1. Secure database

The application employs encryption to protect the filenames of recordings stored in the database, ensuring that only authorized users can access and understand the data. Here’s a detailed breakdown of how this encryption helps in preventing copyright infringement:

**Storage of Encrypted Filenames:** When a recording is saved, its filename is encrypted before being stored in the database. This means that even if someone gains unauthorized access to the database, they would not be able to determine the names of the files, let alone access the recordings themselves.

**Retrieval of Encrypted Filenames:** When a user views their recordings, the application decrypts the filenames before displaying them. This ensures that the data remains secure during storage and transit but is accessible in a readable format to the rightful owner.

**Generation and Storage of Encryption Keys:** A secure encryption key is generated and stored in a file when the application is first run. This key is essential for both encrypting and decrypting the filenames. The key management process ensures that the encryption is strong and that the key is not easily accessible.

**Loading the Encryption Key:** Every time the application runs, it checks for the existence of the key file. If the file exists, the key is loaded for use in encryption and decryption operations. This ensures consistency and security across sessions.

**Encrypting Messages:** The encrypt\_message function uses the encryption key to securely encrypt the filenames. This makes the filenames unreadable to anyone who does not have access to the key.

**Decrypting Messages:** Conversely, the decrypt\_message function decrypts the filenames when they need to be accessed by authorized users. This ensures that only legitimate users can view and manage the recordings.

1. Controlled access

The application prevents copyright infringement through controlled access by implementing several security measures, including user authentication, role-based access control, and encryption. Here’s how these mechanisms work together to ensure that only authorized users can access or manage recordings:

**User Registration:** During registration, users create a unique username and password. The password is encrypted before being stored in the database, ensuring it remains secure.

**User and Admin Roles:** The application distinguishes between regular users and the admin. Regular users can only see and manage their own recordings, while the admin has broader access for oversight. This role-based access control, combined with encrypted filenames, ensures that data is not exposed inappropriately.

**User Login:** Users must provide their username and password to log in. The application decrypts the stored password and compares it with the entered password to authenticate the user.

**Admin and User Roles:** The application differentiates between regular users and the admin. The admin has broader access and control over the system, while regular users can only access their own recordings.

**Admin Access:** The admin can view all recordings, delete recordings, and perform other administrative tasks.

**User Access:** Regular users can view and manage only their recordings. This access is restricted to ensure that users cannot view or modify other users' recordings.

**Viewing Recordings:** Users can view only their recordings, ensuring that they do not have access to recordings made by other users.

**Admin Management:** The admin can view and delete any recordings, providing oversight and control over the entire database.