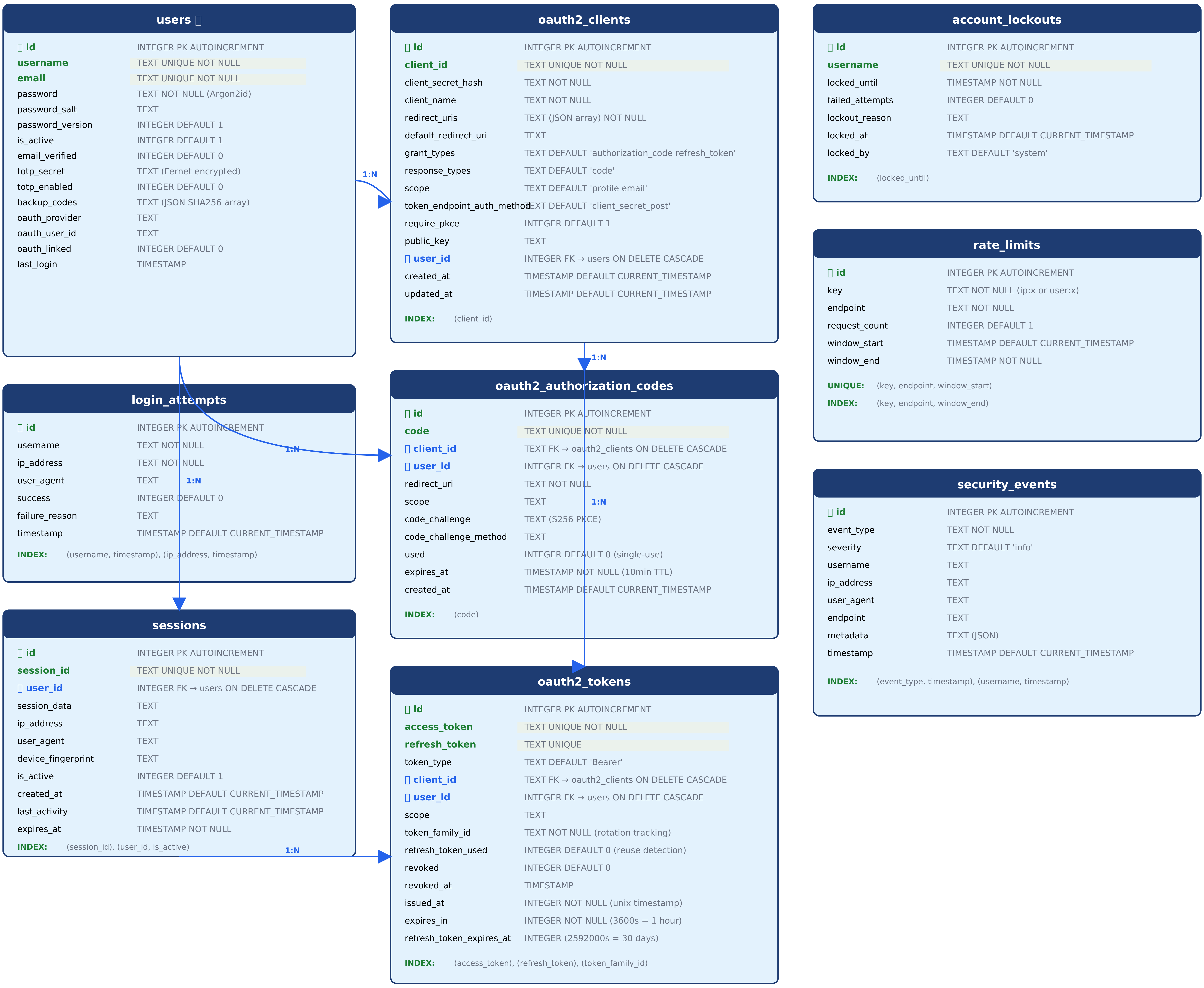
Database Schema (recipe_app.db)

9 Tables • 15 Indexes • 8 Foreign Keys with CASCADE



users

id	INTEGER PK AUTOINCREMENT
username	TEXT UNIQUE NOT NULL
email	TEXT UNIQUE NOT NULL
password	TEXT NOT NULL (Argon2id)
password_salt	TEXT
password_version	INTEGER DEFAULT 1
is_active	INTEGER DEFAULT 1
email_verified	INTEGER DEFAULT 0
totp_secret	TEXT (Fernet encrypted)
totp_enabled	INTEGER DEFAULT 0
backup_codes	TEXT (JSON SHA256 array)
oauth_provider	TEXT
oauth_user_id	TEXT
oauth_linked	INTEGER DEFAULT 0
last_login	TIMESTAMP

oauth2_clients

id	INTEGER PK AUTOINCREMENT
client_id	TEXT UNIQUE NOT NULL
client_secret_hash	TEXT NOT NULL
client_name	TEXT NOT NULL
redirect_uris	TEXT (JSON array) NOT NULL
default_redirect_uri	TEXT
grant_types	TEXT DEFAULT 'authorization_code refresh_token'
response_types	TEXT DEFAULT 'code'
scope	TEXT DEFAULT 'profile email'
token_endpoint_auth_method	TEXT DEFAULT 'client_secret_post'
require_pkce	INTEGER DEFAULT 1
public_key	TEXT
user_id	INTEGER FK → users ON DELETE CASCADE
created_at	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
updated_at	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
INDEX:	(client_id)

account_lockouts

id	INTEGER PK AUTOINCREMENT
username	TEXT UNIQUE NOT NULL
locked_until	TIMESTAMP NOT NULL
failed_attempts	INTEGER DEFAULT 0
lockout_reason	TEXT
locked_at	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
locked_by	TEXT DEFAULT 'system'
INDEX:	(locked_until)

rate_limits

id	INTEGER PK AUTOINCREMENT
key	TEXT NOT NULL (ip:x or user:x)
endpoint	TEXT NOT NULL
request_count	INTEGER DEFAULT 1
window_start	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
window_end	TIMESTAMP NOT NULL
UNIQUE:	(key, endpoint, window_start)
INDEX:	(key, endpoint, window_end)

login_attempts

id	INTEGER PK AUTOINCREMENT
username	TEXT NOT NULL
ip_address	TEXT NOT NULL
user_agent	TEXT
success	INTEGER DEFAULT 0
failure_reason	TEXT
timestamp	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
INDEX:	(username, timestamp), (ip_address, timestamp)

oauth2_authorization_codes

id	INTEGER PK AUTOINCREMENT
code	TEXT UNIQUE NOT NULL
client_id	TEXT FK → oauth2_clients ON DELETE CASCADE
user_id	INTEGER FK → users ON DELETE CASCADE
redirect_uri	TEXT NOT NULL
scope	TEXT
code_challenge	TEXT (S256 PKCE)
code_challenge_method	TEXT
used	INTEGER DEFAULT 0 (single-use)
expires_at	TIMESTAMP NOT NULL (10min TTL)
created_at	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
INDEX:	(code)

security_events

id	INTEGER PK AUTOINCREMENT
event_type	TEXT NOT NULL
severity	TEXT DEFAULT 'info'
username	TEXT
ip_address	TEXT
user_agent	TEXT
endpoint	TEXT
metadata	TEXT (JSON)
timestamp	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
INDEX:	(event_type, timestamp), (username, timestamp)

sessions

id	INTEGER PK AUTOINCREMENT
session_id	TEXT UNIQUE NOT NULL
user_id	INTEGER FK → users ON DELETE CASCADE
session_data	TEXT
ip_address	TEXT
user_agent	TEXT
device_fingerprint	TEXT
is_active	INTEGER DEFAULT 1
created_at	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
last_activity	TIMESTAMP DEFAULT CURRENT_TIMESTAMP
expires_at	TIMESTAMP NOT NULL
INDEX:	(session_id), (user_id, is_active)

oauth2_tokens

id	INTEGER PK AUTOINCREMENT
access_token	TEXT UNIQUE NOT NULL
refresh_token	TEXT UNIQUE
token_type	TEXT DEFAULT 'Bearer'
client_id	TEXT FK → oauth2_clients ON DELETE CASCADE
user_id	INTEGER FK → users ON DELETE CASCADE
scope	TEXT
token_family_id	TEXT NOT NULL (rotation tracking)
refresh_token_used	INTEGER DEFAULT 0 (reuse detection)
revoked	INTEGER DEFAULT 0
revoked_at	TIMESTAMP
issued_at	INTEGER NOT NULL (unix timestamp)
expires_in	INTEGER NOT NULL (3600s = 1 hour)
refresh_token_expires_at	INTEGER (2592000s = 30 days)
INDEX:	(access_token), (refresh_token), (token_family_id)

Database Schema Details

✓ **Primary Keys (9 tables):**

All tables use INTEGER PRIMARY KEY AUTOINCREMENT for auto-generated IDs

✓ **UNIQUE Constraints:**

- users: username, email
- account_lockouts: username
- oauth2_clients: client_id
- oauth2_authorization_codes: code
- oauth2_tokens: access_token, refresh_token
- sessions: session_id
- rate_limits: UNIQUE(key, endpoint, window_start)

✓ **Foreign Keys (8 total, all with ON DELETE CASCADE):**

- oauth2_clients.user_id → users.id
- oauth2_authorization_codes.client_id → oauth2_clients.client_id
- oauth2_authorization_codes.user_id → users.id
- oauth2_tokens.client_id → oauth2_clients.client_id
- oauth2_tokens.user_id → users.id
- sessions.user_id → users.id

✓ **Indexes (15 total):**

- login_attempts: (username, timestamp), (ip_address, timestamp)
- account_lockouts: (locked_until)
- rate_limits: (key, endpoint, window_end)
- security_events: (event_type, timestamp), (username, timestamp)
- oauth2_clients: (client_id)
- oauth2_authorization_codes: (code)
- oauth2_tokens: (access_token), (refresh_token), (token_family_id)
- sessions: (session_id), (user_id, is_active)

✓ **Security Features:**

- Password: Argon2id (t=2, m=19456 KiB, p=1, hash=32B, salt=16B)
- TOTP: Fernet encrypted (AES-128 CBC + HMAC, PBKDF2 100k iterations)
- Backup Codes: JSON array of SHA-256 hashes
- OAuth2: PKCE required, token rotation with family tracking
- Sessions: Device fingerprinting, IP tracking, expiration
- Rate Limiting: Database-backed with sliding window

✓ **Token Lifetimes:**

- Authorization Codes: 10 minutes
- Access Tokens: 3600s (1 hour)
- Refresh Tokens: 2592000s (30 days)