***R. Yakushevskyi**, BA student*
***O. Mahdiuk**, PhD in Ped., As. Prof*
Khmelnytskyi National University

MODERN METHODS OF DATA ENCRYPTION IN CLOUD COMPUTING SYSTEMS

The rapid evolution of cloud computing has fundamentally transformed the paradigm of data processing and storage for both individuals and large enterprises. However, transferring sensitive information to third-party servers introduces critical security risks, including unauthorized access, data breaches, and loss of control over digital assets. Traditional perimeter defense methods are becoming increasingly ineffective in the face of sophisticated cyber threats and insider attacks. Therefore, robust encryption has become the last and most reliable line of defense in modern cybersecurity.

The relevance of this study is driven by the urgent need to ensure data integrity, availability, and confidentiality in distributed environments, especially for cybersecurity specialists working with hybrid and multi-cloud infrastructures in 2026.

To build a comprehensive security model, it is essential to consider the three states of data in the cloud: Data-at-Rest, Data-in-Transit, and Data-in-Use. For data-at-rest, the Advanced Encryption Standard (AES) with a 256-bit key remains the industry benchmark due to its high throughput and computational efficiency. For data-in-transit, Transport Layer Security (TLS 1.3) protocols combined with asymmetric algorithms like RSA or Elliptic Curve Cryptography (ECC) ensure that information remains intercepted-proof during transmission between the client and the cloud provider. Protecting data-in-use, however, remains the most challenging task, requiring advanced cryptographic primitives [1, p. 148-166].

A significant advancement in protecting data-in-use is the emergence of Confidential Computing. This technology relies on hardware-based Trusted Execution Environments (TEEs), such as Intel SGX or AMD SEV. TEEs provide a secure enclave within the CPU where data can be decrypted and processed in complete isolation from the rest of the system, including the operating system and the hypervisor. This ensures that even if a cloud administrator or a malicious actor gains root access to the server, they cannot inspect or tamper with the data being processed inside the secure enclave.

Encryption is only as secure as the management of its cryptographic keys. Modern Cloud KMS solutions provide a centralized control plane for generating, rotating, and auditing keys. These services often utilize FIPS 140-2 Level 3 certified Hardware Security Modules (HSM) to ensure that keys never leave a protected hardware boundary. Implementing a robust KMS allows organizations to maintain 'Bring Your Own Key' (BYOK) or 'Hold Your Own Key' (HYOK) policies. This ensures that even the cloud provider cannot access the raw data without explicit permission, which is crucial for meeting strict regulatory compliance standards.

Integrating blockchain technology into cloud encryption frameworks offers a decentralized approach to key management and audit trails. By storing cryptographic hashes of key access logs on a distributed ledger, organizations can ensure that no unauthorized person has tampered with the security policies. This provides an immutable record of who accessed which data and when, significantly enhancing the transparency of cloud operations and reducing the risk of 'man-in-the-cloud' attacks [2, p. 895].

In the context of cloud identity management, ZKP (Zero-Knowledge Proofs) is a revolutionary method that allows one party to prove to another that a statement is true without revealing the actual information. In cloud systems, ZKP can be used for secure logins where the user proves they possess the correct credentials without those credentials ever being transmitted to or stored on the cloud server. This 'zero-knowledge' approach eliminates the risk of credential theft during massive data breaches and strengthens the overall authentication framework [3, p. 14].

Method Homomorphic Encryption (HE) allows mathematical operations to be performed directly on encrypted data without decrypting it first. This solves a major cloud dilemma: the ability to process data on a remote server without granting the provider access to the actual content. While Full Homomorphic Encryption (FHE) is currently computationally intensive, its partial implementations (PHE) are already being integrated into secure medical data analytics and financial auditing systems where privacy is paramount [4, p. 148–162].

In complex corporate cloud environments, traditional access control often proves insufficient. ABE (Attribute-Based Encryption) technology allows data to be encrypted such that it can only be decrypted by a user whose set of attributes (e.g., job title, department, or physical location) matches the specific access policy embedded in the ciphertext. This approach significantly minimizes the risks associated with internal threats and ensures that data sharing remains secure within multi-tenant cloud environments [5, p. 561–568].

As cloud databases grow, the ability to search through encrypted content becomes essential for usability. Searchable encryption allows the cloud server to search for specific keywords within encrypted documents without learning anything about the underlying plaintext. Furthermore, modern cloud security is shifting towards a Zero Trust model, which operates on the principle of 'never trust, always verify.' Within this framework, encryption is not just a tool but a continuous process where every data flow must be encrypted, authenticated, and authorized.

Looking ahead to the next generation of cybersecurity, the industry must address the systemic vulnerabilities of current standards. Post-Quantum Cryptography (PQC) represents the necessary evolution of these standards to withstand the unprecedented processing power of future machines. With the looming threat of quantum computing, traditional algorithms like RSA and ECC may become vulnerable to Shor's algorithm. The development and implementation of quantum-resistant algorithms – such as those based on lattices (Lattice-based cryptography) – is a top priority for securing cloud systems. Transitioning to PQC ensures long-term data protection against 'harvest now, decrypt later' attacks, providing a future-proof security layer for sensitive cloud assets in the upcoming decade [6, p. 10].

The following summarizes the core findings of this study regarding the protection of information in distributed environments. The implementation of hybrid encryption models, combined with advanced KMS, ZKP, and Confidential Computing technologies, allows for a balance between system performance and maximum security. The integration of these methods into a Zero Trust framework represents the most effective strategy for protecting data in the modern cloud landscape. As cyber threats continue to evolve, the adoption of post-quantum and homomorphic encryption will become the standard for ensuring digital sovereignty and data privacy.

REFERENCES

1. Stallings, W. Cryptography and Network Security: Principles and Practice, 5th Edition. Pearson, 2010. P. 148–166.
2. Zheng, Z., et al. Blockchain-based Secure Data Sharing in Cloud Computing. IEEE Transactions on Services Computing, 2024. Vol. 17, №3, P. 890–905.
3. Sun, X., et al. A Survey of Zero-Knowledge Proofs in Cloud Identity Management. ACM Computing Surveys, 2025. Vol. 57, №4. P. 14.
4. 4. Chris Gilbert and Mercy Abiola Gilbert, 'Homomorphic Encryption Algorithms for Secure Data Computation,' International Research Journal of Advanced Engineering and Science, 2025. Vol. 10, Issue 2, P. 148–162.
5. Akinyele, J. A., et al. Attribute-Based Encryption for Secure Access Control in Personal Health Records. IEEE 4th International Conference on Cloud Computing (CLOUD), 2011. P. 561–568.
6. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology, 2024. P. 10.