RESEARCH ARTICLE OPEN ACCESS

EVALUATING THE EFFECTIVENESS OF SECURITY AND ENCRYPTION METHODS FOR CLOUD DATA PROTECTION: APPLICATION TO DATA DIGITIZATION AT HAI PHONG UNIVERSITY

Nguyen Van Quang[1], Hoang Van Lam[1], Tran Bien Thuy[1]
[1]*Faculty of Information Tehcnlogy, Hai Phong University. Haiphong, Vietnam*
Emails: quangnv@dhhp.edu.vn; lamhv@dhhp.edu.vn; thuytb@dhhp.edu.vn

Received: Revised: Accepted: Published:

Abstract – *Digital transformation and data digitization in higher-education institutions raise pressing requirements for protecting data hosted on cloud computing platforms. This paper reports preliminary findings from a university-level research project evaluating three representative encryption approaches — symmetric AES-256, asymmetric RSA-2048, and a hybrid AES+RSA scheme — for protecting digitized records (student, staff, and training documents) at Hai Phong University. Because the university's digitization system is still being deployed, the research team built a simulation model whose baseline performance parameters were calibrated against published benchmarks for AES-NI and RSA-OAEP implementations (see Section 3 and the References) to illustrate the proposed evaluation framework; all figures reported here are simulated data, not measurements from a production system. Simulation results show AES-256-GCM achieving an average throughput of 400–450 MB/s with near-linear scaling; direct RSA-2048 encryption of bulk data incurs rapidly growing processing time and is impractical at scale; the hybrid AES+RSA scheme retains throughput close to pure AES while inheriting RSA's key-management advantages, at a negligible additional storage cost (under 0.1%). Based on these findings, the team recommends adopting a hybrid AES-256/RSA-2048 (or ECC) scheme for the university's data digitization system and proposes empirical validation on live infrastructure as the next research phase*

Keywords *- data encryption; cloud computing; AES; RSA; hybrid encryption; data digitization; information security*

1. Introduction

Digital transformation across Vietnamese universities is driving the storage, processing, and exchange of large volumes of student, faculty, and training records on cloud computing platforms. Alongside the benefits of scalability and reduced operating cost, the cloud model introduces new information-security risks, since data is stored and processed outside the direct physical control of the owning institution [1-3]. Domestic surveys indicate that most existing solutions focus on securing infrastructure (network, virtual machines) rather than encrypting data content directly, while international cloud providers typically offer only default storage-level encryption that is not tailored to the specifics of educational data [4, 5].

Motivated by the ongoing data-digitization effort at Hai Phong University, the university-level research project "Evaluating the Effectiveness of Security and Encryption Methods for Cloud Data Protection" aims to compare representative encryption algorithms and propose suitable application scenarios. This paper presents the theoretical foundation, evaluation methodology, and preliminary simulation results, laying the groundwork for a subsequent empirical phase on the university's live infrastructure.

2. Theoretical Background

2.1. Symmetric Encryption — AES

The Advanced Encryption Standard (AES), published by NIST in 2001, is a block cipher that uses the same secret key for both encryption and decryption. With a 256-bit key length and the Galois/Counter Mode (GCM) of operation, AES-256-GCM provides both confidentiality and integrity (authenticated encryption) without requiring a separate mechanism. Hardware acceleration via the AES-NI instruction set on most modern processors gives AES high throughput and low latency, making it well suited to bulk encryption [6, 12].

2.2. Asymmetric Encryption — RSA

RSA relies on a public/private key pair whose security is based on the difficulty of factoring large integers. It enables key exchange and identity authentication without a pre-shared secret, but its processing speed is orders of magnitude lower than symmetric algorithms, and each encryption operation is limited to a small plaintext block (bounded by key length and

OAEP padding), making RSA unsuitable for direct encryption of large data volumes [7, 8].

2.3. Hybrid Encryption

A hybrid scheme combines the strengths of both algorithm classes: bulk data is encrypted with a randomly generated AES session key, which is then encrypted with the recipient's RSA public key and transmitted alongside the ciphertext. This preserves AES's high throughput while leveraging RSA's secure key-management and distribution properties, and is the model widely adopted in TLS/SSL and commercial cloud security protocols [9, 10].

2.4. Homomorphic Encryption and Future Directions

Homomorphic encryption allows computations to be performed directly on encrypted data without intermediate decryption, enabling processing of sensitive data in the cloud without exposing plaintext content to the service provider. Given its still-high computational cost, this technique was not included in the quantitative simulation of this paper and is identified as a direction for future work [11-13].

3. Research method and Simulation model

At the current stage, the university's data-digitization system is still being deployed, so direct measurement on a production environment is not yet feasible. To illustrate the evaluation framework proposed in the project outline (encryption/decryption time, throughput, storage overhead, CPU utilization), the research team built a numerical simulation model whose baseline parameters for each algorithm were calibrated to typical published performance figures for AES-NI and RSA-OAEP, with random noise added to reflect realistic variation.

It should be stated explicitly: all figures presented in Section 4 are simulated data, disclosed transparently for the purpose of illustrating the methodology; they are not measurements from an empirical test on Hai Phong University's live infrastructure.

3.1. Simulation Configuration

- **Algorithms compared:** AES-256-GCM; RSA-2048-OAEP (direct encryption); hybrid AES-256 + RSA-2048.
- **Test data sizes:** 1, 10, 50, 100, 250, and 500 MB, representing digitized record types from single documents to large data bundles.
- **Evaluation metrics:** encryption/decryption time (ms), throughput (MB/s), additional storage overhead (%), CPU utilization (%).
- **Simulation repetitions:** 30 runs per configuration, averaged to reduce random noise

4. Results and Discussion

4.1. Processing Time and Throughput

Table 1 summarizes the simulated encryption/decryption time and throughput of AES-256-GCM and the hybrid AES+RSA scheme across the surveyed data sizes.

Table 1. Simulated processing time and throughput — AES-256-GCM and hybrid AES+RSA

Size (MB)	AES Encrypt (ms)	AES Decrypt (ms)	AES Throughput (MB/s)	Hybrid Encrypt (ms)	Hybrid Decrypt (ms)	Hybrid Throughput (MB/s)
1	4.92	4.69	203.3	8.41	45.48	118.9
10	25.99	24.86	384.7	28.98	60.42	345
50	118.03	113.53	423.6	121.15	158.14	412.7
100	236.91	223.21	422.1	235.77	259.14	424.2
250	598	535.02	418.1	615.72	591.51	406
500	1220.35	1108.05	409.7	1192.87	1093	419.2

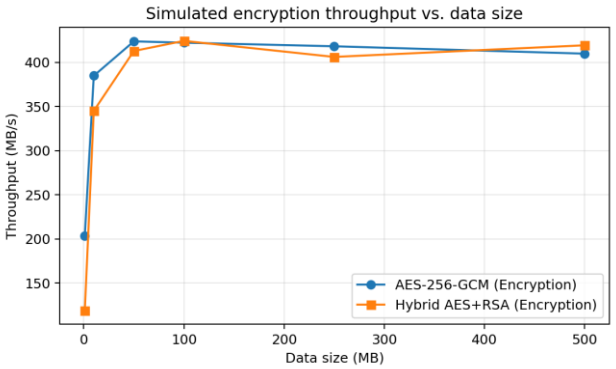

Figure 1. Simulated encryption throughput vs. data size

The simulation shows AES-256-GCM maintaining a stable throughput of roughly 400–450 MB/s for data sizes of 50 MB and above, reflecting the near-linear behaviour of symmetric block encryption. The hybrid AES+RSA scheme shows markedly lower throughput on small files (1 MB) due to the fixed cost of the RSA session-key decryption operation (~40 ms), but this gap narrows quickly as data size increases — at 500 MB, hybrid throughput is nearly on par with pure AES (419.2 vs. 409.7 MB/s). This confirms that RSA overhead in the hybrid scheme is a one-time, per-session cost that does not scale with data volume.

4.2. Storage Overhead and CPU Utilization

Table 2. Simulated storage overhead and CPU utilization

Size (MB)	AES Storage Overhead (%)	Hybrid Storage Overhead (%)	AES CPU (%)	RSA CPU (%)	Hybrid CPU (%)
1	0.043	0.067	35.5	74.5	39.8
10	0.043	0.045	34.5	76.8	39.1
50	0.043	0.044	37	80.9	40.2
100	0.043	0.043	35.5	80.7	40.5
250	0.043	0.043	36.8	82.6	39.7
500	0.043	0.043	38.2	89.6	43.6

The additional storage overhead of AES-GCM (initialization vector and authentication tag) remains stable at roughly 0.043%, negligible relative to the original data volume. The hybrid scheme adds only a single RSA-encrypted session-key block (256 bytes) per file, so its overhead converges toward that of pure AES as file size grows. Regarding CPU utilization, direct RSA-2048 consumes 75–90% of simulated single-core processing capacity — substantially higher than AES (34–38%) or the hybrid scheme (39–44%) — indicating a resource-bottleneck risk if RSA were deployed at scale on shared servers within the digitization system.

4.3. Discussion

Taken together, the simulation results indicate that: (i) AES-256-GCM is well suited to bulk data encryption owing to its high throughput and low resource cost; (ii) RSA-2048 should be reserved for session-key exchange, digital signatures, and authentication rather than direct encryption of large data; and (iii) the hybrid AES+RSA scheme offers a balanced solution appropriate for an educational digitization system that requires both high throughput and secure key management/distribution across multiple units (academic affairs office, student affairs office, faculties). A limitation of this study is that the reported figures are entirely simulation-based, calibrated to reference literature, and do not yet capture real-world factors such as network latency, multi-user system load, or the specific hardware configuration of the university's servers — motivating the empirical phase planned next.

5. Conclusion and Recommendations

This paper presented the theoretical background and preliminary simulated evaluation of three encryption approaches — AES-256, RSA-2048, and a hybrid AES+RSA scheme — for protecting digitized data on cloud infrastructure at Hai Phong University. Results show that the hybrid scheme achieves a favourable balance between performance and secure key management, and it is recommended as the foundational solution for the university's data-digitization system. The team proposes to: (1) conduct empirical measurement on the university's actual cloud infrastructure to validate and calibrate the simulation model; (2) establish a centralized key-management policy combined with role-based access control; (3) further investigate homomorphic encryption for operations requiring processing of sensitive data without decryption; and (4) compile a unified data-security guideline for use across the university.

References

[1] Ngo Ba Hung, Thai Minh Tuan, Trieu Thanh Ngoan (2021), Cloud Computing Textbook, Can Tho University Publishing House, ISBN 978-604-965-542-5.
[2] Le Dac Nhuong (2018), Data Security Textbook, Vietnam National University, Hanoi Press.
[3] Pham Huy Dien, Ha Huy Khoai (2004), Information Encryption: Mathematical Foundations and Applications, VNU Hanoi Press.
[4] Ghonge M.M., Pramanik S., Mangrulkar R., Le D.-N. (2022), Cyber Security and Digital Forensics, Wiley, ISBN 9781119795636.
[5] Le D.-N., Bhatt C., Madhukar M. (2019), Security Designs for the Cloud, IoT, and Social Networking, Wiley, ISBN 9781119592266.
[6] Gudimetla S.R. (2024), "Data Encryption in Cloud Storage".
[7] Hossain M., Sharma V. (2024), "Data Security in the Cloud Using pTree-based Homomorphic Intrinsic Data Encryption System (pHIDES)".
[8] Blessing M. (2024), "Cloud Encryption Strategies and Key Management".
[9] Dhinakaran, D., Selvaraj, D., Dharini, N., Raja, S. E., & Priya, C. (2024). Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution. *arXiv preprint arXiv:2407.18923*.
[10] Mukhopadhyay D. et al. (2014), "Securing the Data in Clouds with Hyperelliptic Curve Cryptography".
[11] NIST FIPS 197 (2001), Advanced Encryption Standard (AES).
[12] RSA Laboratories, PKCS #1 v2.2: RSA Cryptography Standard.
[13] Van, T. H., Vinh, N. P., Ngan, V. T. T., Phuong, L. H., & Le, D. N. (2026). A Course-Specific Agentic RAG Chatbot for IT Student Support: Architecture, Local Deployment, and Preliminary Evaluation at Hai Phong University. *Next-Generation Computing Systems and Technologies*, *2*(2), 21-34.