UDK 004.056.5

Lidiia TYMOSHENKO, Anna YAKYMOVA, Irina NAZAROVA

Odesa Polytechnic National University

DEVELOPMENT OF AN APPLICATION FOR THE CRYPTOGRAPHIC PROTECTION OF AUDIO STREAMING SERVICES CONSIDERING COMPRESSION CODECS

Introduction. The modern world actively utilizes audio streaming services, which creates new challenges in the field of transmitted information protection. Audio streams often contain confidential or copyrighted data that require reliable protection against interception, tampering, or unauthorized access. The use of compression codecs adds particular complexity, as they alter the structure of audio data and affect compatibility with cryptographic methods [1].

Objective. The objective of this thesis is to develop an application for the cryptographic protection of audio streaming services, considering the specifics of compression codecs. The relevance of this study is driven by the need to protect transmitted audio data from unauthorized access and ensure their integrity while using compression methods.

One of the most effective methods for ensuring confidentiality and integrity is the AES algorithm in GCM mode [2]. Figure 1 shows a general scheme of encryption using the AES-GCM algorithm.

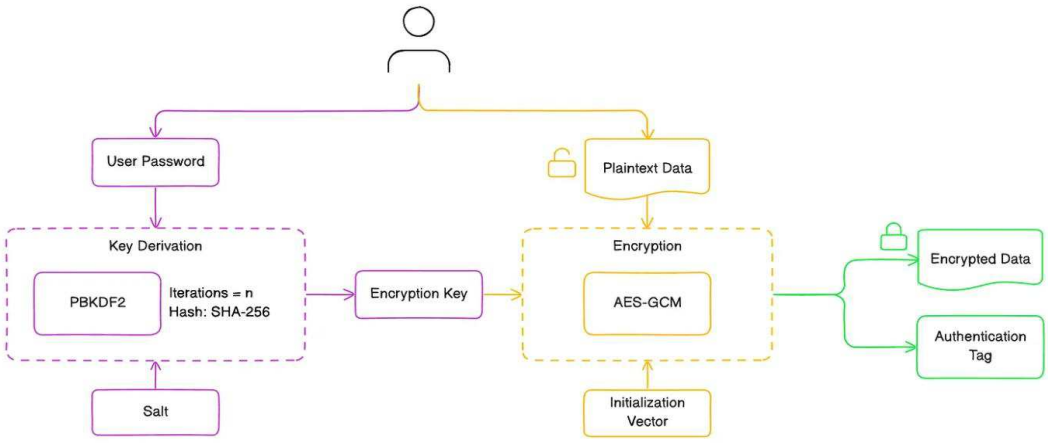

Figure 1 – AES-GCM encryption

This mode allows simultaneous encryption of data and verification of its authenticity through a tag. It is suitable for real-time data stream processing due to its high speed and support for parallel block processing. The reliability of the algorithm relies on the use of a unique initialization vector and authentication tag, which prevents replay or tampering attacks [3].

Figure 2 schematically depicts the generalized process of data decryption and authentication.

The combination of cryptography with the specific features of compression codecs plays a significant role. Encrypting audio before or after compression requires a precise understanding of stream structure changes in order to avoid quality loss and ensure compatibility. It is important to ensure such processing does not affect

transmission time, reduce performance, or compromise playback quality [4].

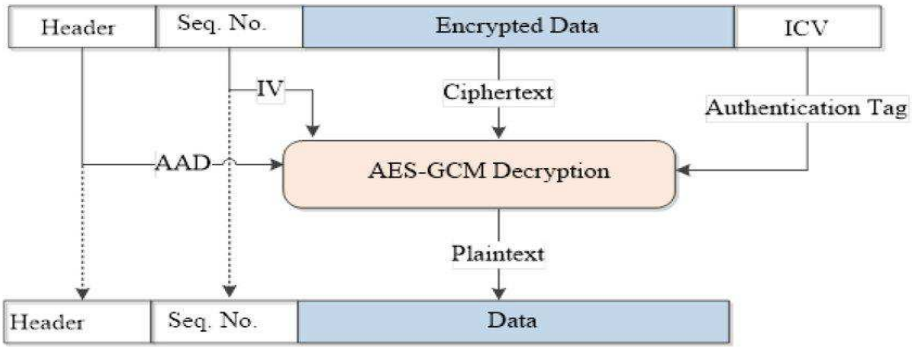

Figure 2 – AES-GCM Decryption

Special attention should be given to synchronization between the sender and receiver. Each encrypted packet must contain an initialization vector, a sequence number, and an authentication tag. This structure ensures correct decryption, enables detection of packet loss, and provides protection against replay attacks. Ensuring the uniqueness of vectors and reliable encryption key management are essential security conditions.

It is worth noting that AES-GCM has found widespread adoption among leading technology companies. Google uses it to protect data in its cloud platform and Chrome browser traffic, Amazon uses it in its AWS services to encrypt information, Microsoft uses this approach in Azure, and Apple protects messages in iMessage and data in iCloud. All of these companies have chosen AES-GCM because of its efficiency, speed, and comprehensive approach to data security. To achieve this goal, an analysis of modern cryptographic protection methods for audio streams was conducted, with a particular focus on the AES-GCM algorithm, which provides efficient encryption in streaming mode. The study includes the implementation of encryption and decryption algorithms for audio streams.

The advantages of AES-GCM include compatibility with streaming transmission, minimal latency, high speed, and resistance to common attacks. The effective implementation of this method in audio streaming services helps maintain a balance between security, performance, and user experience quality.

Conclusions. The main result of the research is the development of a software application that ensures the cryptographic protection of audio streaming without significantly affecting system performance or audio playback quality.

List of sources.

1. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Boston: Pearson, 2020. 752 p.

2. National Institute of Standards and Technology. FIPS PUB 197: Advanced Encryption Standard (AES) / NIST. 2001. 51 p.

3. Dworkin M.J. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. Gaithersburg, MD: National Institute of Standards and Technology, 2007. 56 p.

4. Baccour L., Atri M. Security Challenges in Multimedia Streaming Services: A Survey. Multimedia Tools and Applications. 2022. 27973 p.