**Database Schema Documentation**

**Overview**

This document provides the schema documentation for a system that manages user authentication, credential management, presentation file processing, task tracking, authentication tokens, and auditing of user activities. The schema consists of six main tables: users, user\_credentials, presentations, tasks, auth\_tokens, and audit\_logs.

**1. Table: users**

This table stores user information including identity, contact information, and account status.

|  |  |  |
| --- | --- | --- |
| **Column Name** | **Data Type** | **Description** |
| user\_id | INT | Primary key. Auto-incremented unique identifier. |
| email | VARCHAR(255) | Unique email address. |
| full\_name | VARCHAR(255) | Full name of the user. |
| created\_at | TIMESTAMP | Record creation timestamp. |
| updated\_at | TIMESTAMP | Record last update timestamp. |
| is\_active | BOOLEAN | Indicates if the account is active. |
| last\_login\_at | TIMESTAMP | Timestamp of the last login. |

Constraints:

* email is unique.
* email\_unique constraint enforces email uniqueness.

Indexes:

* idx\_users\_email: index on email column.

**2. Table: user\_credentials**

This table stores sensitive credentials related to user accounts.

|  |  |  |
| --- | --- | --- |
| Column Name | Data Type | Description |
| credential\_id | INT | Primary key. Auto-incremented. |
| user\_id | INT | Foreign key referencing users(user\_id). |
| password\_hash | VARCHAR(255) | Hashed password string. |
| two\_factor\_secret | VARCHAR(512) | Optional 2FA secret. |
| created\_at | TIMESTAMP | Record creation timestamp. |
| updated\_at | TIMESTAMP | Record last update timestamp. |

Constraints:

* Foreign key: user\_id references users(user\_id).

**3. Table: presentations**

This table stores metadata for presentation files uploaded or generated by users.

|  |  |  |
| --- | --- | --- |
| Column Name | Data Type | Description |
| presentation\_id | INT | Primary key. Auto-incremented. |
| user\_id | INT | Foreign key referencing users(user\_id). |
| file\_url | VARCHAR(255) | URL or file path of the presentation. |
| status | ENUM | Status of the presentation: 'pending', 'in\_progress', 'completed', 'failed'. |
| created\_at | TIMESTAMP | Record creation timestamp. |
| updated\_at | TIMESTAMP | Record last update timestamp. |

Indexes:

* idx\_presentations\_user\_id: index on user\_id column.

**4. Table: tasks**

This table tracks processing tasks related to presentations.

|  |  |  |
| --- | --- | --- |
| Column Name | Data Type | Description |
| task\_id | INT | Primary key. Auto-incremented. |
| presentation\_id | INT | Foreign key referencing presentations(presentation\_id). |
| task\_status | ENUM | Task status: 'queued', 'in\_progress', 'completed', 'failed'. |
| result | TEXT | Result of the task execution. |
| started\_at | TIMESTAMP | Timestamp when task started. |
| completed\_at | TIMESTAMP | Timestamp when task completed. |
| created\_at | TIMESTAMP | Record creation timestamp. |
| updated\_at | TIMESTAMP | Record last update timestamp. |

Indexes:

* idx\_tasks\_presentation\_id: index on presentation\_id column.

**5. Table: auth\_tokens**

This table stores authentication tokens issued to users.

|  |  |  |
| --- | --- | --- |
| Column Name | Data Type | Description |
| token\_id | INT | Primary key. Auto-incremented. |
| user\_id | INT | Foreign key referencing users(user\_id). |
| token | VARCHAR(512) | Authentication token. |
| created\_at | TIMESTAMP | Token creation timestamp. |
| expires\_at | TIMESTAMP | Token expiration timestamp. |
| revoked | BOOLEAN | Indicates if the token has been revoked. |

Indexes:

* idx\_auth\_tokens\_user\_id: index on user\_id column.

**6. Table: audit\_logs**

This table logs all critical actions performed by users for auditing purposes.

|  |  |  |
| --- | --- | --- |
| Column Name | Data Type | Description |
| log\_id | INT | Primary key. Auto-incremented. |
| user\_id | INT | Foreign key referencing users(user\_id). |
| action\_type | VARCHAR(255) | Type or category of user action. |
| action\_details | TEXT | Detailed description of the action performed. |
| ip\_address | VARCHAR(50) | IP address from which the action was initiated. |
| user\_agent | VARCHAR(255) | Device/browser information. |
| created\_at | TIMESTAMP | Timestamp of the action. |

Indexes:

* idx\_audit\_logs\_user\_id: index on user\_id column.

**Security Considerations**

* Sensitive data (passwords, API keys, secrets) must be encrypted at rest.
* Access to credential data must be restricted to authorized services only.
* Authentication tokens should be time-bound and revoked after logout or expiration.
* Audit logs should be immutable and securely stored for compliance.

**Performance Optimizations**

* Use indexes on frequently queried fields to optimize performance.
* Archive old audit logs and tasks periodically to maintain performance.
* Consider using background job processing systems for task execution scalability.

**Compliance and Monitoring**

* Log user activities for security auditing.
* Implement role-based access control (RBAC) to protect sensitive endpoints.
* Monitor access logs and suspicious activities for security incidents.