International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03597
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Use of Cryptography in Cloud Computing: Enhancing Data Security and Privacy

Veerkant Bhaskar, Assistant Professor, Computer Science & Engineering
Mewar University Gangrar, Chittorgarh (Raj.)

Abstract

Strong security measures are now more important than ever to preserve data integrity and confidentiality as cloud computing grows in popularity. In cloud systems, cryptography is a fundamental tool for guaranteeing safe data transport, storage, and access. This study investigates the function of cryptographic methods in cloud computing, looking at key management systems, symmetric and asymmetric encryption, and homomorphic encryption. This study offers a thorough overview of how encryption technologies support data security and handle privacy concerns in distributed systems by examining modern cryptographic solutions and their use in cloud platforms.

Keywords: cloud computing, cryptography, data security, encryption, privacy, public key infrastructure, homomorphic encryption, secure cloud storage

1. Introduction

By providing scalable, on-demand computer resources via the Internet, cloud computing has completely changed how data is stored and accessed. However, there are serious security risks when handing private information to outside cloud service providers (CSPs). To reduce these threats, the science of information security known as cryptography becomes essential. The purpose of this study is to examine how cryptographic methods can be used in cloud computing environments to guarantee data availability, confidentiality, and integrity.

2. Cryptographic Fundamentals in Cloud Computing

2.1 Symmetric Encryption

One key is used for both encryption and decryption in symmetric key cryptography. Its efficiency and speed make it a popular choice for encrypting big datasets in cloud computing. Blowfish and the Advanced Encryption Standard (AES) are examples of popular symmetric algorithms.

2.2 Asymmetric Encryption

A public key for encryption and a private key for decryption are the two keys used in asymmetric cryptography, also known as public-key cryptography. Elliptic Curve Cryptography (ECC) and RSA are extensively used in secure key exchange and cloud authentication systems.

2.3 Hash Functions and Digital Signatures

By transforming data into a fixed-length digest, hashing protects data integrity. Asymmetric cryptography and hashing are used by digital signatures to verify the integrity and validity of data transferred between cloud services.

---

3. Cryptographic Applications in Cloud Computing

3.1 Data-at-Rest Protection

Unauthorized access to data kept on cloud servers is a possibility. Even if data is physically accessed, encryption at rest guarantees that it cannot be decrypted without the right keys.

3.2 Data-in-Transit Protection

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols use cryptography to protect data as it travels between users and cloud servers, guarding against man-in-the-middle attacks and eavesdropping.

3.3 Homomorphic Encryption

Homomorphic encryption maintains confidentiality while processing by allowing computation on encrypted data without the need for decryption. This method works especially well for outsourced computation and cloud analytics that protect privacy.

---

4. Key Management and Access Control

Encrypted cloud data security depends heavily on efficient key management. Public key infrastructure (PKI), key management services (KMS), and hardware security modules (HSMs) are some of the solutions. To guarantee that only authorized users can decrypt data, cryptographic systems integrate access control mechanisms like role-based access control (RBAC).

---

5. Challenges and Limitations

- Cloud computing cryptography has drawbacks despite its benefits:
  • Complexity of key management: It is difficult to safely store and manage cryptographic keys across dispersed systems.
  • Performance overhead: The operations of encryption and decryption may cause latency and lower system effectiveness.

  • Regulatory compliance: Careful implementation is necessary to guarantee that cryptographic methods adhere to international data protection regulations (such as GDPR and HIPAA).

---

6. Future Directions

New cryptographic techniques that show promise for improving cloud security include blockchain-based key management and quantum-resistant algorithms. Research on effective and scalable encryption techniques must continue in order to meet the expanding demands of cloud infrastructures for data protection.

---

7. Conclusion

Cryptography, which offers strong safeguards for data confidentiality, integrity, and access control, is still a crucial part of safe cloud computing. The use of cutting-edge cryptographic algorithms will be essential in protecting user data from changing cyber threats as cloud services grow.

References

1. Tallings, W. (2017). Network Security and Cryptography: Fundamentals and Applications Pearson Education.

2. Lindell, Y., and Katz, J. (2020). An Overview of Contemporary Cryptography. CRC Publishing.

3. "CryptDB: Protecting Confidentiality with Encrypted Query Processing," by R. A. Papa et al. (2011). The 23rd ACM Symposium on Operating Systems Principles Proceedings.

4. NIST (2018). Storage Infrastructure Security Guidelines. The National Institute of Standards and Technology