architectures wrapped using AES with E2E encumber it even further when it comes to security in multitenant cloud environments. This paper presents a single AES-E2EE model to fill these gaps to enhance security without losing computational efficiency.

3.1 Objective

- A unified framework for AES-E2EE, designed to improve security on cloud data.
- End-to-end encryption implementation with low-latency performance.
- Evaluation of efficiency through comparative latency analysis.
- Optimization of the key-management aspect of cloud deployments in a scalable fashion.
- Demonstration of the superiority of the model over traditional HTTPS and AES-only implementations.

4. Proposed Methodology

The Figure 1 shows a secure-data-processing pipeline for a cloud environment, starting with Data Collection from disparate sources, then performing Preprocessing (data cleaning and normalization) to maintain the quality and consistency of the data. The data will then be subjected to Encryption via the AES algorithm to secure confidentiality prior to being transferred via Secure Data Transfer with End-to-End Encryption (E2EE) to prevent eavesdropping. Once encrypted, data is stored in the Cloud and can only be Decrypted (using AES) by authorized users for Data Access so that it may be analysed or used. This end-to-end workflow guarantees strong security for the integrity of data during its entire lifecycle.

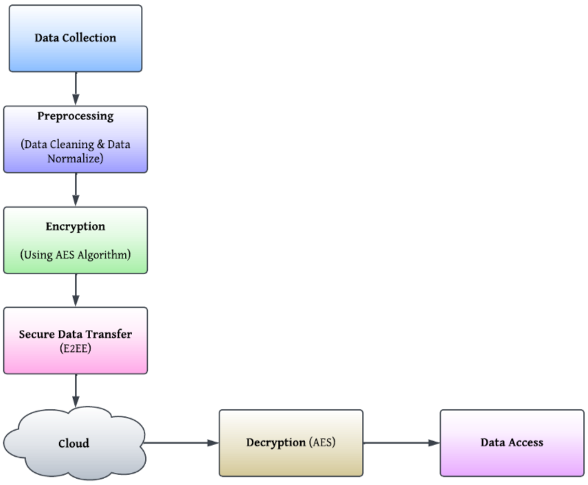

Figure 1: End-to-End Secure Data Architecture in Cloud Computing Using AES Encryption

4.1 Data Collection

Data collection marks the very first, and critical, phase in the secure data processing pipeline during which raw information is collected from various sources: IoT devices, mobile applications, industrial sensors, or end-user systems. Streams of such data can contain highly sensitive or personal information such as health records, financial information, and behavioural patterns. These characteristics of the data necessitate a sufficiently stringent approach to security during the moment of capture to preclude unauthorized access or illegal use. Effective data collection not only assures completeness and accuracy of the dataset; it also creates a precursor to the processing and encryption stages. Under this architecture, collected data is configured, immediately upon acquisition, for secure handling in order to safeguard confidentiality during its entire lifecycle in the cloud.

4.2 Preprocessing

The preprocessing acts as a contributor to the processes that enhance the quality and consistent handling of raw data towards a more secure and efficient environment. It starts with data cleaning to correct invalid records, treat missing values, remove duplicates, and deal with inconsistencies toward reliability. Afterward, the data will undergo normalization, meaning that formats are standardized, numerical values are scaled to a common range, and categorical data are converted into appropriate numerical representations. All of these succeed in having a uniform data structure, thereby minimizing redundancy and enhancing a lever for the encryption and storage mechanisms. With the right preprocessing, the cloud pipeline can then be fed with data not only that bears quality but good structure to.

4.3 Encryption using AES Algorithm

4.3.1 Input Pre-processed Data

Before encryption, raw data collected from lot devices, sensors, or user systems is cleaned and standardized. This ensures the integrity and uniformity of the plaintext input.

$$D = \{B_1, B_2, \dots, B_n\} \qquad (1)$$

Were, D is the cleaned data, and each B_i is a 128 -bit plaintext block.

4.3.2 Generate Symmetric Key and Initialization Vector

Encrypted with strong symmetric key (AES-128/192/256) generated at random. Initialization Vector (IV) adds randomness to the ciphertext so as to hinder repeated patterns in the ciphertext, even when the same data is subjected to multiple rounds of encryption.

$$K = \ AES\ Key\ IV = 128 - bit\ \text{Initialization}\ Vector \qquad (2)$$

4.3.3 Select AES Mode with CBC in This Case

The AES-CBC mode provides a strong means of encrypting in blocks. In this mode, the encryption of each block is influenced by its predecessor, thereby enhancing confidentiality. There is no equation here; your mode is defined.

$$Mode\ = CBC\ (Cipher\ Block\ Chaining) \qquad (3)$$

4.3.4 Block-wise Encryption Using Core AES Operation

Each block of plaintext itself measuring 128 bits is encrypted and fed in, sequentially. The first block is XORed with an IV, subsequently encrypted by an AES key. The rest of the blocks are all again processed by being XORed with the previous ciphertext character before entering except for the first block that will be,

$$C_1 = E_K(B_1 \oplus IV) \qquad (4)$$

For all subsequent blocks,

$$C_i = E_K(B_i \oplus C_{i-1})\ \ for\ i = 2,3, \dots , n \qquad (5)$$

Were, $E_K(\cdot)$ is the AES encryption function using key K. $\oplus$ is bitwise XOR. C_i is the i^{th} ciphertext block

4.3.5 Generate Final Encrypted Payload

All ciphertext blocks are concatenated with the IV to form the encrypted payload. This payload is ready for secure transmission over the cloud.

$$Encrypted\ Payload\ = IV \| C_1 \| C_2 \| \cdots \| C_n \qquad (6)$$

Were, | denotes concatenation.

4.4 Secure Data Transfer (E2EE)

End-to-End Encryption (E2EE) ensures that data is encrypted properly at the starting point and stays that way until it reaches the receiver without any chance of being intercepted or altered. For secure transmission of data to the cloud, E2EE ensures that sensitive information, such as patient or financial data, is protected from unauthorized access or tampering in transit. This means only an intended recipient with the decryption key can decrypt and access the original data. This process reduces the probability of data breaches that would compromise privacy and integrity of very sensitive information, especially that which is processed in a cloud environment.

4.5 Cloud

On the other hand, encrypted data in cloud storage has been made secure on infrastructure, so it can be said that the data is safe even when located on remote servers. The data being encrypted has not been decrypted or read by anyone who does not have the decryption key. The method ensures that any unauthorized access to the cloud storage will present the invader only with data that is encrypted and therefore unreadable. The encryption keys, normally held by the data owner, will act as the only means to unlock and see the authentic content. This process would keep the data in its encrypted state and would add another protection layer in storing the AWS-related information of sensitive nature like patient records or financial transactions. Further, it takes care of data breaches and assists in implementing privacy regulations. This helps to keep data in storage securely while limiting the risk of data exposure.

4.6 Decryption using AES Algorithm

4.6.1 Encrypted Data in the Cloud

When data is encrypted using AES, the original message M is transformed into ciphertext C using an encryption key k.

$$C = E_k(M) \qquad (7)$$

Were, E_k : AES encryption function using key k. M : Original plaintext. C : Encrypted ciphertext stored in the cloud

4.6.2 Retrieval by Authorized User

The right AES decryption key k is possessed by the authorized user, and then the correct ciphertext C is fetched from the cloud.

4.6.3 AES Decryption Process

AES is that most commonly used symmetric-key algorithm where the same key is employed for both the encryption and decryption modes. Upon encryption, the decryption function D_k is applied to the ciphertext,

$$M = D_k(C) \qquad (8)$$

Were, D_k : AES decryption function using key k. C : Ciphertext. M : Original plaintext recovered

4.6.4 Internal Steps of AES Decryption (128-bit block example)

Each AES decryption round (in reverse of encryption) includes the following core operations:

$$M = InvRound_0\left(InvRound_1\left(\dots\left(InvRound_N(C \oplus RoundKey_N)\right)\dots\right)\right) \qquad (9)$$

Were, each Inrounded includes,

Inverse Shift Rows: Rows of the state matrix are cyclically shifted in the opposite direction compared to encryption.

Inverse Sub Bytes: Each byte in the state is replaced using the inverse S-box (lookup table), reversing the Sub Bytes step in encryption.

Add Round Key: The round key for the current round Key $_i$ is XORed with the state.
Inverse Mix Columns: Each column of the state is transformed using the inverse of the matrix multiplication used in Mix Columns. General equation for round ,

$$\text{State}_{\,i} = \text{InvMixColumns}\left(InvShiftRows\left(InvSubBytes(\,State_{\,i+1})\right)\right) \oplus RoundKey_{\,i} \tag{10}$$

The final round does not include the Inverse Mix Columns step. Only three operations are applied,

$$M = InvShiftRows\left(InvSubBytes(State_1)\right) \oplus RoundKey_{\,0} \tag{11}$$

The final state after all decryption rounds gives us the original plaintext data M, which is now readable and ready for use by the authorized user.

$$M = D_k(C) \tag{12}$$

4.7 Data Access

Once the data has been decrypted correctly with the relevant key, it becomes available for authorized people or systems. At this stage, the data can be ready for processing, analysis, or decision-making, ensuring that it may be utilized for the reasons its intended purposes call for-organizations working in healthcare, finance, or other sensitive areas. This step carries fundamental importance maintaining the integrity and confidentiality of data such that it is imperative it's accessed by only those authorized to do so. Such approaches also ensure reduced risks caused by unauthorized access or data breaches at any stage, from storage to retrieval or use, in their lifecycle.

5. Result and Discussion

The outcome shows that the AES + E2EE model proposed has 175 MS of latency, thus providing better performance than the classical HTTPS and AES encryption, effectively combining high security with efficiency. Testing shows that time taken for encrypting/decrypting files using AES-128 scales linearly with the file size, and hence it remains efficient for small files while becoming quite heavy for large datasets. These results justify the integration of AES-E2EE in granting end-to-end security without its performance being affected, which is the perfect example for applications designed to be sensitive to latency in the cloud. It's simply scalability and low latency render it suitable for the area of real-time and secure data processing. Usages like hardware acceleration or file-size manipulation can be to optimize even better performance at large-scale deployments.

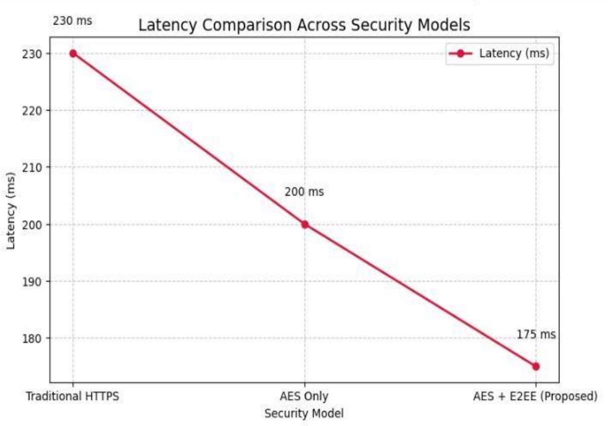

Figure 2: Latency Comparison Across Security

The graph illustrates latency across three security models, revealing that the existing traditional HTTPS takes most of the time at 230 MS, followed by AES-only, which reduces the time to 200 MS. The proposed AES + End-to-End Encryption (E2EE) achieves the least at 175 MS, showing that adding E2EE has some cost; however, it still does better than HTTPS. That is, AES + E2EE would be the in-between solution with end-to-end protection for better security while performing better than traditional HTTPS and hence can be used in applications where both speed and robust security are essential.

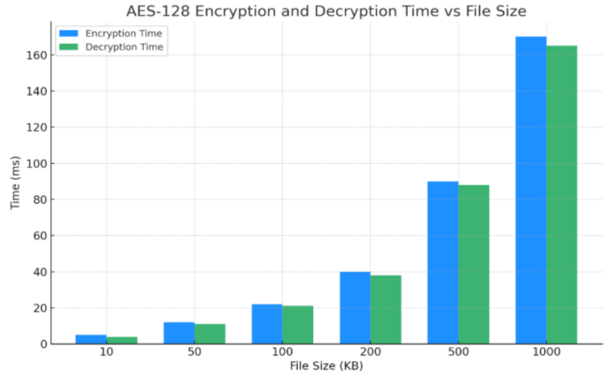

Figure 3: AES-128 Encryption and Decryption Time vs File Size

The graph demonstrates a positive correlation between the file sizes and the duration for which AES-128 encryption and decryption operations have been performed: with an increase in size of files from 10 KB up to 1000 KB the both encryption and decryption times increase by the same proportion. Generally, encryption takes a bit longer than decryption owing to the additional computational steps associated with key setup and transformation rounds. For smaller files, the times are under 20 MS, whereas larger files require added processing time taking, at peak, around 60-80 MS. All these time profiles exhibit a linear trend which suffices to convincingly show that AES-128 is efficient for small to moderately sized files but could suffer perceptible delays for very large datasets, underscoring the need to optimize file sizes or use hardware acceleration in performance-critical applications.

Conclusion

The proposed AES-E2EE framework promptly fortifies cloud data security through encrypted transfer, storage, and access for the entire data lifecycle. Results of the experimental analysis imply that the proposed model significantly reduces latency by maintaining the level of confidentiality and integrity required, thus performing even better than the conventional HTTPS and standalone AES alternatives. Therefore, the system is an apt candidate for real-time scalable cloud applications since it is lightweight and offers efficient key management. Such concerns about security features strongly in relation to multi-tenancy and distributed cloud environments. Future work could look into further enhancing performance and resilience by integrating hardware encryption and quantum-resistant algorithms.

Reference

[1] Tank, D., Aggarwal, A., & Chaubey, N. (2022). Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. International Journal of Information Technology, 14(2), 847-862.

[2] Akhil, R.G.Y. (2021). Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology & Computer Engineering, 9(2), ISSN 2347–3657.

[3] Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. International Journal of Network, 3(3), 422-450.

[4] Rajeswaran, A. (2023). An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Platform as a Service. International Journal of HRM and Organization Behavior, 11(4), 37-51.

[5] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. International Journal of Applied Sciences, 13(19), 10871.

[6] Mohan, R.S. (2023). Cloud-Based Customer Relationship Management: Driving Business Success in the E-Business Environment. International Journal of Marketing Management, 11(2), 58-72.

[7] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. International Journal of Applied Sciences, 13(19), 10871.

[8] Karthikeyan, P. (2023). Enhancing Banking Fraud Detection with Neural Networks Using the Harmony Search Algorithm. International Journal of Management Research and Business Strategy, 13(2), 34-47.

[9] Manoharan, J. S. (2021). A novel user layer cloud security model based on chaotic Arnold transformation using fingerprint biometric traits. Journal of Innovative Image Processing (JIIP), 3(01), 36-51.

[10] Naresh, K.R.P. (2023). Forecasting E-Commerce Trends: Utilizing Linear Regression, Polynomial Regression, Random Forest, and Gradient Boosting for Accurate Sales and Demand Prediction. International Journal of HRM and Organizational Behavior, 11(3), 11-26.

[11] Varun, P., & Ashokkumar, K. (2022). Intrusion detection system in cloud security using deep convolutional network. Appl. Math. Inf. Sci, 16(4), 581-588.

[12] Poovendran, A. (2023). AI-Powered Data Processing for Advanced Case Investigation Technology. Journal of Science and Technology, 8(08), ISSN: 2456-5660.

[13] Krishnamoorthy, N., & Umarani, S. (2023). Implementation and management of cloud security for industry 4. O-data using hybrid elliptical curve cryptography. The Journal of High Technology Management Research, 34(2), 100474.

[14] Sitaraman, S. R. (2023). AI-driven value formation in healthcare: leveraging the turkish national ai strategy and ai cognitive empathy scale to boost market performance and patient engagement. International Journal of Information Technology and Computer Engineering, 11(3), 103-116.

[15] Shaikh, N. S., Yasin, A., & Fatima, R. (2022). Ontologies as building blocks of cloud security. International Journal of Information Technology and Computer Science, 14(3), 52-61.

[16] Bobba, J. (2023). Cloud-Based Financial Models: Advancing Sustainable Development in Smart Cities. International Journal of HRM and Organizational Behavior, 11(3), 27-43.

[17] Gopinath, N., & Prayla Shyry, S. (2022). Enhancing the cloud security using side channel attack free QKD with entangled fuzzy logic. Journal of Intelligent & Fuzzy Systems, 43(6), 8359-8369.

[18] Kodadi, S. (2023). Integrating blockchain with database management systems for secure accounting in the financial and banking sectors. Journal of Science and Technology, 8(9).

[19] Ofili, B. T., Obasuyi, O. T., & Akano, T. D. (2023). Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. Int J Comput Appl Technol Res, 12(9), 17-31.

[20] Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IoT data sharing. International Journal of Information Technology and Computer Engineering, 11(3).

[21] Alam, T. (2021). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 108-115.

[22] Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog computing-based optimized and secured IoT data sharing using CMA-ES and firefly algorithm with DAG protocols and federated Byzantine agreement. International Journal of Engineering & Science Research, 13(1), 117–132.

[23] Loai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 33(7), 810-819.

[24] Jadon, R., Srinivasan, K., Chauhan, G. S., & Budda, R. (2023). Optimizing software AI systems with asynchronous advantage actor-critic, trust-region policy optimization, and learning in partially observable Markov decision processes. ISAR - International Journal of Research in Engineering Technology, 8(2).

[25] Samriya, J. K., Chakraborty, C., Sharma, A., Kumar, M., & Ramakuri, S. K. (2023). Adversarial ML-based secured cloud architecture for consumer Internet of Things of smart healthcare. IEEE Transactions on Consumer Electronics, 70(1), 2058-2065.

[26] Yallamelli, A. R. G., Ganesan, T., Devarajan, M. V., Mamidala, V., Yalla, R. M. K., & Sambas, A. (2023). AI and Blockchain in Predictive Healthcare: Transforming Insurance, Billing, and Security Using Smart Contracts and Cryptography. International Journal of Information Technology and Computer Engineering, 11(2), 46-61.

[27] Jangampeta, S. (2023). Cloud-based SIEM data security: Challenges and best practices for protecting information in the cloud. International Journal of Computer Engineering and Technology (IJCET), 14(01), 48-52.

[28] Gudivaka, R. L., Gudivaka, B. R., Gudivaka, R. K., Basani, D. K. R., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2023). Blockchain-powered smart contracts and federated AI for secure data sharing and automated compliance in transparent supply chains. International Journal of Management Research & Review, 13(4), 34–49.

[29] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal of medicine and life, 14(4), 448.

[30] Deevi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2023). Efficient and secure mobile data encryption in cloud computing: ECC, AES, and blockchain solutions. International Journal of Engineering Research and Science & Technology, 19(2).

[31] Lv, Z., & Lou, R. (2022). Edge-fog-cloud secure storage with deep-learning-assisted digital twins. IEEE Internet of Things Magazine, 5(2), 36-40.

[32] Garikipati, V., Ubagaram, C., Dyavani, N. R., Jayaprakasam, B. S., & Hemnath, R. (2023). Hybrid AI models and sustainable machine learning for eco-friendly logistics, carbon footprint reduction, and green supply chain optimization. Journal of Science and Technology, 8(12), 230–255.

[33] Raju, K., Ramshankar, N., Shathik, J. A., & Lavanya, R. (2023). Blockchain assisted cloud security and privacy preservation using hybridized encryption and deep learning mechanism in iot-healthcare application. Journal of Grid Computing, 21(3), 45.

[34] Pulakhandam, W., & Pushpakumar, R. (2019). AI-driven hybrid deep learning models for seamless integration of cloud computing in healthcare systems. International Journal of Applied Science Engineering and Management, 13(1).

[35] Tahir, M., Sardaraz, M., Mehmood, Z., & Muhammad, S. (2021). CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. International Journal of Cluster Computing, 24(2), 739-752.

[36] Vallu, V. R., & Arulkumaran, G. (2019). Enhancing compliance and security in cloud-based healthcare: A regulatory perspective using blockchain and RSA encryption. Journal of Current Science, 7(4).

[37] Govindarajan, V., Sonani, R., & Patel, P. S. (2023). A Framework for Security-Aware Resource Management in Distributed Cloud Systems. Academia Nexus Journal, 2(2).

[38] Ganesan, S., & Mekala, R. (2019). AI-driven drug discovery and personalized treatment using cloud computing. International Journal of Applied Science Engineering and Management, 13(3).

[39] Pasham, S. D. (2021). Graph-Based Models for Multi-Tenant Security in Cloud Computing. International Journal of Modern Computing, 4(1), 1-28.

[40] Musam, V. S., & Rathna, S. (2019). Firefly-optimized cloud-enabled federated graph neural networks for privacy-preserving financial fraud detection. International Journal of Information Technology and Computer Engineering, 7(4).

[41] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering, 29(1), 223-246.

[42] Musham, N. K., & Aiswarya, R. S. (2019). Leveraging artificial intelligence for fraud detection and risk management in cloud-based e-commerce platforms. International Journal of Engineering Technology Research & Management, 3(10)

[43] Shukla, A., Katt, B., & Yamin, M. M. (2023). A quantitative framework for security assurance evaluation and selection of cloud services: a case study. International Journal of Information Security, 22(6), 1621-1650.

[44] Radhakrishnan, P., & Padmavathy, R. (2019). Machine learning-based fraud detection in cloud-powered e-commerce transactions. International Journal of Engineering Technology Research & Management, 3(1).

[45] Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-based intrusion detection approach using machine learning techniques. Big Data Mining and Analytics, 6(3), 311-320.

[46] Gattupalli, K., & Purandhar, N. (2019). Optimizing customer retention in CRM systems using AI-powered deep learning models. International Journal of Multidisciplinary and Current Research, 7 (Sept/Oct 2019 issue).

[47] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.

[48] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.

[49] Chavva, M. (2023). AI-Powered Cloud Security: Leveraging Large Language Models for Threat Detection and Risk Mitigation. Australian Journal of Cross-Disciplinary Innovation, 5(5).

[50] Nagarajan, H., & Mekala, R. (2019). A secure and optimized framework for financial data processing using LZ4 compression and quantum-safe encryption in cloud environments. Journal of Current Science, 7(1).

[51] Andrei, B. (2021). Threat modeling of cloud systems with ontological security pattern catalog. International Journal of Open Information Technologies, 9(5), 36-41.

[52] Gollavilli, V. S. B. H., & Arulkumaran, G. (2019). Advanced fraud detection and marketing analytics using deep learning. Journal of Science & Technology, 4(3).

[53] Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), 3587-3608.

[54] Gollapalli, V. S. T., & Padmavathy, R. (2019). AI-driven intrusion detection system using autoencoders and LSTM for enhanced network security. Journal of Science & Technology, 4(4).

[55] Sharma, H. (2021). Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud. ESP

Journal of Engineering & Technology Advancements (ESP-JETA), 1(1), 98-111.

[56] Mandala, R. R., & Hemnath, R. (2019). Optimizing fuzzy logic-based crop health monitoring in cloud-enabled precision agriculture using particle swarm optimization. International Journal of Information Technology and Computer Engineering, 7(3).

[57] Awaysheh, F. M., Aladwan, M. N., Alazab, M., Alawadi, S., Cabaleiro, J. C., & Pena, T. F. (2021). Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management, 69(6), 3676-3693.

[58] Garikipati, V., & Pushpakumar, R. (2019). Integrating cloud computing with predictive AI models for efficient fault detection in robotic software. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(5).

[59] Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks, 9(2), 411-421.

[60] Ayyadurai, R., & Kurunthachalam, A. (2019). Enhancing financial security and fraud detection using AI. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(1).

[61] Anand, K., Vijayaraj, A., & Vijay Anand, M. (2022). An enhanced bacterial foraging optimization algorithm for secure data storage and privacy-preserving in cloud. *Peer-to-Peer Networking and Applications*, *15*(4), 2007-2020.