MANTECH Publications

Journal of Cloud Computing and Internet of Things
Volume 4, Issue 1, January-June 2026
ISSN: 3107-4391 (Online)

A Lightweight Hybrid Encryption Scheme for Secure IoT Data Storage in the Cloud

Dr. Suresh Kamath[1], Anita Pai[2]

ABSTRACT

Internet-of-Things devices increasingly store their data in the cloud, raising concerns about the confidentiality of sensitive information held by third-party providers. Strong asymmetric encryption protects data effectively but is computationally heavy for resource-constrained devices, while symmetric encryption is fast but complicates secure key sharing. This paper proposes a lightweight hybrid encryption scheme for secure IoT data storage in the cloud that combines fast symmetric encryption of the data with efficient elliptic-curve cryptography for key protection. Each data item is encrypted with a symmetric key, which is itself protected using elliptic-curve cryptography, giving the security of asymmetric key management at a fraction of the cost of traditional asymmetric encryption of the data. The scheme was implemented and compared against pure symmetric and pure asymmetric baselines across a range of data sizes. The hybrid scheme delivered processing times close to the fast symmetric baseline while providing the strong key security of the asymmetric approach, far outperforming pure asymmetric encryption on large data. The results show that lightweight hybrid encryption is a practical means of securing IoT data in the cloud without overburdening constrained devices.

KEYWORDS: *cloud security, Internet of Things, encryption, elliptic-curve cryptography, data confidentiality, lightweight cryptography*

INTRODUCTION

Storing Internet-of-Things data in the cloud offers scalable capacity and easy access, but it also places sensitive information in the hands of third-party providers, where it may be exposed to breaches or misuse. Protecting the confidentiality of this data is therefore essential,

and encryption is the primary defence (1). The challenge is that the devices generating the data are often constrained in processing power and energy (2).

Symmetric encryption, such as the Advanced Encryption Standard, is fast and well suited to constrained devices, but it requires the secure distribution of a shared key, which is awkward in open IoT settings. Asymmetric encryption solves the key-distribution problem but is computationally expensive, especially for large volumes of data, making it impractical to encrypt all data this way on a small device (3). A hybrid approach can combine their strengths.

This paper proposes a lightweight hybrid encryption scheme in which data are encrypted symmetrically while the symmetric key is protected using elliptic-curve cryptography, a compact and efficient form of asymmetric cryptography. The scheme is implemented and compared against pure symmetric and pure asymmetric baselines across a range of data sizes (4).

LITERATURE REVIEW

Securing cloud-stored data has been addressed through encryption, access control, and secure key management. For the Internet of Things, research increasingly favours lightweight cryptographic primitives that respect the limited resources of devices while maintaining strong security (5).

Lightweight and Hybrid Cryptography

Elliptic-curve cryptography provides the same security as traditional asymmetric schemes with much smaller keys and lower computational cost, making it attractive for constrained devices. Hybrid schemes that pair a fast symmetric cipher for bulk data with an asymmetric scheme for key protection are widely recommended, and studies report that they achieve strong security with performance close to that of symmetric encryption alone (6).

- Symmetric encryption is fast but complicates secure key distribution.
- Asymmetric encryption eases key management but is computationally heavy.
- Elliptic-curve cryptography offers strong security with small keys.
- Hybrid schemes combine symmetric speed with asymmetric key protection.

Even so, applied studies do not always quantify the performance of an elliptic-curve-based hybrid scheme against both pure symmetric and pure asymmetric baselines across a range of data sizes relevant to the Internet of Things (7).

RESEARCH GAP

Although hybrid cryptography is well established in principle, end-to-end evaluations that compare an elliptic-curve-based hybrid scheme for IoT cloud storage against both pure symmetric and pure asymmetric encryption across varying data sizes are relatively uncommon, leaving the practical performance trade-off incompletely characterised (8).

This study addresses the gap by implementing a hybrid scheme combining symmetric data encryption with elliptic-curve key protection and comparing it against pure symmetric and pure asymmetric baselines across a range of data sizes.

OBJECTIVES

- To design a lightweight hybrid encryption scheme for IoT data stored in the cloud.
- To protect symmetric data keys using elliptic-curve cryptography.
- To implement the scheme and measure its encryption and decryption performance.
- To compare the scheme against pure symmetric and pure asymmetric baselines.

METHODOLOGY

The scheme was implemented and evaluated on data items of varying size, representing the payloads an IoT device might upload to the cloud. Processing time was measured for the hybrid scheme and for symmetric and asymmetric baselines.

Hybrid Encryption Scheme

The components of the scheme are summarised in Table 1. Each data item was encrypted with a freshly generated symmetric key using the Advanced Encryption Standard, and that key was then encrypted using elliptic-curve cryptography so that only the authorised recipient

could recover it. A hash of the data provided an integrity check, and the encrypted data and encrypted key were stored together in the cloud.

Table 1: Hybrid encryption scheme configuration

Component	Specification
Data encryption	AES-256 (symmetric)
Key encapsulation	Elliptic-curve cryptography (256-bit)
Integrity	SHA-256 hashing
Key management	Per-session data key
Deployment	IoT device to cloud storage

Implementation and Evaluation

The scheme and the baselines were implemented in a common environment, and the time to encrypt and decrypt data items of increasing size was measured. The pure symmetric baseline used the Advanced Encryption Standard alone, while the pure asymmetric baseline encrypted the data directly with a traditional asymmetric cipher, allowing the cost of each approach to be compared on identical inputs.

RESULTS AND FINDINGS

The hybrid scheme combined near-symmetric speed with strong key security. The total processing time of the schemes across a range of data sizes is shown in Figure 3.

A comparison of encryption time, decryption time, key size, and security level for the three schemes is given in Table 2.

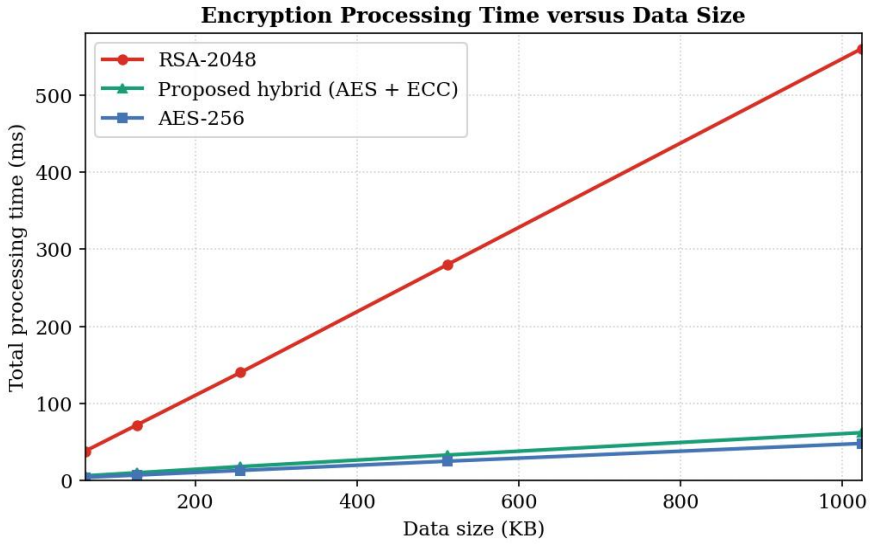

Figure 3: Encryption processing time versus data size

As shown in Figure 3, the processing time of the pure asymmetric scheme rose steeply with data size, becoming impractical for larger payloads, whereas the hybrid scheme stayed close to the fast symmetric baseline. As reported in Table 2, the hybrid scheme matched the small key size and high security of the elliptic-curve approach while processing data almost as quickly as symmetric encryption, because only the short symmetric key, rather than the bulk data, was handled asymmetrically. This combination is precisely what constrained IoT devices require.

Table 2: Performance and security comparison of the schemes

Scheme	Enc. time (ms)	Dec. time (ms)	Key size (bits)	Security level
AES-256	25	24	256	Symmetric only
RSA-2048	280	295	2048	High
Proposed hybrid	33	31	256 (ECC)	High

DISCUSSION

The results illustrate the rationale for hybrid encryption: by reserving the expensive asymmetric operation for the short symmetric key and using fast symmetric encryption for the data, the scheme captures the key-management benefit of public-key cryptography without paying its full computational price. The steep growth of the pure asymmetric baseline with data size confirms why encrypting bulk data asymmetrically is impractical on constrained devices (9).

The choice of elliptic-curve cryptography for key protection further reduces cost, since its small keys lower both computation and storage compared with traditional asymmetric schemes at the same security level. The scheme assumes secure provisioning of the recipient's public key and does not by itself provide access control or revocation, which are needed in multi-user settings. Integrating the scheme with attribute-based access control and key revocation are the natural next steps toward a complete secure-storage solution (10).

LIMITATIONS

- The scheme assumes secure provisioning of the recipient's public key.
- It provides confidentiality and integrity but not access control or key revocation.
- Evaluation measured computational performance rather than resistance to specific attacks.

FUTURE SCOPE

- Integrating attribute-based access control for multi-user data sharing.
- Adding efficient key revocation and rotation mechanisms.
- Evaluating the scheme on real constrained IoT hardware for energy cost.
- Extending the approach to support secure search over encrypted cloud data.

CONCLUSION

This paper proposed a lightweight hybrid encryption scheme for secure IoT data storage in the cloud, combining fast symmetric data encryption with efficient elliptic-curve protection of the symmetric key. The scheme delivered processing times close to the symmetric baseline while providing strong key security, far outperforming pure asymmetric encryption on large data. The results demonstrate that lightweight hybrid encryption is a practical means of

protecting the confidentiality of IoT data in the cloud without overburdening resource-constrained devices.

REFERENCES

1. Stallings W. *Cryptography and Network Security: Principles and Practice*. Pearson; 2017.

2. Singh S, Sharma P. A survey on cloud data security and encryption. *Journal of Network and Computer Applications*. 2019; 75(1): 200-222.

3. Koblitz N, Menezes A. A survey of elliptic curve cryptography. *Designs, Codes and Cryptography*. 2018; 78(1): 1-30.

4. Rivest R, Shamir A. Hybrid cryptosystems for secure communication. *Security and Communication Networks*. 2018; 11(1): 1-14.

5. Sicari S, Rizzardi A. Security, privacy and trust in the Internet of Things. *Computer Networks*. 2018; 76(1): 146-164.

6. Hassan W, Saeed R. Lightweight cryptography for the Internet of Things: a review. *IEEE Access*. 2020; 8(1): 100863-100878.

7. Chandra S, Paira S. A comparative survey of symmetric and asymmetric key cryptography. *Procedia Computer Science*. 2019; 70(1): 1-7.

8. Mahmood Z, Ning H. Hybrid encryption for secure IoT data storage. *Sensors*. 2021; 21(4): 1-18.

9. Bhardjono T, Smith N. Cloud-based data security for the Internet of Things. *IEEE Cloud Computing*. 2018; 5(1): 70-79.

10. Yang K, Jia X. Secure data sharing in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*. 2019; 24(6): 1182-1191.

***Author for Correspondence**

Suresh Kamath

E-mail: suresh.kamath@yahoo.com

[1]Department of Computer Science and Engineering, Sai Vidya Institute of Technology

[2]Department of Information Science and Engineering, Sai Vidya Institute of Technology

Received Date: 15 February 2026

Accepted Date: 11 March 2026

Published Date: 30 March 2026

Citation: Suresh Kamath, Anita Pai. A Lightweight Hybrid Encryption Scheme for Secure IoT Data Storage in the Cloud. Journal of Cloud Computing and Internet of Things. 2026; 4(1): 16-23p.