Claims

1. **Claim 1**: A method for controlled information retrieval that combines facial recognition with a language model, restricting AI-generated responses based on user access levels.
2. **Claim 2**: The use of a facial recognition module to authenticate users, linking their biometrics to content access permissions for the purpose of retrieving AI-based responses limited to the authorized data.
3. **Claim 3**: A system in which an Access Control Module dynamically filters AI responses based on content permissions, ensuring that information output is restricted to user-specific access levels.
4. **Claim 4**: An auditing and logging feature that records user access attempts, queries, and AI responses, enabling compliance monitoring and review of information retrieval activities.
5. **Claim 5**: The integration of QR code scanning with facial authentication to allow mobile access to AI-restricted responses, further safeguarding information accessibility.
6. **Claim 6**: A filtering mechanism that screens AI responses in real time, dynamically omitting any data elements that exceed the user's verified access level.

Advantages

- **Enhanced Security**: Ensures that sensitive information is accessible only to authorized individuals based on biometric verification.
- **Role-Based Access Control**: Restricts AI response content dynamically, based on the authenticated user's role and access level.
- **Compliance Assurance**: Built-in auditing ensures regulatory compliance, allowing the organization to track who accessed specific data and when.
- **User Convenience**: Facial recognition offers a streamlined user experience, making secure access easier without manual login processes.