ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Enhanced Secure Storage Architecture for IAAS Cloud Environments

Yahaya Coulibaly[1], Ouedraogo Paloute Karim Charlemagne[2], Ouedraogo Yann Christian Florian[2], Alfadoulou Abdoulahi[1]

[1]Research and Innovation Centre, Agency for Information and Communication Technology (AGETIC), Bamako, Mali

[2]Higher School of Computer Science, University Nazi Boni, Bobo-Dioulasso, Burkina Faso

***Corresponding Author**

***ORCID: 0000-0002-5940-3168**

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150700103

Received: 01 August 2026; Accepted: 06 August 2026; Published: 18 August 2026

ABSTRACT

The growing adoption of Cloud Computing has profoundly transformed the management of IT infrastructures by providing flexible, scalable, and on-demand accessible resources. Among the various cloud computing service models, Infrastructure as a Service (IaaS) enables organizations to outsource their computing, networking, and storage resources to cloud providers. However, this outsourcing raises significant security concerns, particularly regarding the confidentiality, integrity, and availability of stored data. This paper presents an analytical study of storage security techniques in IaaS environments and examines the main threats that may affect data hosted in the cloud, including unauthorized access, misconfigurations, insider threats, and cyber attacks. Particular attention is given to cryptographic mechanisms used to protect data, including symmetric, asymmetric, and hybrid encryption techniques, as well as client-side and server-side encryption approaches. Based on this analysis, an enhanced secure storage architecture is proposed. This architecture relies on three main techniques: client-side data encryption using AES-256, encryption key protection through RSA, and the use of a Key Management System (KMS). It also incorporates secure communication protocols and enhanced authentication mechanisms. The objective is to ensure effective data protection while preserving the advantages provided by cloud infrastructures. The results of this study highlight the importance of combining robust encryption techniques, secure key management, and appropriate access control mechanisms to strengthen trust in cloud storage solutions. Finally, emerging approaches such as homomorphic encryption and Zero Trust architectures are presented as promising directions for future developments in cloud security.

Keywords: Cloud Computing, Infrastructure as a Service (IaaS), Cloud Storage Security, Data Encryption, AES-256, RSA, Key Management System (KMS), Zero Trust Architecture.

INTRODUCTION

The rise of Cloud Computing has profoundly transformed the way organizations design, deploy, and operate their IT infrastructures. Through its on-demand resource provisioning model, cloud computing enables enterprises to access computing, storage, and networking capabilities without the need to invest in costly physical infrastructures [1]. Among the various service models offered, Infrastructure as a Service (IaaS) represents the fundamental layer upon which many digital applications and platforms are built. This model provides significant flexibility, high scalability, and a substantial reduction in operational costs associated with infrastructure management.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

However, migrating data to outsourced cloud environments raises significant security concerns [2]. In a context where storage resources are generally shared among multiple customers, organizations lose part of the direct control they traditionally exercised over their data. This situation increases the risks associated with unauthorized access, sensitive information leakage, misconfigurations, insider threats, and attacks targeting storage infrastructures. Therefore, protecting stored data has become a major challenge for both cloud service providers and their customers.

Faced with these challenges, the central research question addressed in this work is: ***how can the confidentiality, integrity, and availability of data stored in a Cloud IaaS environment be ensured?*** This issue is particularly critical because the trust placed in cloud services strongly depends on their ability to guarantee the security of hosted information.

The objective of this paper is to analyse the main risks associated with data storage in IaaS environments and to investigate protection mechanisms capable of mitigating these risks. Particular attention is given to modern cryptographic techniques, including symmetric, asymmetric, and hybrid encryption, as well as key management and access control mechanisms. Based on this analysis, a secure storage architecture is proposed to enhance data protection throughout its entire lifecycle.

To achieve these objectives, a two-phase methodological approach is adopted. The first phase consists of a state-of-the-art study covering the fundamental concepts of cloud computing, threats affecting cloud storage, and the various encryption technologies used in this context. The second phase focuses on the design of a secure storage architecture integrating encryption, authentication, and key management mechanisms tailored to IaaS environments. The remainder of this paper is organized as follows: **Section II** presents the state of the art related to IaaS cloud storage security and the main encryption techniques. **Section III** describes the proposed secure storage architecture and its operational mechanisms. **Section IV** discusses the advantages, limitations, and potential improvements of the proposed solution. Finally, **Section V** concludes the paper and outlines future research directions.

LITERATURE REVIEW: SECURITY OF IAAS CLOUD STORAGE

Threats to cloud storage

Data Breach: Exposure of sensitive data to unauthorized third parties due to logical vulnerabilities, security weaknesses, or malicious attacks [3].

Misconfiguration: Critical human errors, such as the unintended public exposure of object storage repositories (e.g., publicly accessible S3 buckets), which represent one of the leading causes of cloud security breaches [4].

Insider Threats: Risks originating from malicious or compromised insiders, such as cloud provider employees or internal administrators with elevated privileges, who may improperly access or misuse stored data [5].

Cloud Ransomware: A category of malware specifically targeting cloud environments and APIs to encrypt an organization's stored data without authorization and demand ransom payments for data recovery [5].

Unauthorized Access: Compromise of user credentials or privilege escalation that enables attackers to bypass security policies and gain unauthorized access to exfiltrate, modify, or destroy sensitive data [3].

Cloud encryption techniques

Encryption represents the ultimate line of defense for data protection. Even if perimeter-based access controls fail, properly encrypted data remains completely unusable to attackers without the appropriate decryption keys.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Symmetric Encryption: This mechanism relies on the use of a single shared secret key for both encryption and decryption operations. The most widely adopted and recognized standard algorithm is the Advanced Encryption Standard (AES), typically implemented with 256-bit keys (AES-256). Its main strength lies in its exceptional execution speed and low CPU overhead, making it particularly suitable for encrypting large volumes of data in real time, such as virtual disks and cloud storage volumes [6].

Asymmetric Encryption

Asymmetric encryption relies on a pair of mathematically linked keys: a public key, which can be freely distributed and is used for encryption, and a private key, which must be securely protected and is used for decryption. Traditional algorithms such as RSA, as well as more recent approaches such as Elliptic Curve Cryptography (ECC), belong to this category. ECC provides the advantage of achieving security levels comparable to RSA while using significantly shorter key sizes, thereby reducing computational overhead and improving processing efficiency. However, asymmetric encryption remains computationally expensive and is therefore unsuitable for directly encrypting large volumes of data [7], [8].

Hybrid Encryption

Hybrid encryption represents the dominant approach in modern cloud security architectures. It combines the high performance of symmetric encryption with the flexible key management capabilities of asymmetric encryption. In practice, through a mechanism commonly known as Envelope Encryption, large data objects are encrypted using a symmetric key called the Data Encryption Key (DEK). The DEK is then encrypted using an asymmetric key or a centrally managed master key known as the Key Encryption Key (KEK). This approach enables centralized key governance and secure key lifecycle management without requiring the movement of the encrypted data itself [9].

Homomorphic Encryption

Homomorphic encryption is considered a cutting-edge cryptographic technology that enables mathematical computations and analytical operations to be performed directly on encrypted data, without requiring prior decryption in memory. Although highly promising for ensuring strong confidentiality protection during the processing of extremely sensitive information, such as medical or financial data, its widespread adoption remains limited due to its extremely high computational cost and significant performance overhead [10], [11].

Client-side encryption vs. Server-side encryption

The main distinction between client-side and server-side encryption lies in the location where the cryptographic operations are performed.

Server-Side Encryption (SSE): The encryption process is transparently handled by the cloud service provider (e.g., AWS SSE-S3). Data is transmitted in plaintext (protected during transmission by **TLS**) to the cloud environment, where it is encrypted before being written to physical storage. The cloud provider owns or manages the encryption keys, depending on the selected key management model [12].

Client-Side Encryption (CSE): Data is encrypted locally within the client's infrastructure before being transmitted to the cloud. The cloud provider receives and stores only opaque encrypted data blocks and never has access to the decryption keys. This approach represents a strong implementation of the Zero Trust security model, as data confidentiality remains under the exclusive control of the data owner [13].

THE PROPOSED ENHANCED SECURE ARCHITECTURE

Architecture Objectives

The proposed architecture aims to satisfy the four fundamental pillars of information security within an IaaS environment, in accordance with the recommendations of ISO/IEC 27001 and the NIST Cyber security Framework (NIST CSF) [14]:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Confidentiality

Ensuring that only authorized entities can access data in plaintext form. This objective is achieved through systematic Client-Side Encryption (CSE) using AES-256-GCM before any data is transmitted to the cloud infrastructure [15].

Integrity

Ensuring that no unauthorized or accidental modification of data can remain undetected. The use of the GCM (Galois/Counter Mode) encryption mode provides built-in authentication through the GMAC authentication tag, complemented by SHA-256 hash values computed for each data block to guarantee integrity verification [15].

Authentication

Verifying the identity of every user or service accessing the data. The system relies on an Identity and Access Management (IAM) framework [16], implementing the principle of least privilege and reinforced by mandatory Multi-Factor Authentication (MFA) [16] for all operations involving encryption keys and key management processes [17].

Availability

Ensuring service resilience against failures, disruptions, and potential attacks. The proposed solution incorporates geographical replication of encrypted data and ensures high availability of the Key Management System (KMS) through an active-active clustering architecture [18].

Description of the proposed architecture

The proposed architecture is based on a Client-Side Encryption (CSE) approach [13] combined with an Envelope Encryption mechanism using dynamic key derivation (KD-KEK) [17]. It is designed to ensure the confidentiality, integrity, and data sovereignty of user information stored in the cloud, while enabling secure and transparent access through the application layer. The main components of the proposed architecture are described as follows:

End User

The end user connects exclusively to the Backend Application through a secure communication channel (HTTPS/TLS 1.3). The user does not directly interact with the IAM, KMS, or cloud storage components.

Backend Application

The Backend Application represents the central component of the proposed architecture. It acts as the encryption and decryption client and manages secure interactions with the following components:

IAM (Identity and Access Management): Used for user authentication and for authenticating the backend application itself as a trusted Service Account.

KMS + HSM (Key Management System + Hardware Security Module): Used for all key derivation, encryption, and decryption operations involving Data Encryption Keys (DEKs) [17], [19].

Cloud Storage: Used for storing and retrieving encrypted data objects, including the ciphertext and the encrypted DEK (eDEK) [20].

IAM (Identity and Access Management)

The IAM component provides centralized authentication and authorization services. It establishes secure

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

relationships with: The Backend Application through OIDC/OAuth2 protocols for user and service authentication. The KMS for validating access tokens and authorizing cryptographic operations requested by the application.

KMS + HSM (Key Management System + Hardware Security Module)

The KMS + HSM component is the critical element responsible for secure cryptographic key management. The Root Master Key (RMK) is physically protected inside the HSM and never leaves the secure hardware environment [19]. The KMS communicates exclusively with the Backend Application through TLS 1.3 with mutual authentication or IAM-based authentication tokens. No direct communication is permitted with the end user or the cloud storage system.

Cloud Storage (e.g., S3, Azure Blob Storage, GCS)

The cloud storage layer stores only encrypted objects, including ciphertext, encrypted DEKs (eDEKs), and associated metadata [20]. Access is exclusively controlled through the Backend Application. The cloud service provider has no visibility into the encryption keys or the original plaintext data, thereby preserving data confidentiality and sovereignty.

Operational workflow of the proposed architecture

The complete operational workflow of the proposed architecture is illustrated in the following **Figures 1, 2, and 3**.

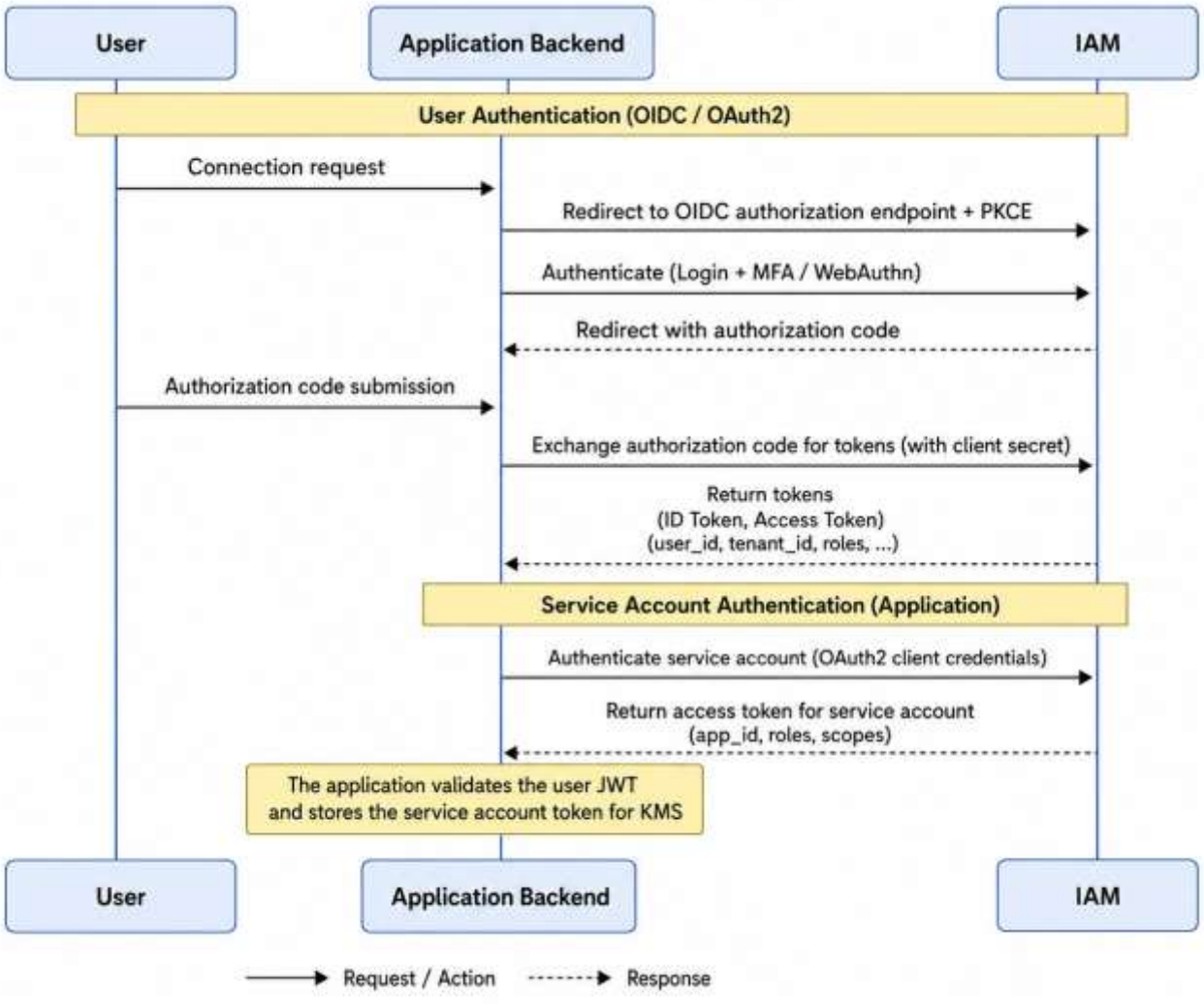
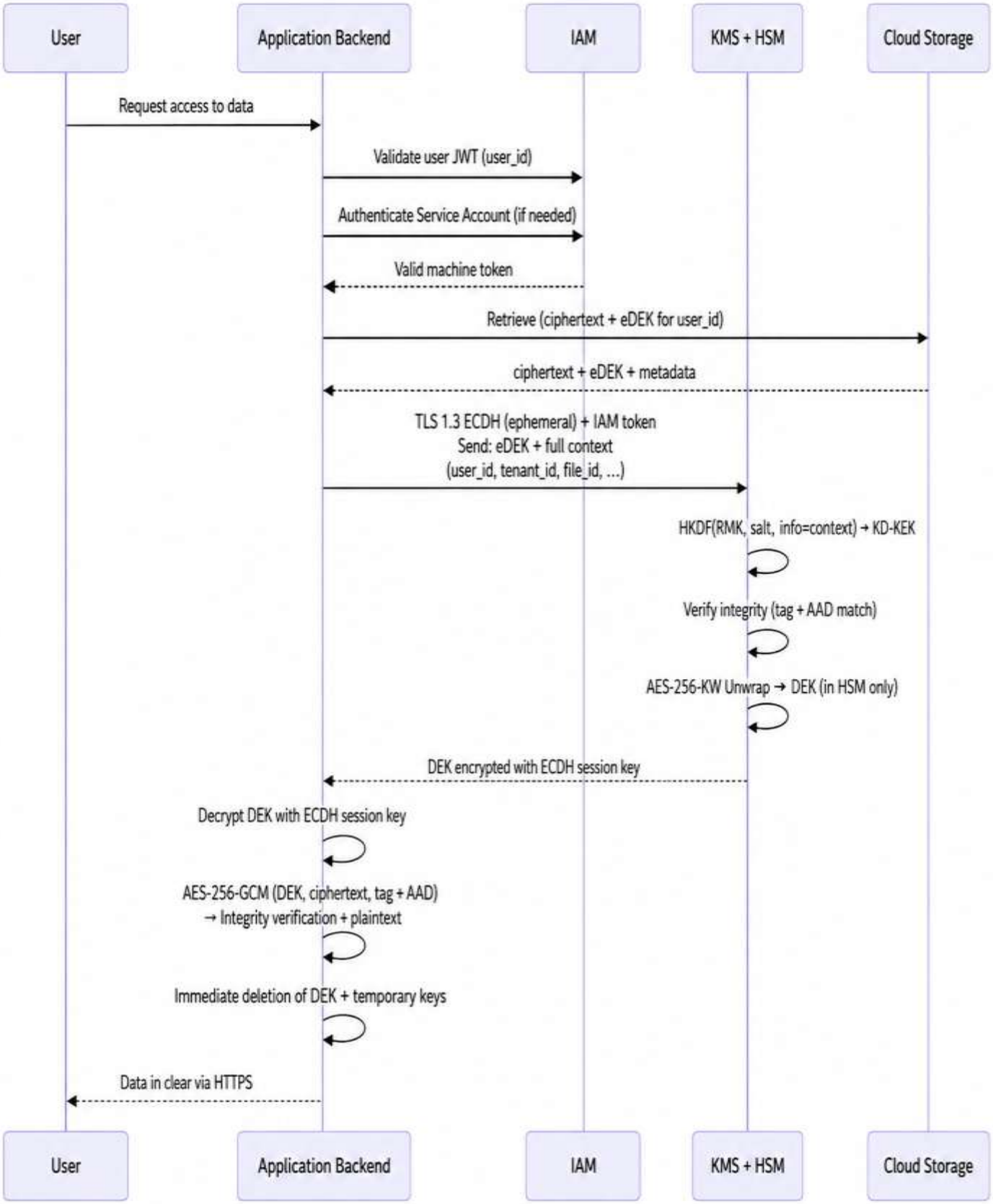


Figure 1. User and Application Authentication Flow with the IAM

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Figure 2. Data Upload Flow to the Cloud



ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

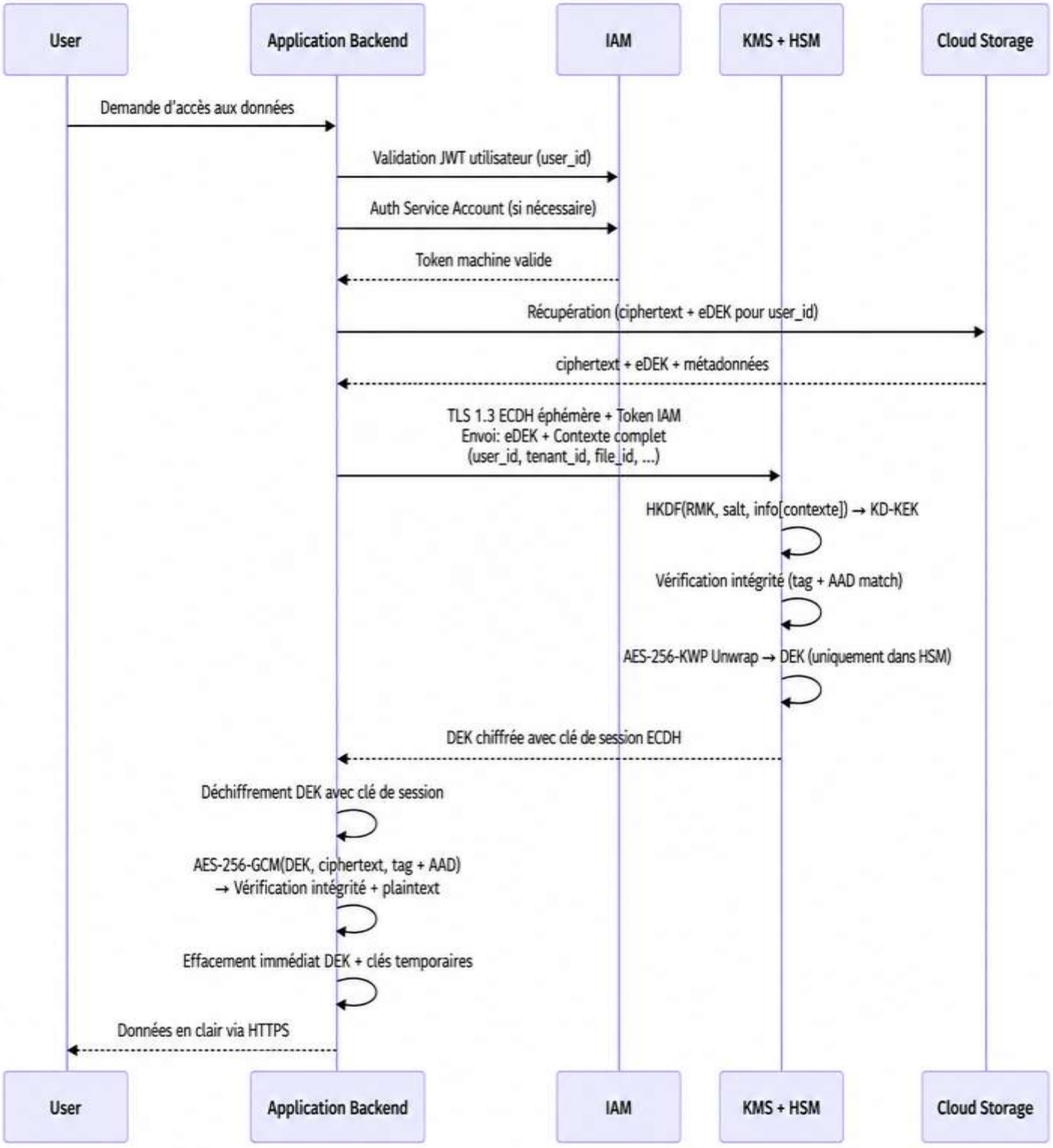


Figure 3. Data Download Flow from the Cloud to the User

DISCUSSION

Analysis of the proposed architecture

The proposed architecture addresses the key security requirements of confidentiality, integrity, authentication, and availability for Cloud IaaS storage environments. The use of AES-256-GCM Client-Side Encryption (CSE) ensures data confidentiality, while integrated authentication mechanisms and SHA-256

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

integrity hashes provide strong protection against unauthorized data modification. The implementation of IAM and MFA strengthens access control and identity verification mechanisms.

Data availability is ensured through encrypted data replication, high availability of the Key Management System (KMS), and the service guarantees provided by the IaaS provider through Service Level Agreements

(SLAs). Overall, the proposed architecture effectively mitigates the risks of unauthorized access, data leakage, and data tampering while preserving user control and data sovereignty in cloud environments.

Comparison with Existing Solutions

The proposed solution combines Client-Side Encryption (CSE) with an enhanced Envelope Encryption mechanism based on dynamic key derivation (KD-KEK). It differs from the conventional approaches adopted by major cloud service providers as follows:

AWS: The SSE-S3 and SSE-KMS mechanisms allow AWS to manage encryption keys, which may limit data sovereignty. Although CSE with AWS KMS provides greater client control, it remains dependent on AWS-

ecosystem. The proposed approach provides greater flexibility through HKDF-based key derivation and HSM independence [21].

Google Cloud

Customer-Managed Encryption Keys (CMEK) and Customer-Supplied Encryption Keys (CSEK) provide customer-controlled encryption capabilities; however, the Root Master Key (RMK) may still involve partial dependence on the cloud provider's infrastructure [22].

Compared with these existing solutions, the proposed architecture provides a higher level of data sovereignty. Even under legal frameworks such as the CLOUD Act [23], the cloud provider cannot access data in plaintext because the root encryption keys remain exclusively stored within the HSM controlled by the organization.

Limitations of the Architecture

Despite its advantages, the proposed architecture presents several limitations:

managed services. The proposed architecture goes further by introducing dynamic key derivation through an HSM-based approach and enabling the use of a potentially self-hosted or multi-cloud KMS environment [9].

Azure:

Azure Key Vault with Bring Your Own Key (BYOK) and Always Encrypted provides a high level of key control and data protection. However, key management often remains tightly integrated with the Microsoft

Operational Complexity

The management of the KMS, HSM, and key derivation context (e.g., *user_id*, *tenant_id*, etc.) increases administrative overhead and requires advanced skills in cryptography and security management [24].

Performance Overhead

Network interactions with the KMS for each encryption and decryption operation introduce additional latency. However, this overhead remains limited when using optimized connections and modern hardware acceleration technologies such as **AES-NI**.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

KMS Dependency

The KMS becomes a critical component of the architecture; any temporary unavailability may prevent access to encrypted data [25].

User Management

In multi-tenant environments, the effective management of key rotation, access revocation, and user lifecycle operations remains a complex challenge.

FUTURE RESEARCH DIRECTIONS

Several improvement directions are considered for future work:

Post-Quantum Resistance

Integration of post-quantum cryptographic algorithms [26], [27] into the KMS infrastructure and secure key exchange mechanisms such as ECDH to enhance long-term security against quantum computing threats.

Automation and Scalability

Development of an orchestration layer to enable automated key rotation, dynamic key lifecycle management, and scalable handling of key derivation contexts.

Database Support

Extension of the proposed architecture to encrypted database systems, including solutions similar to Always Encrypted, with support for encrypted database columns while preserving secure query operations.

Auditing and Traceability

Integration of an immutable logging system and mechanisms for verifying encryption proofs (Proof of Encryption) to improve security auditing, compliance monitoring, and data protection accountability.

CONCLUSION

This paper has presented an application-level encryption architecture that combines Envelope Encryption with dynamic key derivation (KD-KEK) mechanisms protected by an HSM. Through a clear separation of responsibilities among the Backend Application, IAM, KMS, and Cloud Storage components, the proposed solution provides a high level of data confidentiality, integrity, and sovereignty while maintaining transparent and secure user access. The sequence diagrams illustrated the authentication, upload, and download workflows, demonstrating the practical feasibility of the proposed approach. Although more complex to implement than native cloud security solutions, this architecture addresses stringent security and compliance requirements, such as GDPR and HIPAA [11], in the context of increasing cyber threats and evolving international regulations. Future research will focus on enhancing the architecture's post-quantum resistance and simplifying its deployment and management in multi-cloud and multi-tenant environments.

REFERENCES

1. P. Mell et T. Grance, « The NIST Definition of Cloud Computing », National Institute of Standards and Technology, Gaithersburg, MD, Special Publication (NIST SP) 800-145, sept. 2011. doi: 10.6028/NIST.SP.800-145.
2. P. Yang, N. Xiong, et J. Ren, « Data Security and Privacy Protection for Cloud Storage: A Survey », *IEEE Access*, vol. 8, p. 131723-131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

3. « Threat Landscape | ENISA ». Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape
4. « Top Threats to Cloud Computing 2024 | CSA ». Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024
5. « Cloud Security Threats: Top Threats and 3 Mitigation Strategies », Exabeam. Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://www.exabeam.com/explainers/cloud-security/cloud-security-threats-top-threats-and-3-mitigation-strategies/
6. N. I. of S. and Technology, « Advanced Encryption Standard (AES) », U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 197, mai 2023. doi: 10.6028/NIST.FIPS.197-upd1.
7. « RSA and Elliptic Curve Encryption System »:, *Int. J. Inf. Secur. Priv.*, vol. 18, nº 1, janv. 2024, doi: 10.4018/IJISP.340728.
8. M. R. Khan *et al.*, « Analysis of Elliptic Curve Cryptography & RSA », *J. ICT Stand.*, p. 355-378, nov. 2023, doi: 10.13052/jicts2245-800X.1142.
9. « Using server-side encryption with AWS KMS keys (SSE-KMS) - Amazon Simple Storage Service ». Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html
10. K. Munjal et R. Bhatia, « A systematic review of homomorphic encryption and its contributions in healthcare industry », *Complex Intell. Syst.*, p. 1-28, mai 2022, doi: 10.1007/s40747-022-00756-z.
11. J. S. Rauthan, « Homomorphic Encryption in Healthcare Industry Applications for Protecting Data Privacy », 7 janvier 2025, *arXiv*: arXiv:2501.04058. doi: 10.48550/arXiv.2501.04058.
12. « Protecting data with server-side encryption - Amazon Simple Storage Service ». Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html
13. S. Rose, O. Borchert, S. Mitchell, et S. Connelly, « Zero Trust Architecture », National Institute of Standards and Technology, NIST Special Publication (SP) 800-207, août 2020. doi: 10.6028/NIST.SP.800-207.
14. « Cybersecurity Framework », *NIST*, nov. 2013, Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://www.nist.gov/cyberframework
15. M. Dworkin, « Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC », National Institute of Standards and Technology, NIST Special Publication (SP) 800-38D, nov. 2007. doi: 10.6028/NIST.SP.800-38D.
16. « (PDF) IDENTITY AND ACCESS MANAGEMENT (IAM) IN CLOUD SECURITY FRAMEWORKS », ResearchGate. Consulté le: 14 juin 2026. [En ligne]. Disponible sur: https://www.researchgate.net/publication/391270909_IDENTITY_AND_ACCESS_MANAGEMENT_IAM_IN_CLOUD_SECURITY_FRAMEWORKS
17. I. T. L. Computer Security Division, « Key Management Guidelines - Key Management | CSRC | CSRC », CSRC | NIST. Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://csrc.nist.gov/projects/key-management/key-management-guidelines
18. E. Barker, « Recommendation for Key Management: Part 1 – General », National Institute of Standards and Technology, NIST Special Publication (SP) 800-57 Part 1 Rev. 5, mai 2020. doi: 10.6028/NIST.SP.800-57pt1r5.
19. garrodonnell, « How to generate & transfer HSM-protected keys – BYOK – Azure Key Vault ». Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://learn.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-byok
20. « Customer-managed encryption keys (CMEK) | Cloud Key Management Service », Google Cloud Documentation. Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://docs.cloud.google.com/kms/docs/cmek
21. msmbaldwin, « Azure encryption overview ». Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview
22. « Customer-managed encryption keys | Cloud Storage », Google Cloud Documentation. Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://docs.cloud.google.com/storage/docs/encryption/customer-managed-keys

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

23. « Cross-Border Data Sharing Under the CLOUD Act ». Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://www.congress.gov/crs-product/R45173
24. « Demystifying AWS KMS key operations, bring your own key (BYOK), custom key store, and ciphertext portability | AWS Security Blog ». Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://aws.amazon.com/blogs/security/demystifying-kms-keys-operations-bring-your-own-key-byok-custom-key-store-and-ciphertext-portability/
25. « Cloud HSM vs KMS: What's Best for Enterprise Security? », Fortanix. Consulté le: 15 juin 2026. [En ligne]. Disponible sur: https://www.fortanix.com/blog/cloud-hsm-vs-kms-which-is-right-for-your-enterprise-data-security-strategy
26. N. I. of S. and Technology, « Module-Lattice-Based Key-Encapsulation Mechanism Standard », U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 203, août 2024. doi: 10.6028/NIST.FIPS.203.
27. N. I. of S. and Technology, « Module-Lattice-Based Digital Signature Standard », U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 204, août 2024. doi: 10.6028/NIST.FIPS.204.