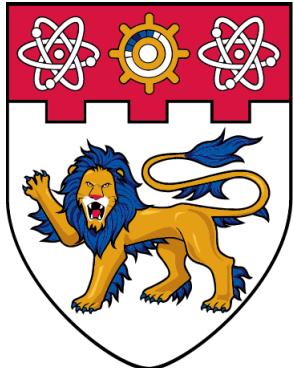


NANYANG TECHNOLOGICAL UNIVERSITY
COLLEGE OF COMPUTING AND DATA SCIENCE



**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

**Full Stack Development and
Deployment of Web-based Speech
Recognition System**

By
NGUYEN PHUONG LINH

Project Supervisor: Prof Chng Eng Siong

Singapore
Academic Year 2025/2026

Abstract

This project focuses on the design and implementation of the **Gateway Dashboard**, a comprehensive management interface for the Speech Gateway API, alongside critical backend enhancements to support secure authentication and monetization.

On the **frontend**, a responsive Single Page Application (SPA) was developed using **Vue.js** and **Vuetify**, featuring a modular architecture that ensures scalability and maintainability. Key implemented features include a secure authentication system supporting **Email/Password**, **Google OAuth 2.0**, and **Apple Sign-In**, enhancing user accessibility and security.

The **backend**, built with **NestJS**, was significantly upgraded to include a **Token Management Module** ensuring session security through token blacklisting and automatic expiration handling using Redis and MongoDB TTL indexes.

Furthermore, a **Subscription and Payment Module** was integrated using **Stripe**, enabling automated recurring billing, plan management, and real-time subscription status tracking. Storage solutions utilizing **MongoDB** for persistent data and **Redis** for caching were implemented to optimize performance.

The result is a **production-ready dashboard** that facilitates seamless user onboarding, secure identity management, and a flexible subscription model, thereby establishing a solid foundation for the commercialization of the Speech Gateway services.

Acknowledgement

I would like to express my deepest gratitude to my mentors **Kyaw Zin Tun, Vu Thi Ly, Surana Tanmay** and my supervisor, **Chng Eng Siong**, for their invaluable guidance, continuous encouragement, and expert advice throughout the course of this Final Year Project. Their insights were instrumental in shaping the direction and reliability of this system.

I extend my sincere thanks to the **Hardware and Embedded Systems Lab** team for providing the necessary resources and technical environment to develop this project. The opportunity to work with real-world technologies like NestJS, Vue.js, and cloud infrastructure has been an immensely rewarding learning experience.

I am also grateful to my friends and family for their unwavering support and patience during the intense periods of development and debugging. Their belief in my abilities kept me motivated to overcome the technical challenges encountered along the way.

Finally, I would like to thank **Nanyang Technological University** for providing the academic foundation that made this work possible.

Contents

Abstract	1
Acknowledgement	2
List of Figures	5
List of Tables	6
1 Introduction	7
1.1 Background	7
1.2 Problem Statement	7
1.3 Project Objectives	7
1.4 Project Scope	8
1.4.1 Single Sign-On (SSO) Authentication	8
1.4.2 Payment Portal with Stripe Integration	8
1.4.3 Frontend Dashboard	9
2 Literature Review	10
2.1 SSO Provider Selection	10
2.1.1 SSO Provider Comparison	10
2.1.2 Why Google and Apple	10
2.2 Payment Platform Selection: Stripe vs PayPal	11
2.2.1 Comparison Overview	11
2.2.2 Why Stripe	11
2.3 Redis Caching: Critical Importance	11
2.3.1 Redis Use Cases	11
2.3.2 Why Redis is Critical	12
2.4 Token Management Strategy	12
2.4.1 Token Architecture	12
2.4.2 Why This Approach	12
2.5 Summary	13
3 System Architecture	14
3.1 Overview	14
3.1.1 High-Level Architecture	14
3.1.2 Component Overview	15
3.1.3 Communication Flow	15
3.2 Technology Stack	15
3.2.1 Frontend Technologies	16
3.2.2 Backend Technologies	16

3.2.3	Data Storage and Caching	16
3.2.4	External Services	18
3.3	Database Design	19
3.3.1	Core Collections	19
3.3.2	Authentication Collections	20
3.3.3	Entity Relationships	21
4	Detailed Implementation	23
4.1	Backend Implementation	23
4.1.1	SSO Implementation	23
4.1.2	Payment & Subscription Management	32
4.2	Frontend Implementation	42
4.2.1	Overview	42
4.2.2	Authentication Frontend	44
4.2.3	Routing and Navigation	46
4.2.4	Subscription Management Interface	50
5	Conclusion and Future Work	54
5.1	Project Summary	54
5.1.1	Authentication System	54
5.1.2	Payment and Subscription System	54
5.1.3	Frontend Dashboard	55
5.2	Conclusions	55
5.3	Future Work	55
5.3.1	Technical Enhancements	55
5.3.2	Business Features	56
5.3.3	Infrastructure Improvements	56
5.4	Final Remarks	56
A	Proof	60

List of Figures

3.1	High-Level System Architecture	14
3.2	Plan Module Caching Architecture	17
3.3	Cache Flow for Latest Plans Retrieval	18
3.4	Entity Relationship Diagram	22
4.1	SSO Authentication Architecture	24
4.2	Google OAuth 2.0 Authentication Flow	25
4.3	State Parameter Encoding Flow	27
4.4	Apple Sign-In Authentication Flow	28
4.5	JWT Token Lifecycle Management	30
4.6	Token Blacklisting Flow	31
4.7	Google SSO Module Structure	32
4.8	Payment System Architecture	32
4.9	Plan Versioning Flow	33
4.10	Stripe Checkout Session Flow	36
4.11	Subscription Quota Checking Flow	39
4.12	Stripe Price Caching with Penetration Protection	41
4.13	Frontend Application Architecture	43
4.14	Navigation Guards Flow	48
4.15	HTTP Interceptor Flow with Token Refresh	50

List of Tables

2.1	SSO Provider Comparison	10
2.2	Stripe vs PayPal Comparison	11
2.3	Redis Usage in Gateway Dashboard	12
2.4	Token Management Strategy	12
2.5	Technology Decision Summary	13
3.1	Frontend Technology Stack	16
3.2	Backend Technology Stack	16
3.3	Storage Technologies	16
3.4	Users Collection Schema	19
3.5	Subscriptions Collection Schema	20
3.6	Plans Collection Schema	20
3.7	UserTokens Collection Schema	21
3.8	TokenBlacklist Collection Schema	21
4.1	Frontend Technology Stack	43
4.2	Auth Service Methods	44
4.3	Route Definitions	47
4.4	PlanCard Component Props	51

Chapter 1

Introduction

1.1 Background

In the rapidly evolving landscape of speech processing technologies, the **Speech Gateway API** serves as a critical infrastructure for delivering advanced speech services to various applications. **Speech Gateway** is a backend service that provides Speech-to-Text (STT) capabilities to end users through a secured API. It acts as a **middle layer** between client applications and an underlying Speech Engine. Instead of allowing clients to call the speech engine directly, Speech Gateway centralizes authentication, access control, token issuance, and (in this project) subscription/payment management.

As the demand for these services grows, the need for a robust, centralized management system becomes paramount. Traditionally, interacting with such APIs required direct integration and manual management, which can be inefficient for end-users and administrators alike. The **Gateway Dashboard** project was initiated to bridge this gap, providing a user-friendly graphical interface that empowers users to manage their speech processing tasks while giving administrators the tools needed to oversee system operations, manage users, and monetize services effectively.

1.2 Problem Statement

Prior to this project, the Speech Gateway ecosystem faced several challenges:

1. **Limited Access Control:** The existing system lacked a flexible authentication mechanism, supporting only basic credentials without modern Single Sign-On (SSO) capabilities.
2. **Absence of Monetization Infrastructure:** There was no automated system to handle subscriptions, billing, or tiered access plans, hindering the commercial viability of the services.

1.3 Project Objectives

The primary objective of this project is to design and implement a comprehensive **Gateway Dashboard** and enhance the backend infrastructure to support commercial-grade features. Specific objectives include:

- **SSO Integration:** Implement secure Single Sign-On (Google, Apple) to streamline user authentication, reduce credential fatigue, and centralize identity management across services.
- **Payment Portal:** Design a subscription and payment module integrating Stripe to handle recurring billing, automated invoicing, and subscription lifecycle management.
- **Frontend Development:** Develop a web-based dashboard using Vue.js and Vuetify to provide an intuitive interface for users to access speech services and manage their data.

1.4 Project Scope

The project scope encompasses three major components: Single Sign-On (SSO) Authentication, Payment & Subscription Management with Stripe Integration, and Frontend Dashboard Development.

1.4.1 Single Sign-On (SSO) Authentication

This component enables users to authenticate using their existing social accounts or traditional credentials.

Key Features:

- **Google SSO:** OAuth 2.0 integration with state management for CSRF protection.
- **Apple SSO:** Apple Sign In integration with token verification and privacy-preserving email relay.
- **JWT Token Management:** Generation and validation of access tokens (15-minute expiry) and refresh tokens with secure cookie storage (HttpOnly, Secure, SameSite).
- **Token Blacklisting:** Redis-based blacklist for immediate token revocation on logout or security events.
- **Traditional Authentication:** Email/password authentication with bcrypt hashing.
- **Session Security:** CSRF protection, XSS prevention, and secure token lifecycle management.

1.4.2 Payment Portal with Stripe Integration

This component handles monetization through Stripe, enabling tiered subscription plans with usage-based quotas.

Key Features:

- **Stripe Checkout:** Hosted checkout session creation and payment processing.
- **Webhook Handling:** Secure webhook signature verification and idempotent event processing for payment lifecycle events.

- **Plan Management:** JSON-based plan configuration with versioning support and admin API.
- **Redis Caching:** Fast plan retrieval and Stripe price data caching with automatic cache invalidation.
- **Subscription Synchronization:** Real-time sync between Stripe and internal database for subscription status.
- **Quota Management:** Usage tracking and access control middleware enforcing plan limits.
- **Payment UI:** Plan comparison cards, checkout flow, and subscription management interface.

1.4.3 Frontend Dashboard

This component provides a complete Single Page Application (SPA) using Vue.js 2 and Vuetify with Material Design.

Key Features:

- **Authentication UI:** Sign In, Sign Up pages with SSO integration and OAuth callback handling.
- **Protected Routing:** Vue Router with role-based navigation guards and lazy loading for performance.
- **State Management:** Vuex store for centralized state management (auth, user, subscription, plans).
- **HTTP Interceptors:** Automatic JWT token injection, token refresh logic, and retry mechanisms.
- **User Dashboard:** Subscription status display, usage quota tracking with progress indicators, profile management.
- **Admin Interface:** Plans management with JSON editor, validation, and version history.
- **Responsive Design:** Mobile and desktop layouts with Vuetify components and intuitive UX.

Chapter 2

Literature Review

This chapter examines the key technology decisions for the Gateway Dashboard, focusing on SSO provider selection, payment platform comparison, Redis caching importance, and token management strategies.

2.1 SSO Provider Selection

The Gateway Dashboard implements Google and Apple SSO as primary authentication methods.

2.1.1 SSO Provider Comparison

Table 2.1 compares major SSO providers:

Table 2.1: SSO Provider Comparison

Provider	Market Share	Key Advantage	Status
Google	71% (Android)	2B+ users, mature API	Implemented
Apple	28% (iOS)	Privacy-focused, email relay	Implemented
Microsoft	Enterprise strong	Azure AD integration	Other dev
Facebook	2.9B users	Large user base	Excluded (privacy)
GitHub	Developer focus	Dev community	Not needed

2.1.2 Why Google and Apple

Selection Rationale:

1. **Market Coverage:** 95%+ of internet users have Google or Apple accounts [50, 49]
2. **User Convenience:** Eliminates credential fatigue; most developers already have these accounts
3. **Technical Maturity:** Robust OAuth 2.0 implementations with 99.9%+ uptime [20, 2]
4. **Team Division:** Microsoft SSO handled by another developer, avoiding duplicate work
5. **Security:** Both provide 2FA, fraud detection, and privacy features

2.2 Payment Platform Selection: Stripe vs PayPal

2.2.1 Comparison Overview

Table 2.2 compares Stripe and PayPal:

Table 2.2: Stripe vs PayPal Comparison

Criteria	Stripe	PayPal
Transaction Fee	2.9% + \$0.30	2.9% + \$0.30
API Quality	RESTful, excellent docs [51]	Complex multi-generation APIs
Checkout Flow	Embedded (no redirect)	Redirect-based (-10-15% conversion) [6]
Subscriptions	Native billing, prorated upgrades [52]	Limited flexibility
Webhooks	Auto-retry, signature verification [48]	Basic webhook support
Integration Time	40% faster [24]	Slower, complex documentation
Developer Focus	✓ Strong	Limited
Metered Billing	✓ Supported	Not supported

2.2.2 Why Stripe

Decision: Stripe chosen for:

- **Subscription Requirements:** Native support for tiered plans, quotas, prorated changes, automated renewals
- **Developer Experience:** Superior API design, documentation, official SDK for Node.js
- **Embedded Checkout:** Maintains user context, better conversion rates
- **Webhook Reliability:** Ensures payment-database consistency with idempotency
- **Target Audience:** Developers value functionality over PayPal's consumer brand

2.3 Redis Caching: Critical Importance

Redis is essential for both **performance** and **security** in the Gateway Dashboard.

2.3.1 Redis Use Cases

Table 2.3 summarizes Redis applications:

Table 2.3: Redis Usage in Gateway Dashboard

Use Case	Purpose	Performance Gain	TTL
Plan Caching	Reduce DB load	95%+ load reduction	1 hour
Stripe Price Caching	Minimize API calls	Sub-ms retrieval	1 hour
Token Blacklist	Immediate revocation	1ms lookup	Token expiry

2.3.2 Why Redis is Critical

1. **Performance:** Sub-millisecond access times [8], in-memory storage
2. **Scalability:** Handles millions of requests/second, horizontally scalable
3. **Security:** Enables JWT token blacklisting for immediate logout/revocation
4. **Database Protection:** Shields MongoDB from read-heavy workloads (99% read, 1% write)
5. **Cache Strategy:** Cache-aside pattern [12] with automatic invalidation
6. **Persistence:** RDB snapshots prevent data loss during restarts

Implementation: Cache warming on startup, automatic invalidation on plan updates, TTL-based expiration.

2.4 Token Management Strategy

Token management balances **security**, **scalability**, and **user experience**.

2.4.1 Token Architecture

Table 2.4 details the token strategy:

Table 2.4: Token Management Strategy

Feature	Implementation	Purpose
Access Token	JWT, 15-min expiry	Minimize compromise window [29]
Refresh Token	7-day expiry, rotation	Seamless re-auth [47]
Blacklisting	Redis-based	Immediate revocation
Cookie Storage	HttpOnly, Secure, SameSite	XSS/CSRF protection [5]
Stateless Auth	JWT self-contained	Horizontal scalability

2.4.2 Why This Approach

- **Stateless Scalability:** JWTs don't require DB lookup on every request [26]
- **Security Layers:** Short-lived tokens + blacklist + secure cookies
- **User Experience:** Automatic refresh = no frequent logins
- **Immediate Revocation:** Redis blacklist solves JWT's "can't revoke" problem
- **Performance:** Sub-millisecond blacklist checks, no DB bottleneck

2.5 Summary

Table 2.5 summarizes key technology decisions:

Table 2.5: Technology Decision Summary

Component	Choice	Key Reason
SSO Providers	Google + Apple	95%+ user coverage, Microsoft by other dev
Payment	Stripe	Better API, subscriptions, webhooks vs PayPal
Caching	Redis	Performance (sub-ms) + security (blacklist)
Token Strategy	JWT + Redis blacklist	Stateless scalability + immediate revocation

Core Principles: All choices prioritize developer experience, security, performance, and scalability for the API management domain.

Chapter 3

System Architecture

This chapter provides a comprehensive overview of the Gateway Dashboard system architecture, detailing the technology stack, component interactions, and database design decisions that underpin the platform.

3.1 Overview

The Gateway Dashboard system follows a modern three-tier architecture consisting of a **Vue.js** frontend, a **NestJS** backend API, and integration with external services. This separation of concerns ensures scalability, maintainability, and clear boundaries between presentation, business logic, and data persistence layers.

3.1.1 High-Level Architecture

Figure 3.1 illustrates the overall system architecture. The frontend communicates with the backend through RESTful APIs, while the backend interacts with external services such as Stripe for payment processing and OAuth providers for authentication.

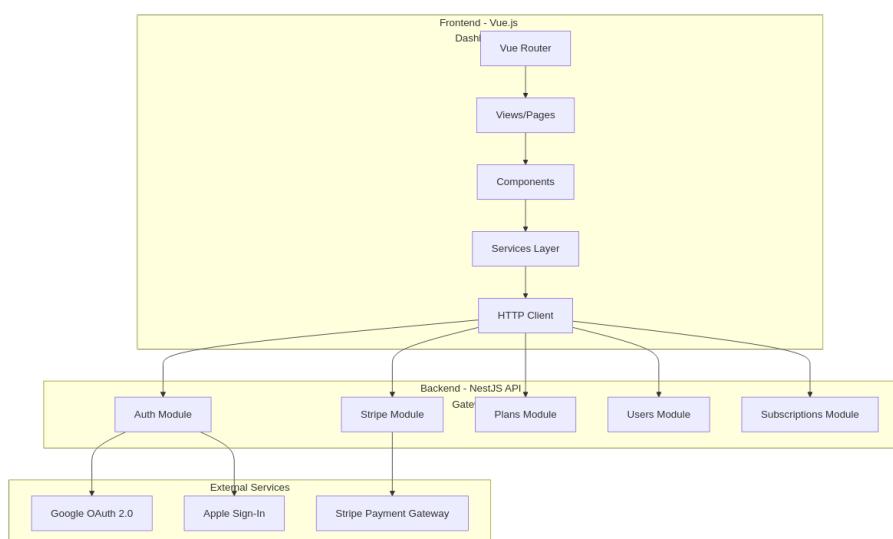


Figure 3.1: High-Level System Architecture

The architecture diagram details the data flow within the system. The **Frontend** layer consists of Vue Router directing requests to Views/Pages, which utilize Components and

a Services Layer that communicates via an HTTP Client. The **Backend** layer comprises modular NestJS components: Auth, Stripe, Plans, Users, and Subscriptions modules. The **External Services** layer includes Google OAuth 2.0, Apple Sign-In, and Stripe Payment Gateway for third-party integrations.

3.1.2 Component Overview

The system is composed of the following major components:

- **Frontend Dashboard:** A Single Page Application (SPA) built with Vue.js 2 and Vuetify, providing user interfaces for authentication, subscription management, and administrative functions.
- **Backend API Gateway:** A NestJS-based REST API that handles authentication, authorization, business logic, and orchestration of external services.
- **Database Layer:** MongoDB serves as the primary data store for users, subscriptions, plans, and tokens, with Redis providing caching for frequently accessed data.
- **External Services:** Integration with Google OAuth 2.0, Apple Sign-In, and Stripe for third-party authentication and payment processing.

3.1.3 Communication Flow

The typical request flow proceeds as follows:

1. The user interacts with the Vue.js frontend through the browser.
2. The frontend dispatches HTTP requests to the backend API via Axios interceptors.
3. The backend validates the JWT token, checks authorization, and processes the request.
4. Business logic is executed, interacting with MongoDB, Redis, or external APIs as needed.
5. The response is returned to the frontend, which updates the user interface accordingly.

3.2 Technology Stack

The Gateway Dashboard leverages modern, industry-standard technologies to ensure robustness, scalability, and developer productivity.

3.2.1 Frontend Technologies

Technology	Version	Purpose
Vue.js	2.x	Progressive JavaScript framework for building user interfaces
Vuetify	2.x	Material Design component framework for Vue.js
Vue Router	3.x	Official router for single-page application navigation
Axios	Latest	Promise-based HTTP client for API communication

Table 3.1: Frontend Technology Stack

Vue.js 2 was selected for its gentle learning curve, excellent documentation, and reactive data binding capabilities. The framework's component-based architecture facilitates code reuse and maintainability. **Vuetify** provides a comprehensive set of Material Design components, enabling rapid UI development with a professional appearance.

3.2.2 Backend Technologies

Technology	Version	Purpose
NestJS	9.x	Progressive Node.js framework for server-side applications
TypeScript	4.x	Typed superset of JavaScript for enhanced code quality
Passport	0.6.x	Authentication middleware for Node.js
JWT	Latest	JSON Web Token for stateless authentication

Table 3.2: Backend Technology Stack

NestJS provides a modular architecture with built-in dependency injection support, ideal for enterprise-grade applications. TypeScript ensures type safety and improved developer experience. **Passport** offers a flexible authentication framework with extensive strategy support for OAuth providers.

3.2.3 Data Storage and Caching

Technology	Version	Purpose
MongoDB	5.x	NoSQL document database for flexible schema design
Redis	6.x	In-memory data store for caching and session management

Table 3.3: Storage Technologies

MongoDB was chosen for its schema flexibility, horizontal scalability, and native JSON support. **Redis** serves dual purposes: caching frequently accessed data (plans, prices) and managing token blacklists for security.

Caching Architecture

Figure 3.2 illustrates the caching architecture for the Plan module. The service layer first checks Redis for cached data, falling back to MongoDB on cache misses.

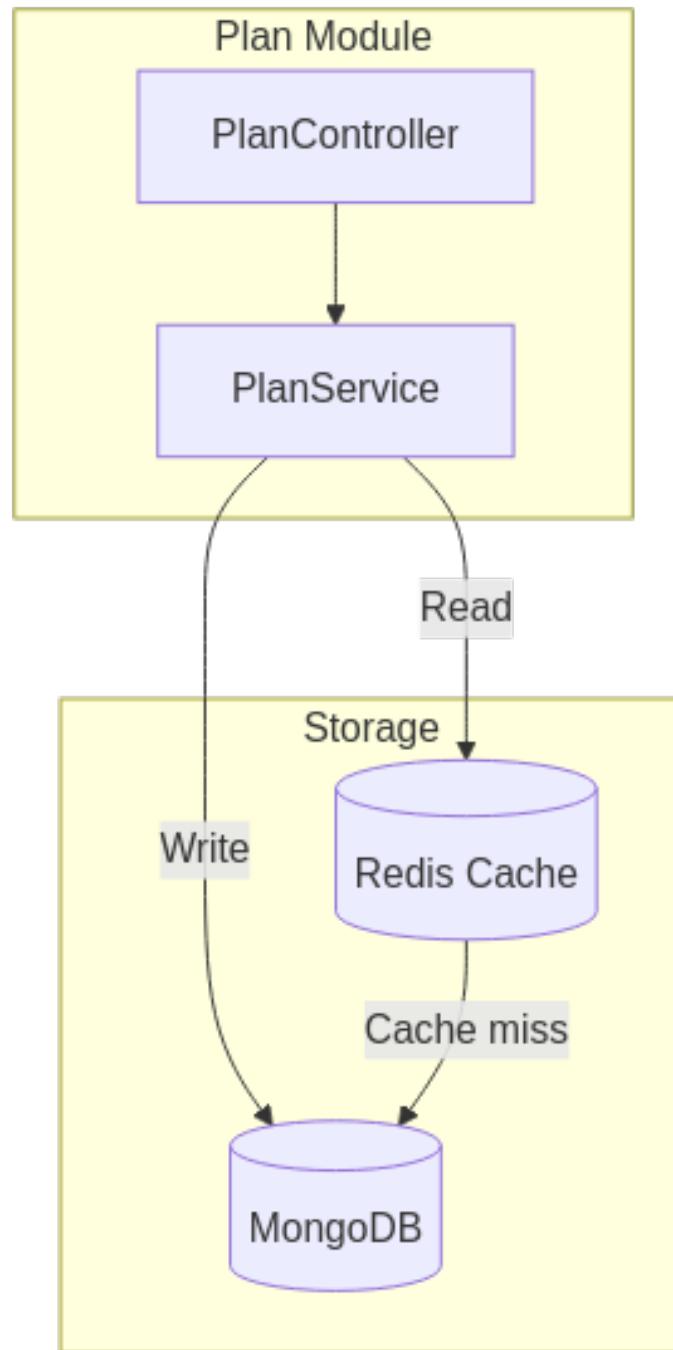


Figure 3.2: Plan Module Caching Architecture

As depicted in Figure 3.2, the Plan Module implements a read-through caching strat-

egy. When a request for plans is received, the `PlanService` first queries the Redis cache. If the data is found (cache hit), it is returned immediately. If not (cache miss), the service retrieves the data from MongoDB, stores it in Redis for future requests, and then returns it to the controller.

Figure 3.3 shows the detailed cache flow for retrieving the latest plans. This strategy includes cache penetration protection by caching NULL values for a short duration when no plans exist.

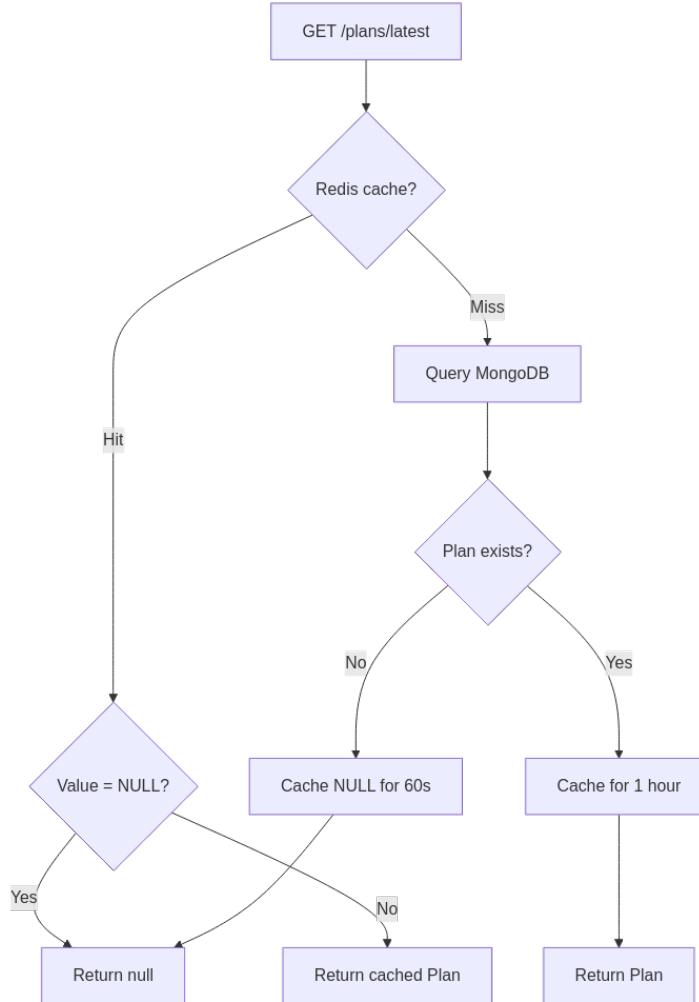


Figure 3.3: Cache Flow for Latest Plans Retrieval

Figure 3.3 provides a granular view of the "get latest plans" logic. It highlights the cache penetration protection mechanism: if a database query returns no plans, a special `NULL` value is cached for a short duration (e.g., 60 seconds). This prevents repeated queries for non-existent data from overwhelming the database essentially acting as a shield during high-traffic periods.

3.2.4 External Services

- **Stripe:** Payment processing platform for subscription billing, checkout sessions, and webhook handling.
- **Google OAuth 2.0:** Identity provider for social login functionality.

- **Apple Sign-In:** Authentication service for iOS and web users.

These third-party services were selected for their reliability, comprehensive documentation, and industry adoption, reducing development time while ensuring security and compliance.

3.3 Database Design

The database schema is designed to support user management, authentication, subscription tracking, and service plan versioning. MongoDB's document-oriented approach allows for flexible schema evolution.

3.3.1 Core Collections

The system utilizes the following primary collections:

Users Collection

The `users` collection stores user account information and authentication credentials.

Field	Type	Description
<code>_id</code>	<code>ObjectId</code>	Primary key
<code>email</code>	<code>String</code>	User email (unique)
<code>password</code>	<code>String</code>	Hashed password
<code>name</code>	<code>String</code>	Full name
<code>role</code>	<code>String</code>	User role (user/admin)
<code>type</code>	<code>String</code>	Account type (trial/paid)
<code>isVerified</code>	<code>Boolean</code>	Email verification status

Table 3.4: Users Collection Schema

Subscriptions Collection

The `subscriptions` collection tracks user subscriptions and quota usage.

Field	Type	Description
_id	ObjectId	Primary key
user	ObjectId	Reference to users collection
stripeSubscriptionId	String	Stripe subscription ID
stripeCustomerId	String	Stripe customer ID
planName	String	Current plan name
priceId	String	Stripe price ID
planId	String	Internal plan identifier
scheduledPriceId	String	Next scheduled price ID
scheduledPlanId	String	Next scheduled plan ID
scheduledPlanName	String	Next scheduled plan name
stripeScheduleId	String	Stripe schedule ID
status	String	Subscription status (active, canceled, etc.)
quota	Object	Service quotas (batch, live duration)
usage	Object	Current usage tracking
startDate	Date	Subscription start date
endDate	Date	Subscription end date

Table 3.5: Subscriptions Collection Schema

The `quota` and `usage` fields store nested objects tracking batch and live processing durations in seconds. A value of -1 indicates unlimited access.

Plans Collection

The `plans` collection maintains versioned service plans.

Field	Type	Description
_id	ObjectId	Primary key
id	String	Unique plan identifier
plans	String	JSON string of plan details
version	Number	Plan version (auto-increment)
createdAt	Date	Creation timestamp

Table 3.6: Plans Collection Schema

Storing plans as JSON strings enables dynamic schema evolution without database migrations.

3.3.2 Authentication Collections

To ensure secure session management, two additional collections were introduced:

UserTokens Collection

The `usertokens` collection tracks active JWT tokens for each user.

Field	Type	Description
_id	ObjectId	Primary key
userId	String	User identifier
token	String	JWT token string
expiresAt	Date	Token expiration (TTL indexed)
userAgent	String	Client user agent
ipAddress	String	Client IP address

Table 3.7: UserTokens Collection Schema

MongoDB’s TTL (Time-To-Live) index on `expiresAt` automatically removes expired tokens.

TokenBlacklist Collection

The `tokenblacklists` collection stores revoked tokens to prevent reuse.

Field	Type	Description
_id	ObjectId	Primary key
token	String	Revoked JWT token
userId	String	User identifier
expiresAt	Date	Original token expiration
reason	String	Revocation reason

Table 3.8: TokenBlacklist Collection Schema

3.3.3 Entity Relationships

Figure 3.4 illustrates the relationships between core collections:

- Each `user` has zero or one `subscription`.
- Each `subscription` references a `plan` by Stripe `priceId`.
- Each `user` may have multiple active `tokens`.
- Revoked tokens are stored in `tokenblacklist`.

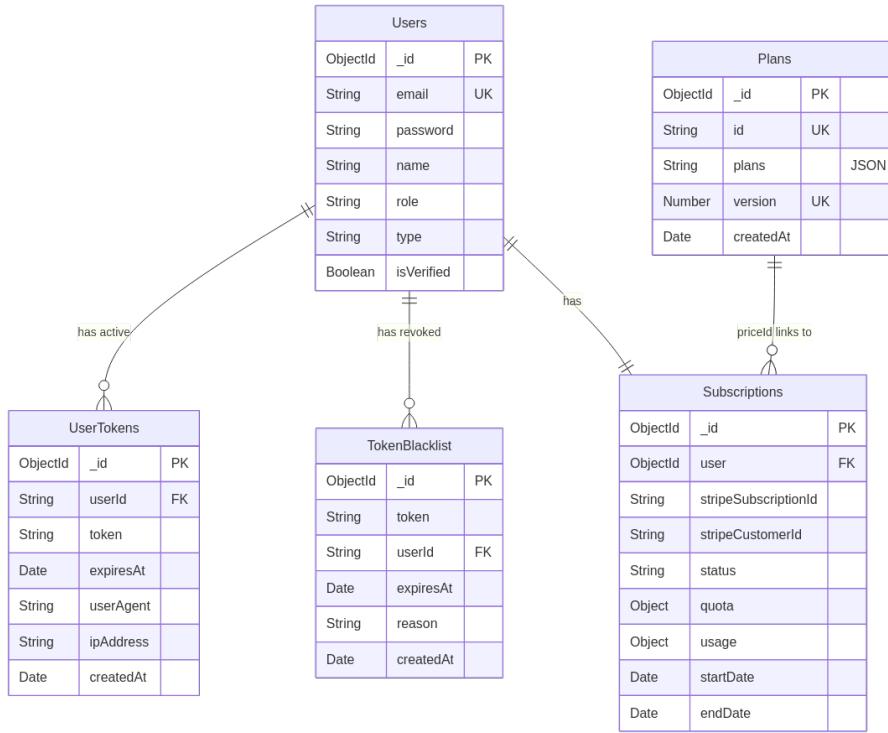


Figure 3.4: Entity Relationship Diagram

The Entity Relationship Diagram in Figure 3.4 showcases the database schema. The **Users** collection is central, linking to **Subscriptions** (1:1 relationship) and multiple **UserTokens**. The **Subscriptions** collection contains embedded objects for **quota** and **usage**, allowing efficient tracking of service limits. The **Plans** collection stands independently but is logically referenced by subscriptions via price IDs. The **TokenBlacklist** stores revoked tokens, ensuring security compliance.

Chapter 4

Detailed Implementation

This chapter provides a comprehensive examination of the key implementation details of the Gateway Dashboard system. It is organized into two main parts: Backend Implementation covering authentication and payment systems, and Frontend Development covering the Vue.js dashboard application.

4.1 Backend Implementation

This section covers the server-side implementation including Single Sign-On (SSO) authentication and payment/subscription management.

4.1.1 SSO Implementation

This subsection provides a comprehensive examination of the authentication system implemented in the Gateway Dashboard. It covers the supported authentication methods, detailed flow descriptions, and key implementation details.

Overview

The Gateway Dashboard supports three authentication methods:

- **Google OAuth 2.0:** Full OAuth flow with Passport.js strategy
- **Apple Sign-In:** POST callback with JWT token verification
- **Traditional Email/Password:** bcrypt-hashed credentials

Figure 4.1 illustrates the SSO architecture showing how both providers integrate with the AuthService.

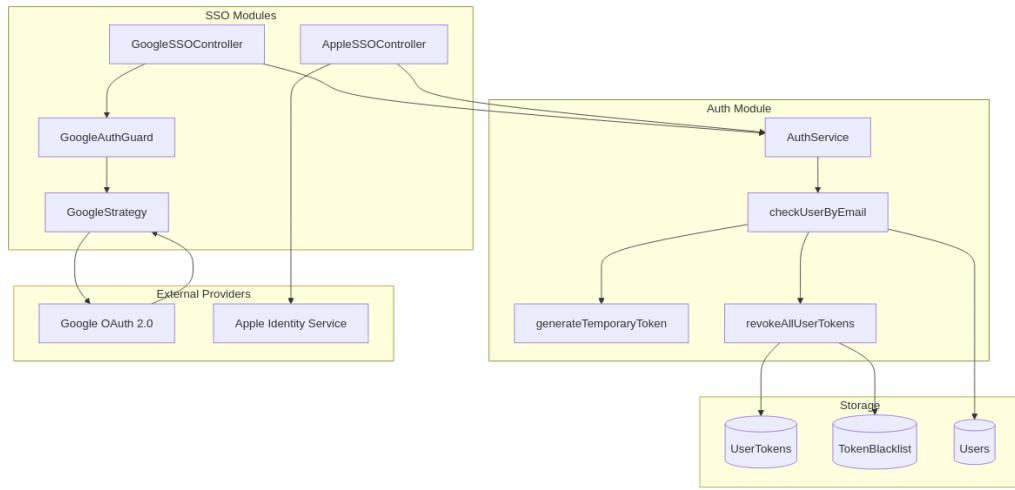


Figure 4.1: SSO Authentication Architecture

Both SSO providers share a common flow: after identity verification, the system checks if the user exists. For new users, a temporary token is generated requiring password setup; for existing users, an access token is issued directly.

Google OAuth 2.0 Implementation

Google SSO uses the `passport-google-oauth20` strategy integrated with NestJS guards.

Google OAuth Flow

Figure 4.2 shows the complete OAuth flow including state parameter handling.

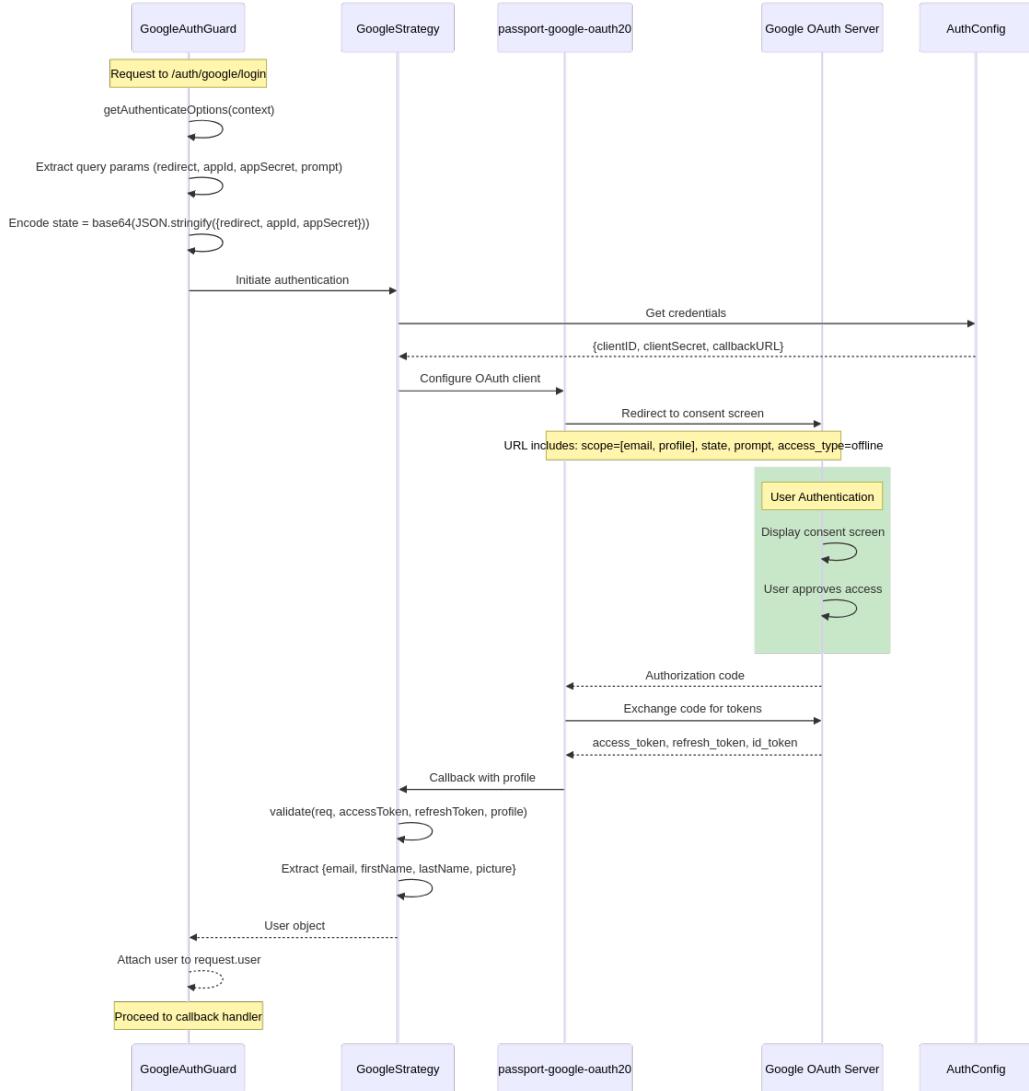


Figure 4.2: Google OAuth 2.0 Authentication Flow

Google Strategy

The strategy is configured with OAuth credentials and requests email and profile scopes:

```

1  @Injectable()
2  export class GoogleStrategy extends PassportStrategy(Strategy, 'google') {
3      constructor(
4          @Inject(authConfig.KEY)
5          private auth: ConfigType<typeof authConfig>,
6      ) {
7          super({
8              clientId: auth.googleClientId,
9              clientSecret: auth.googleClientSecret,
10             callbackURL: auth.googleCallbackURL,
11             scope: ['email', 'profile'],
12             passReqToCallback: true,
13         })
14     }

```

```
15
16  async validate(
17    req: any,
18    accessToken: string,
19    _refreshToken: string,
20    profile: any,
21    done: VerifyCallback,
22  ): Promise<any> {
23    const { name, emails, photos } = profile
24    const user = {
25      email: emails[0].value,
26      firstName: name.givenName,
27      lastName: name.familyName,
28      picture: photos[0].value,
29      accessToken,
30    }
31    done(null, user)
32  }
33 }
```

Listing 4.1: Google Strategy Configuration

State Parameter for CSRF Protection

Figure 4.3 illustrates how state parameters are preserved through the OAuth redirect.

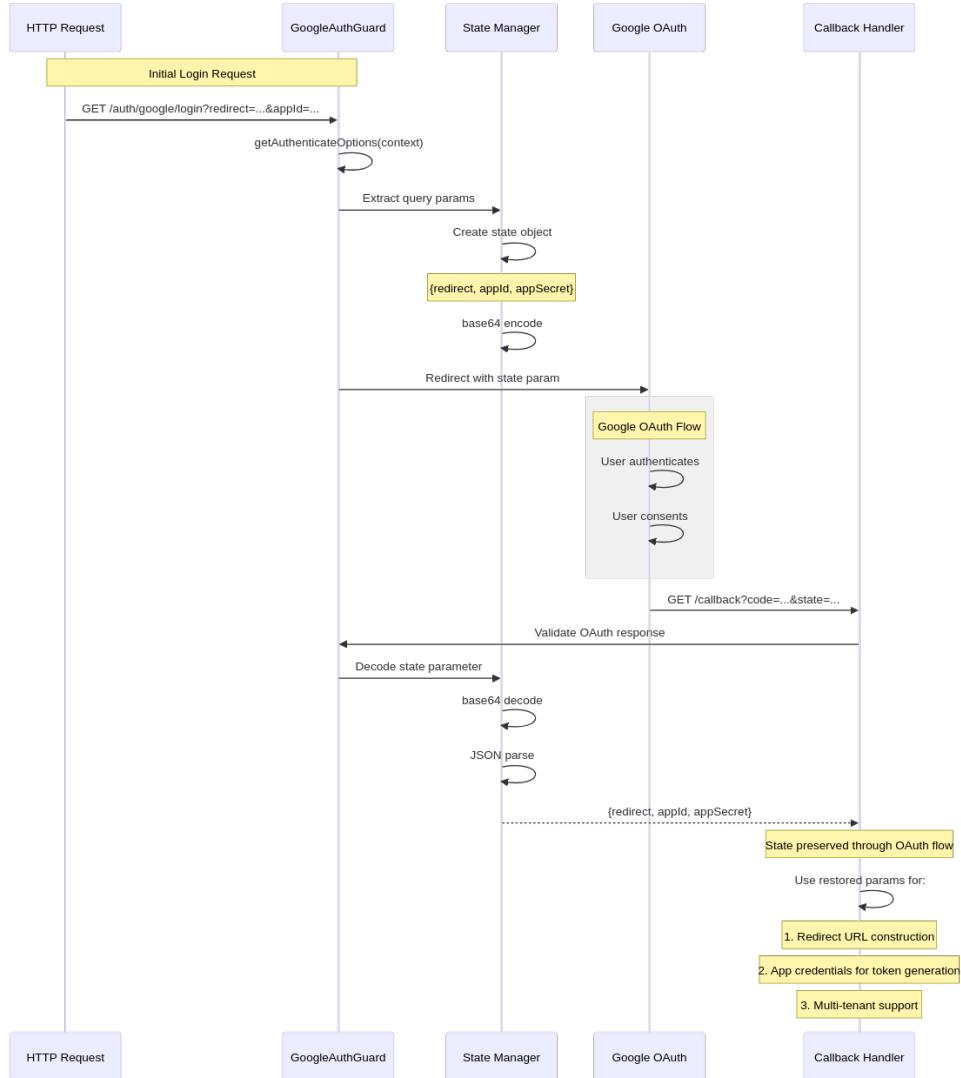


Figure 4.3: State Parameter Encoding Flow

The `GoogleAuthGuard` encodes query parameters into a base64 state parameter:

```

1  @Injectable()
2  export class GoogleAuthGuard extends AuthGuard('google') {
3      getAuthenticateOptions(context: ExecutionContext) {
4          const request = context.switchToHttp().getRequest()
5          const { redirect, appId, appSecret, prompt } = request.query
6
7          // Encode query parameters into state to preserve them through OAuth flow
8          const state = JSON.stringify({
9              redirect: redirect || null,
10             appId: appId || null,
11             appSecret: appSecret || null,
12         })
13
14
15         return {
16             state: Buffer.from(state).toString('base64'),
17             prompt: prompt || 'select_account', // Force account selection
18             access_type: 'offline', // For refresh tokens
19         }
20     }
21
22 }

```

```

19  }
20 }
```

Listing 4.2: Google Auth Guard with State Encoding

Apple Sign-In Implementation

Figure 4.4 shows the Apple Sign-In flow which uses POST callback instead of redirect-based OAuth.

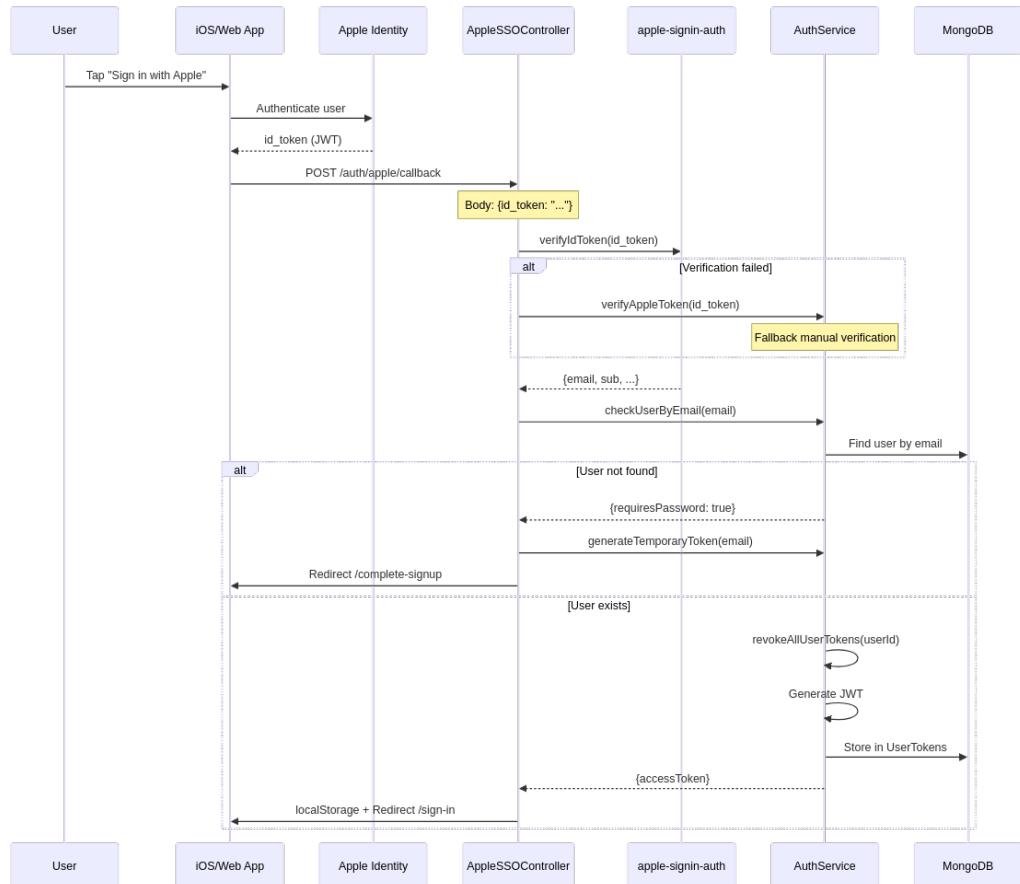


Figure 4.4: Apple Sign-In Authentication Flow

Token Verification

Apple tokens are verified using the `apple-signin-auth` library with fallback to manual verification:

```

1  @Controller('auth/apple')
2  export class AppleSSOController {
3      constructor(private readonly authService: AuthService) {}
4
5      @Post('callback')
6      async appleAuthCallback(@Body() body: AppleAuthDto, @Res() res: Response) {
7          if (!body.code && !body.id_token) {
8              return res.status(HttpStatus.UNAUTHORIZED).json({
9                  message: 'Apple authentication failed: No id_token received',
10             })
11     }
12 }
```

```

11  }
12
13  let appleResponse
14  try {
15    appleResponse = await appleSignin.verifyIdToken(body.id_token, {
16      audience: process.env.APPLE_CLIENT_ID,
17      ignoreExpiration: false,
18    })
19  } catch (verifyError) {
20    // Fallback to manual verification
21    appleResponse = await this.authService.verifyAppleToken(body.id_token)
22  }
23
24  const result = await this.authService.checkUserByEmail(appleResponse.email)
25  // Handle new/existing user and redirect
26
27 }

```

Listing 4.3: Apple SSO Controller

Token Management

Figure 4.5 illustrates the complete token lifecycle from generation to revocation.

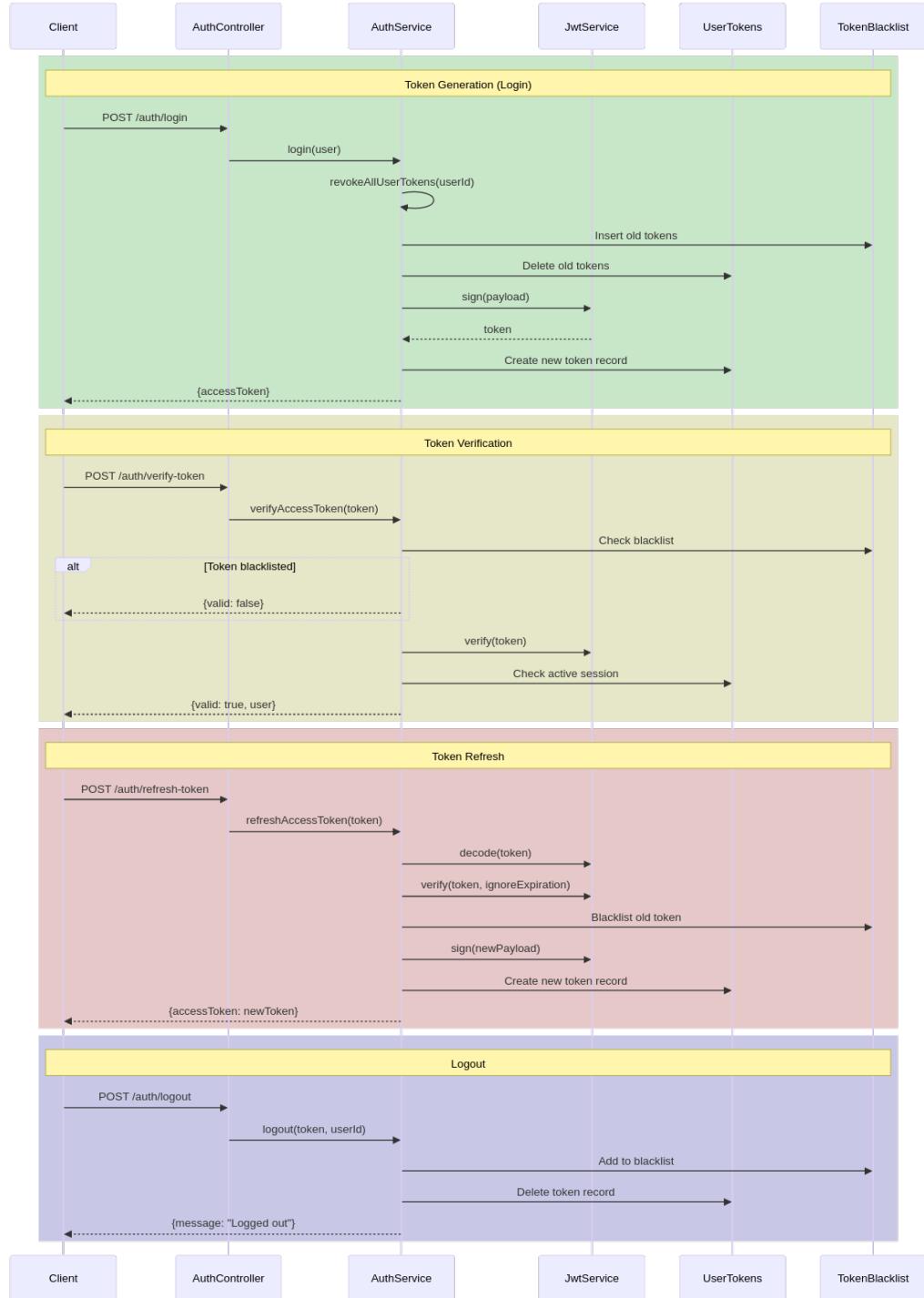


Figure 4.5: JWT Token Lifecycle Management

When users authenticate via SSO:

- New Users:** A 15-minute temporary JWT is generated with `need_password: true`. The frontend redirects to `/complete-signup` where the user sets a password.
- Existing Users:** All previous tokens are revoked (single-session policy), a new JWT is issued, and stored in the `usertokens` collection.
- Token Revocation:** On new login, all active tokens are blacklisted in `tokenblacklists` collection.

Token Blacklisting Flow

Figure 4.6 shows how tokens are blacklisted for security.

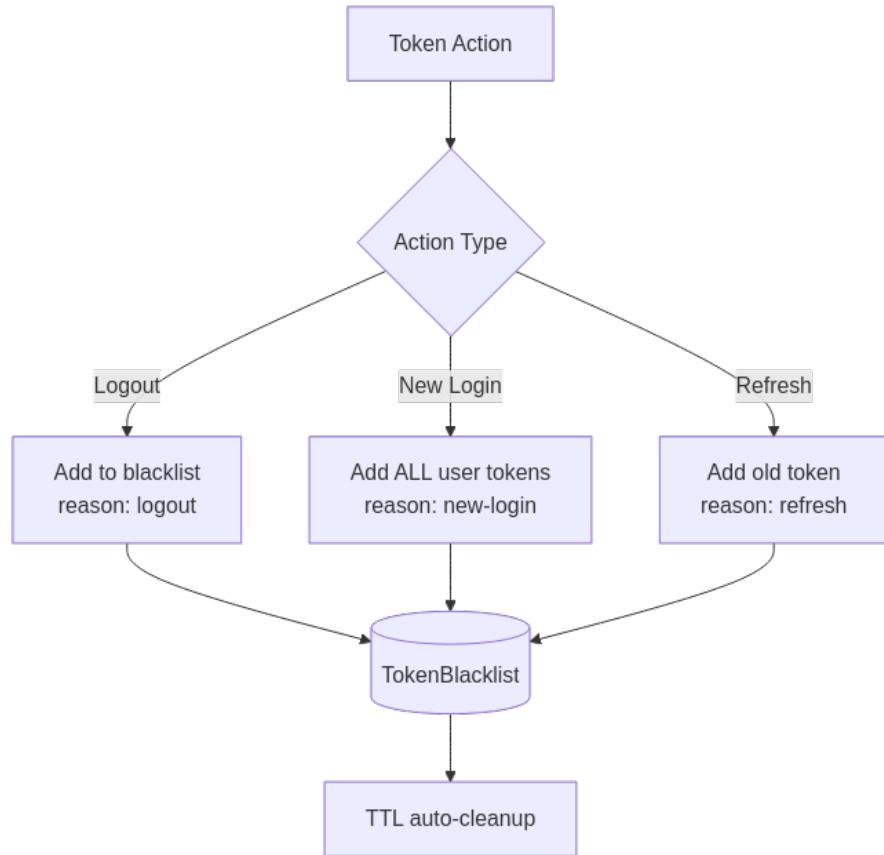


Figure 4.6: Token Blacklisting Flow

```
1  async generateTemporaryToken(email: string, appId?: string): Promise<string> {
2    const payload = {
3      email: email.toLowerCase(),
4      need_password: true,
5      appId: appId || null,
6    }
7    return this.jwtService.sign(payload, { expiresIn: '15m' })
8 }
```

Listing 4.4: Temporary Token Generation

Module Structure

Figure 4.7 shows the Google SSO module organization.

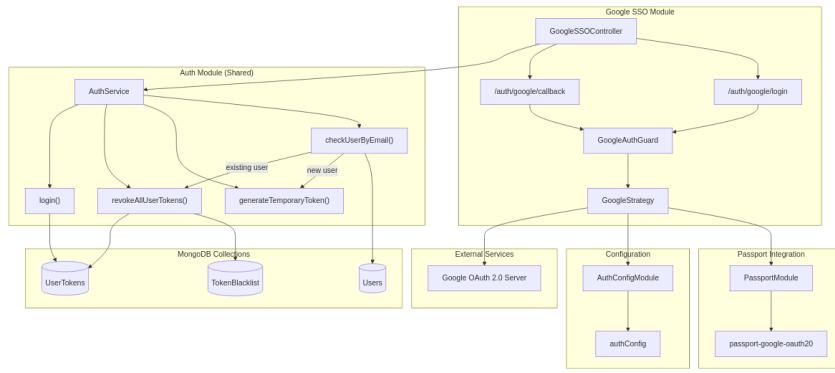


Figure 4.7: Google SSO Module Structure

The SSO modules are organized as independent NestJS modules:

- `GoogleSSOModule`: Imports `PassportModule`, `AuthModule`; provides `GoogleStrategy`
 - `AppleSSOModule`: Imports `AuthModule`; uses `apple-signin-auth` library

Both modules delegate user creation and authentication logic to the shared AuthService.

4.1.2 Payment & Subscription Management

This subsection documents the payment processing and subscription management system built with Stripe integration, Redis caching, and MongoDB persistence.

Architecture Overview

Figure 4.8 illustrates the payment system architecture showing the interaction between modules.

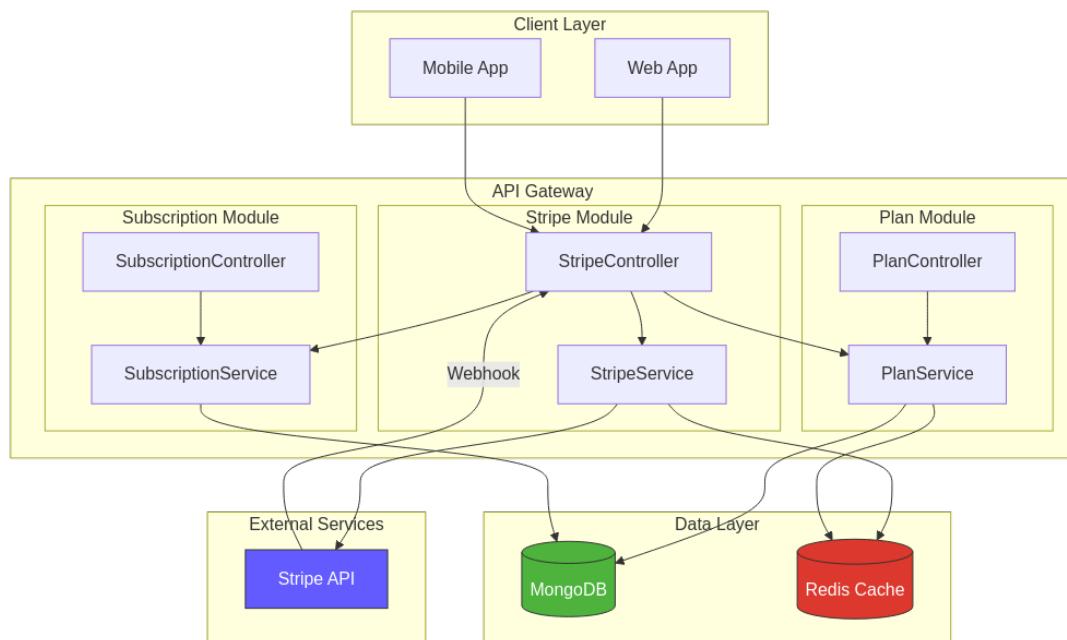


Figure 4.8: Payment System Architecture

The payment system consists of three main modules:

- **StripeModule**: Handles Stripe API interactions, checkout sessions, webhooks
- **PlanModule**: Manages subscription plans with versioning and Redis caching
- **SubscriptionModule**: Tracks user subscriptions, quotas, and usage

Plan Management

Plans are stored as versioned JSON documents, cached in Redis for fast retrieval.

Plan Schema

```

1  @Schema({ timestamps: { createdAt: true, updatedAt: false } })
2  export class Plan extends Document {
3    @Prop({ required: true, type: String, unique: true })
4    id: string;
5
6    @Prop({ required: true, type: String })
7    plans: string; // JSON string of plan details
8
9    @Prop({ required: true, type: Number, unique: true })
10   version: number;
11
12   createdAt?: Date;
13 }
```

Listing 4.5: Plan Schema Definition

Plan Versioning

Figure 4.9 shows how plan versions are managed over time.

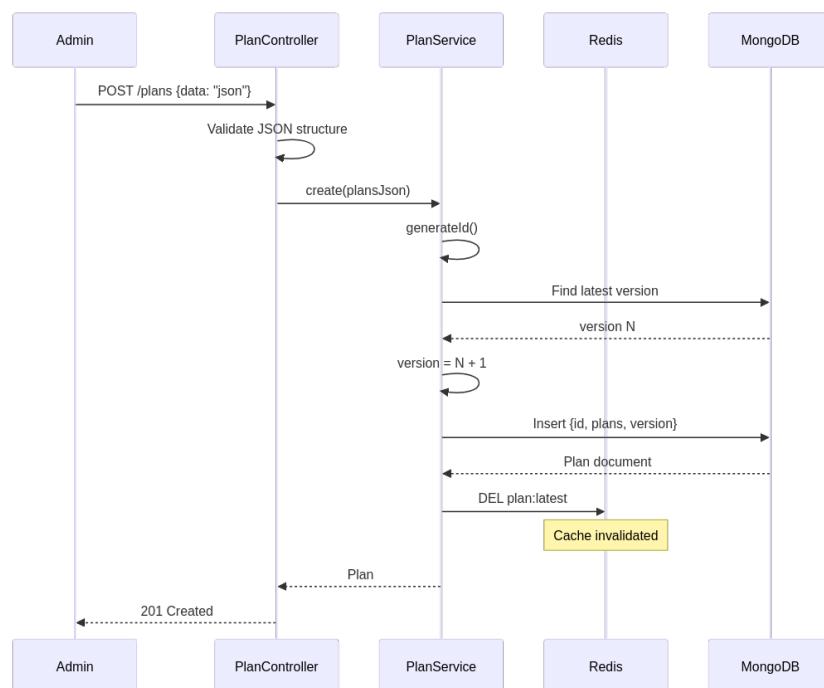
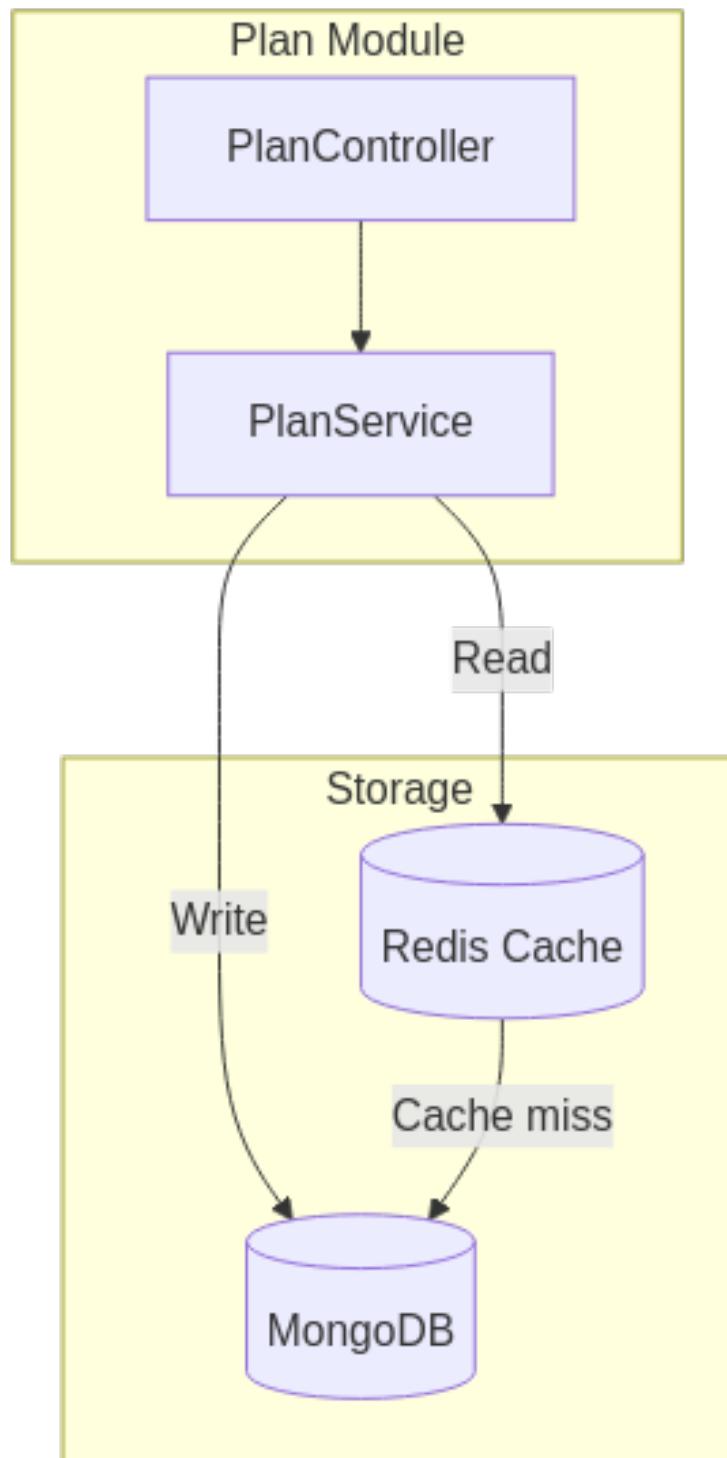


Figure 4.9: Plan Versioning Flow

Redis Caching with Cache Penetration Protection

Figure 3.2 illustrates the cache-aside pattern with NULL value caching.



```
1 @Injectable()
2 export class PlanService implements OnModuleInit, OnModuleDestroy {
3     private readonly CACHE_KEY = 'plan:latest';
4     private readonly CACHE_TTL = 3600; // 1 hour
```

```

5   private readonly NULL_TTL = 60; // 60 seconds
6
7   async getLatestVersion(): Promise<Plan | null> {
8     const cached = await this.redisClient.get(this.CACHE_KEY);
9     if (cached) {
10       if (cached === 'NULL') return null; // Cache penetration protection
11       return JSON.parse(cached) as Plan;
12     }
13
14     const latestPlan = await this.planModel
15       .findOne().sort({ version: -1 }).exec();
16
17     if (latestPlan) {
18       await this.redisClient.set(this.CACHE_KEY, JSON.stringify(latestPlan), {
19         EX: this.CACHE_TTL,
20       });
21     } else {
22       await this.redisClient.set(this.CACHE_KEY, 'NULL', {
23         EX: this.NULL_TTL,
24       });
25     }
26     return latestPlan;
27   }
28 }
```

Listing 4.6: Plan Caching Implementation

Stripe Integration

Checkout Flow

Figure 4.10 shows the complete Stripe Checkout flow from user request to subscription creation.

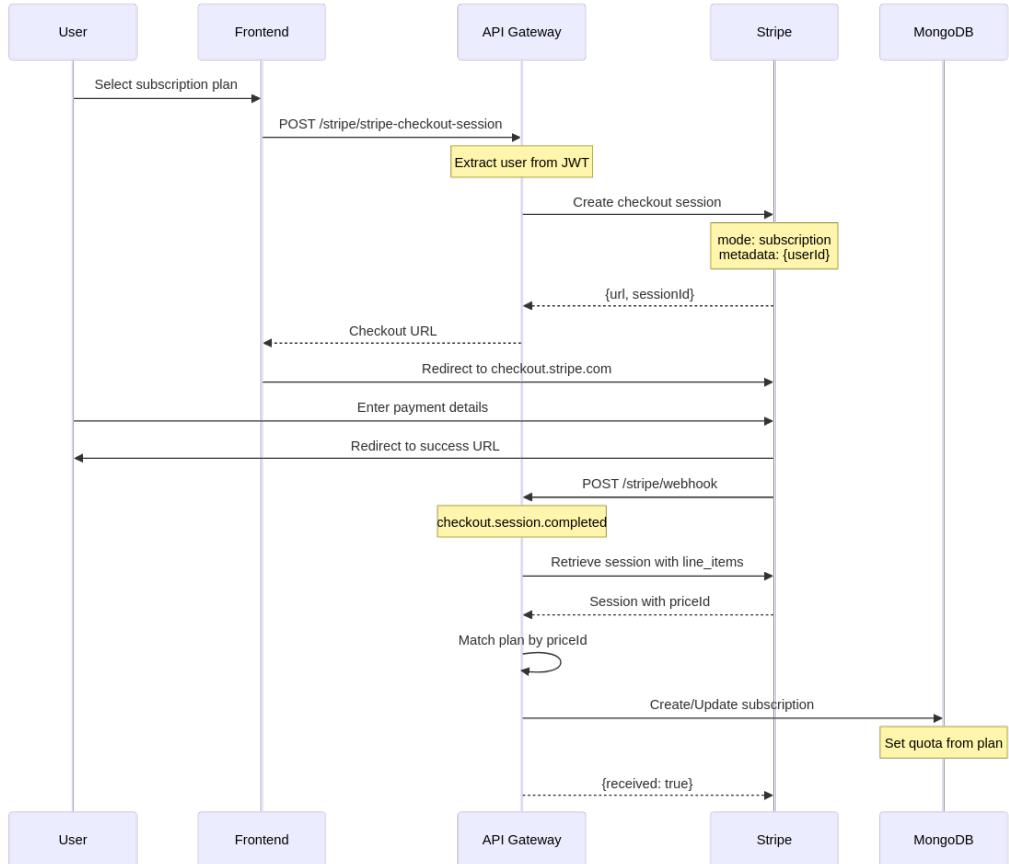


Figure 4.10: Stripe Checkout Session Flow

Checkout Session Creation

```

1  @UseGuards(JwtAuthGuard)
2  @Post('stripe-checkout-session')
3  async createCheckoutSession(@Body() dto: CreateCheckoutSessionDto, @Req() req) {
4      const userId = req.user?._id?.toString();
5      const customerEmail = req.user?.email;
6
7      const result = await this.stripeService.createCheckoutSession(
8          dto.priceId,
9          customerEmail,
10         customerName,
11         userId, // Stored in metadata for webhook
12     );
13     return result;
14 }

```

Listing 4.7: Checkout Session Creation

Webhooks process subscription events with signature verification:

```

1  @Post('webhook')
2  async handleWebhook(@Headers('stripe-signature') signature, @Req() req) {
3      const payload = req.body as Buffer;
4      const event = await this.stripeService.handleWebhook(payload, signature);

```

```

5
6   switch (event.type) {
7     case 'checkout.session.completed':
8       const session = event.data.object;
9       const fullSession = await this.stripeService.getSessionWithLineItems(
10         session.id
11       );
12       const userId = fullSession.metadata?.userId;
13       const priceId = fullSession.line_items?.data?.[0]?.price?.id;
14
15       // Find matching plan and create/update subscription
16       const latestPlans = await this.planService.getLatestVersion();
17       const plansData = JSON.parse(latestPlans.plans);
18       const matchingPlan = plansData.plans.find(p => p.priceId === priceId);
19       // ... create or update subscription
20       break;
21
22     case 'subscription_schedule.updated':
23       // Update scheduled plan change info
24       break;
25
26     case 'subscription_schedule.released':
27       // Clear scheduled change fields
28       break;
29   }
30   return { received: true };
31 }

```

Listing 4.8: Stripe Webhook Handler

Subscription Management

Subscription Schema

```

1 export class Subscription extends Document {
2   @Prop({ required: true, ref: User.name, type: ObjectId })
3   user: string | User;
4
5   @Prop({ type: String }) stripeSubscriptionId?: string;
6   @Prop({ type: String }) stripeCustomerId?: string;
7   @Prop({ type: String }) planName?: string;
8   @Prop({ type: String }) priceId?: string;
9   @Prop({ type: String }) planId?: string;
10
11  // Scheduled change fields (for plan upgrades/downgrades)
12  @Prop({ type: String }) scheduledPriceId?: string;
13  @Prop({ type: String }) scheduledPlanId?: string;
14  @Prop({ type: String }) scheduledPlanName?: string;
15  @Prop({ type: String }) stripeScheduleId?: string;
16
17  @Prop({ type: String, enum: ['active', 'canceled', ...], default: 'active' })
18  status: string;

```

```
19  
20 @Prop(raw({ batchDuration: Number, liveDuration: Number }))  
21 quota: SubscriptionUnit;  
22  
23 @Prop(raw({ batchDuration: Number, liveDuration: Number }))  
24 usage: SubscriptionUnit;  
25  
26 @Prop({ type: Date }) startDate: Date;  
27 @Prop({ type: Date }) endDate: Date;  
28 }
```

Listing 4.9: Subscription Schema (Key Fields)

Quota Checking

Figure 4.11 illustrates the subscription and quota validation flow.

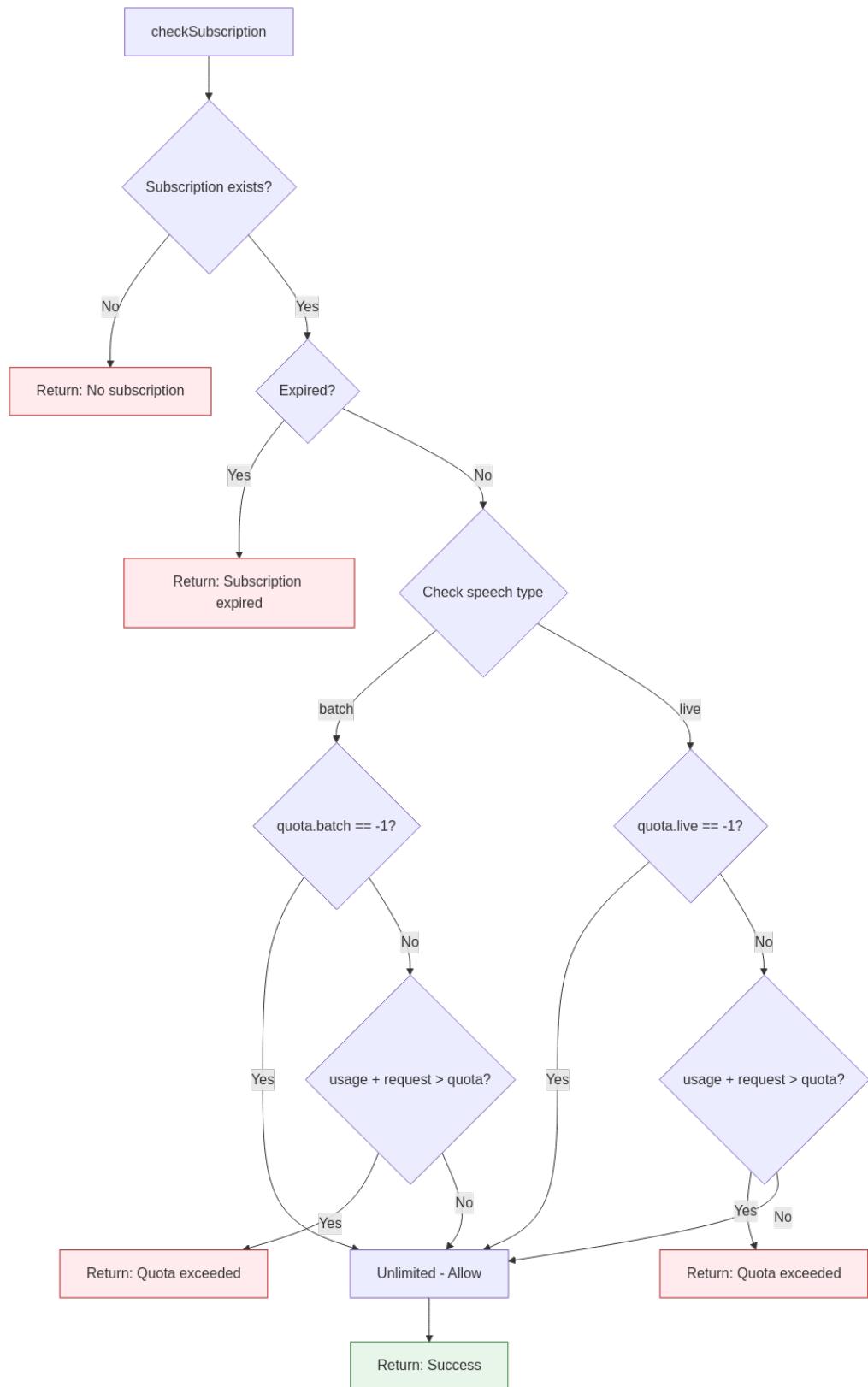


Figure 4.11: Subscription Quota Checking Flow

```

1  async checkSubscription(userId: string, speechType?: 'live' | 'batch') {
2    const sub = await this.subscriptionModel.findOne({ user: userId }).exec();
3
4    if (!sub) return { success: false, message: 'User has no subscription' };

```

```
5   if (speechType === 'batch' && sub.quota.batchDuration !== -1 &&
6     sub.usage.batchDuration > sub.quota.batchDuration) {
7     return { success: false, message: 'Batch quota exceeded' };
8   }
9
10  return { success: true, subscription: sub };
11}
12}
```

Listing 4.10: Subscription Validation

Stripe Price Caching

Figure 4.12 shows the price caching mechanism with cache penetration protection.

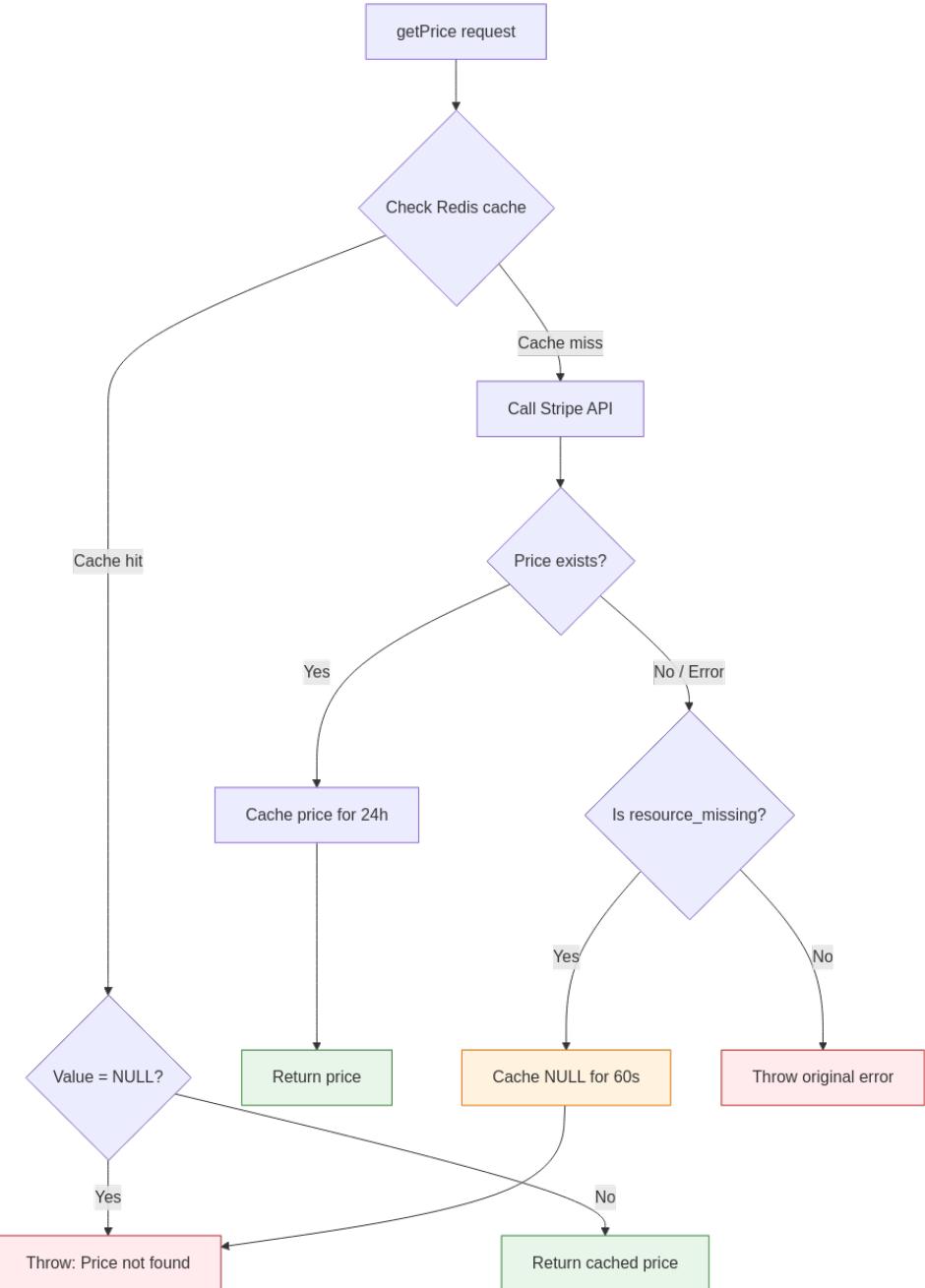


Figure 4.12: Stripe Price Caching with Penetration Protection

```

1  async getPrice(priceId: string): Promise<Stripe.Price> {
2    const cacheKey = `stripe:price:${priceId}`;
3    const cached = await this.redisClient.get(cacheKey);
4
5    if (cached) {
6      if (cached === 'NULL') throw new Error('Price not found (cached)');
7      return JSON.parse(cached) as Stripe.Price;
8    }
9
10   try {
11     const price = await this.stripe.prices.retrieve(priceId);
12     await this.redisClient.set(cacheKey, JSON.stringify(price), {

```

```

13     EX: this.CACHE_TTL, // 24 hours
14   });
15   return price;
16 } catch (error) {
17   if (error?.code === 'resource_missing') {
18     await this.redisClient.set(cacheKey, 'NULL', { EX: 60 });
19   }
20   throw error;
21 }
22 }

```

Listing 4.11: Stripe Price Caching

Module Dependencies

The Stripe module integrates with Subscription and Plan modules:

```

1 @Module({
2   imports: [
3     StripeConfigurationModule,
4     MongooseModule.forRoot([
5       { name: Subscription.name, schema: SubscriptionSchema },
6       { name: Plan.name, schema: PlanSchema },
7     ]),
8   ],
9   controllers: [StripeController],
10  providers: [StripeService, SubscriptionService, PlanService],
11  exports: [StripeService],
12})
13 export class StripeModule {}

```

Listing 4.12: Stripe Module Configuration

4.2 Frontend Implementation

This section details the frontend implementation of the Gateway Dashboard, including the Vue.js architecture, component structure, routing implementation, and subscription management interface.

4.2.1 Overview

The Gateway Dashboard is a Vue.js 2 web application that provides a management interface for the Speech Gateway API.

Frontend Architecture

Figure 4.13 illustrates the layered architecture of the frontend application.

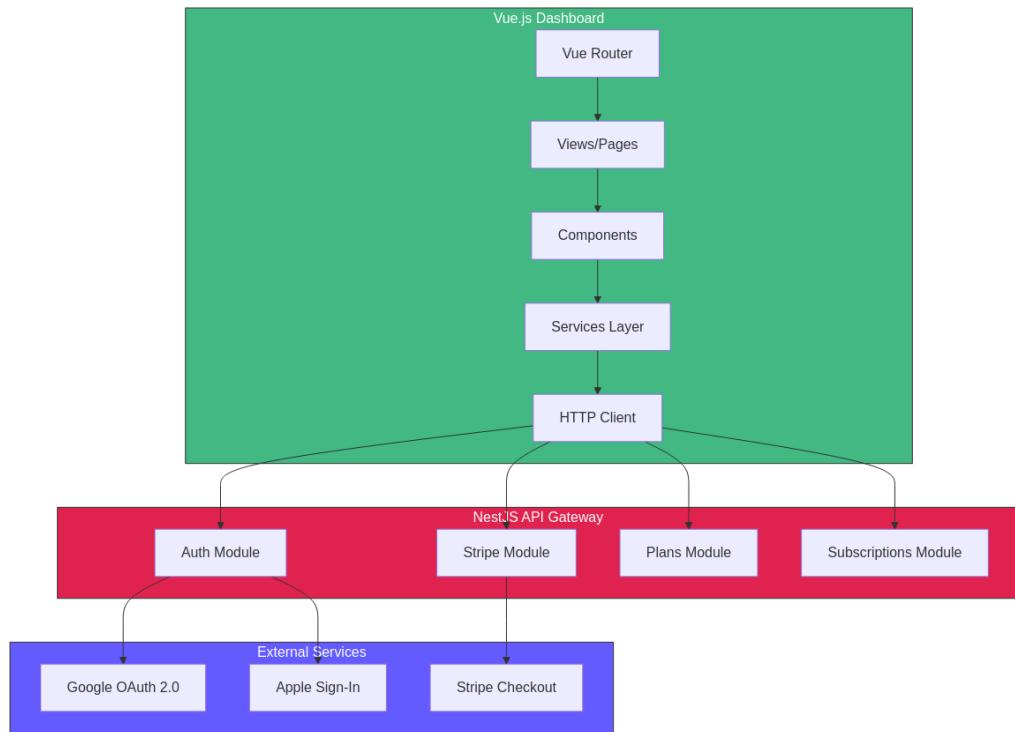


Figure 4.13: Frontend Application Architecture

The frontend follows a layered architecture:

- **Vue Router**: Manages navigation and route guards.
- **Views/Pages**: Page-level components for each route.
- **Components**: Reusable UI components like PlanCard.
- **Services Layer**: API communication logic.
- **HTTP Client**: Axios with interceptors for token handling.

Technology Stack

Layer	Technology	Purpose
Framework	Vue.js 2.x	Reactive UI framework
UI Library	Vuetify 2.x	Material design components
HTTP Client	Axios	API communication
Router	Vue Router	SPA navigation
State	Vue Instance + Mixins	Application state
Payment	Stripe Checkout	Subscription processing

Table 4.1: Frontend Technology Stack

Project Structure

```

1  gateway-dashboard/
2    src/

```

```

3   components/
4     PlanCard.vue          # Subscription plan display
5   layouts/
6     Main.vue              # Main app layout
7   mixins/
8     auth.mixin.js         # Auth functionality mixin
9   router/
10    index.js              # Route definitions
11    hooks.js              # Navigation guards
12   services/
13    auth.service.js       # Authentication API
14    plans.service.js      # Plans API
15    stripe.service.js     # Stripe integration
16    user.service.js       # User/subscription API
17   views/
18    SignIn.vue            # Login page
19    SignUp.vue            # Registration page
20    CompleteSignup.vue   # OAuth completion
21    Subscription.vue      # Subscription management
22    admin/
23      JsonPlansEditor.vue # Admin plans editor
24   http.js                # Axios HTTP client
25   main.js                # App entry point

```

Listing 4.13: Frontend Project Structure

4.2.2 Authentication Frontend

The frontend authentication system supports three login methods: email/password, Google OAuth, and Apple Sign-In.

Auth Service Architecture

The AuthService manages all authentication operations and token storage.

Method	Description
login()	Email/password authentication
register()	New account registration
initiateGoogleLogin()	Redirect to Google OAuth
initiateAppleLogin()	Apple SDK sign-in flow
refreshToken()	Refresh expired JWT
storeAuthData()	Store token in localStorage
clearAuthData()	Clear token on logout

Table 4.2: Auth Service Methods

Token Storage

Authentication data is stored in localStorage for persistence:

```

1  {
2    accessToken: "eyJhbGciOiJIUzI1NiIs...",

```

```

3   jwt: "eyJhbGciOiJIUzI1NiIs...",
4   subscriptionEnd: "1737244800000", // Unix timestamp
5   isVerified: "true"
6 }
```

Listing 4.14: LocalStorage Token Schema

OAuth Integration

Google OAuth

Google OAuth uses redirect-based authentication:

```

1 initiateGoogleLogin() {
2   const frontendUrl = encodeURIComponent(window.location.origin)
3   const redirectUrl = `${API_URL}/auth/google/login` +
4     '?redirect=' + encodeURIComponent(frontendUrl) + '/sign-in'
5
6   window.location.href = redirectUrl
7 }
```

Listing 4.15: Google OAuth Initiation

Apple Sign-In

Apple Sign-In uses the Apple SDK:

```

1 initializeAppleSignIn(clientId) {
2   if (!window.AppleID) {
3     console.warn('Apple SDK not loaded')
4     return false
5   }
6
7   window.AppleID.auth.init({
8     clientId: clientId || process.env.VUE_APP_APPLE_CLIENT_ID,
9     scope: 'name email',
10    redirectURI: `${API_URL}/auth/apple/callback`,
11    usePopup: false
12  })
13  return true
14 }
15
16 async initiateAppleLogin() {
17   await window.AppleID.auth.signIn()
18 }
```

Listing 4.16: Apple Sign-In Initialization

Complete Signup Flow

New OAuth users must complete signup by setting a password:

```

1 async setPassword(temporaryToken, password, fullname) {
2   const response = await http.post('/auth/add-info', {
3     token: temporaryToken,
4     password,
```

```

5     fullname
6   })
7
8   const { accessToken, subscriptionEnd, isVerified } =
9     response.data
10  this.storeAuthData(accessToken, subscriptionEnd, isVerified)
11
12  localStorage.removeItem('temporaryToken')
13  return response.data
14 }

```

Listing 4.17: Complete Signup Implementation

Auth Mixin

The auth mixin provides authentication state to components:

```

1 import { authMixin } from '@/mixins/auth.mixin'
2
3 export default {
4   mixins: [authMixin],
5   // Component now has access to:
6   // - this.isAuthenticated
7   // - this.accessToken
8   // - this.subscriptionEnd
9   // - this.logout()
10  // - this.verifyAndRefreshToken()
11 }

```

Listing 4.18: Auth Mixin Usage

The mixin automatically starts token verification on mount and cleans up on destroy.

4.2.3 Routing and Navigation

Vue Router manages navigation with guards that enforce authentication and role-based access control.

Route Configuration

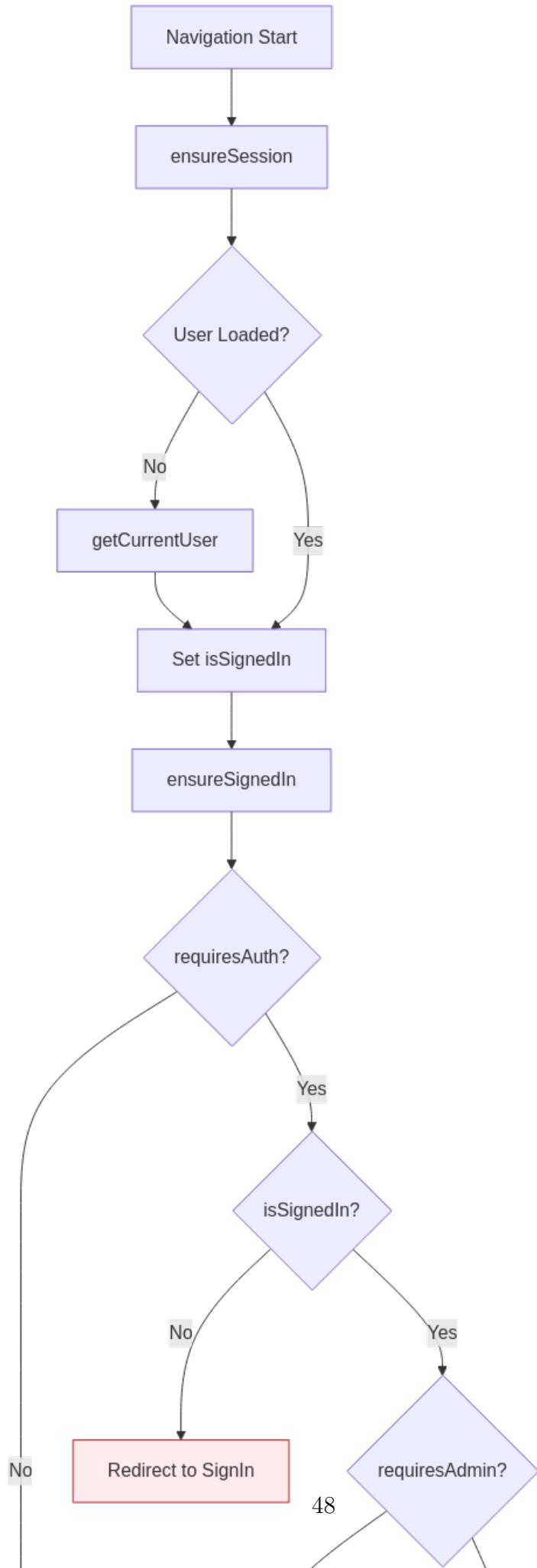
Routes are categorized by authentication requirements:

Path	Auth	Admin	Component
/sign-in	No	No	SignIn.vue
/sign-up	No	No	SignUp.vue
/complete-signup	No	No	CompleteSignup.vue
/success	No	No	Success.vue
/cancel	No	No	Cancel.vue
/speeches	Yes	No	Speeches.vue
/files	Yes	No	Files.vue
/applications	Yes	No	Applications.vue
/subscription	Yes	No	Subscription.vue
/dashboard	Yes	Yes	Dashboard.vue
/users	Yes	Yes	Users.vue
/request-log	Yes	Yes	RequestLog.vue
/settings	Yes	Yes	Settings.vue

Table 4.3: Route Definitions

Navigation Guards Flow

Figure 4.14 illustrates the navigation guard logic.



Guard Implementation

Two navigation guards work together:

Session Guard

Ensures user data is loaded before navigation:

```
1 export const ensureSession = router => async (to, from, next) => {
2   await Vue.nextTick()
3
4   if (!router.app.user && to.name !== 'SignIn') {
5     const user = await router.app.getCurrentUser()
6     to.meta.isSignedIn = !!user
7   } else {
8     to.meta.isSignedIn = router.app.user !== null
9   }
10  next()
11 }
```

Listing 4.19: Session Guard

Auth Guard

Enforces authentication and admin requirements:

```
1 export const ensureSignedIn = router => (to, from, next) => {
2   const requiresAdmin = anyTrue(to, 'requiresAdmin')
3   const requiresAuth = requiresAdmin || anyTrue(to, 'requiresAuth')
4
5   if (requiresAuth) {
6     if (!to.meta.isSignedIn) {
7       next({ name: 'SignIn' })
8     } else if (requiresAdmin &&
9                 router.app.user.role !== 'admin') {
10       next({ name: 'Speeches' })
11     } else {
12       next()
13     }
14   } else {
15     next()
16   }
17 }
```

Listing 4.20: Auth Guard

HTTP Interceptors

Figure 4.15 shows the HTTP interceptor flow for automatic token handling.

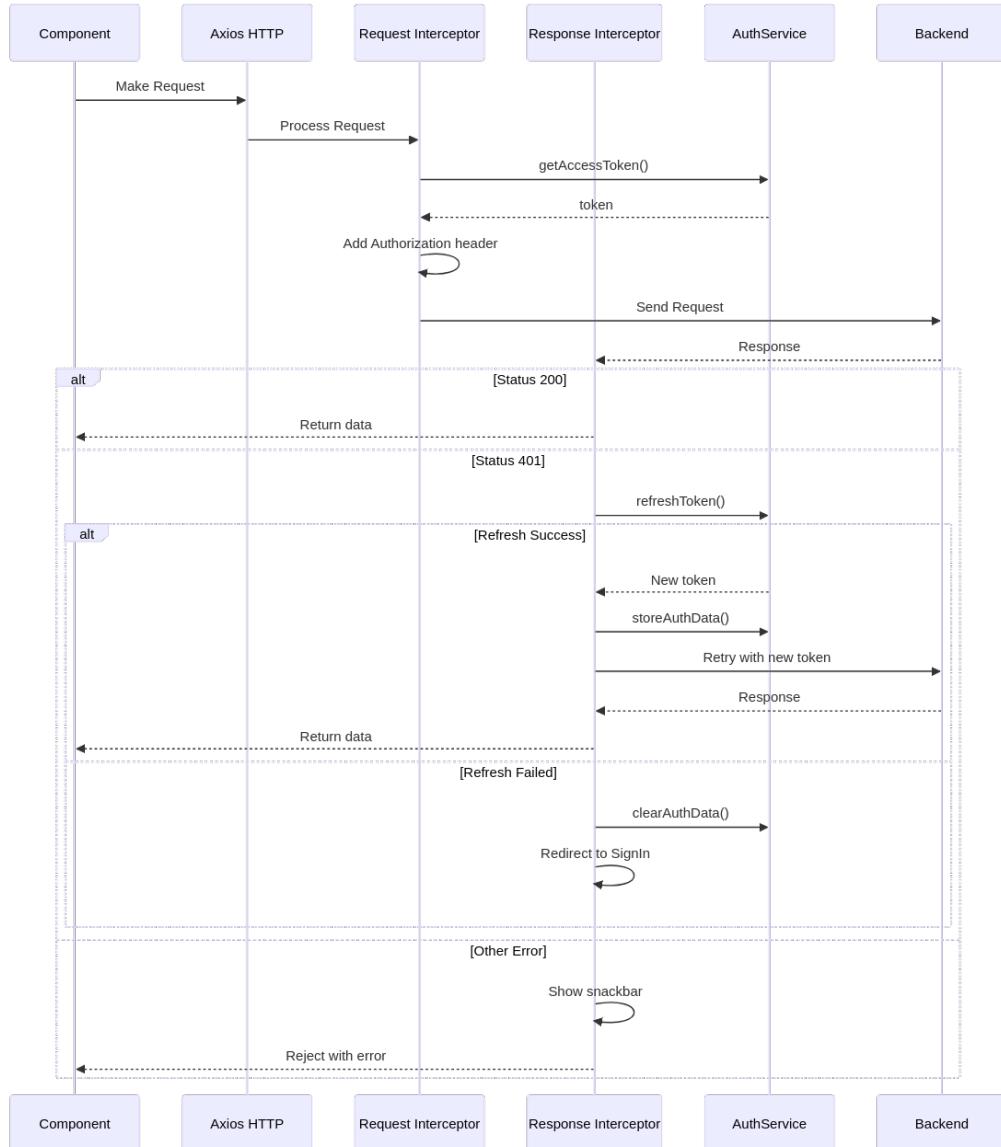


Figure 4.15: HTTP Interceptor Flow with Token Refresh

The interceptors handle:

- **Request:** Automatically attach Authorization header with JWT token.
- **Response 401:** Attempt token refresh; if failed, redirect to login.
- **Other Errors:** Display error message in snackbar.

4.2.4 Subscription Management Interface

The subscription interface provides plan selection, payment processing, and quota monitoring.

Component Architecture

The subscription system consists of interconnected components:

- **Subscription.vue:** Main page with conditional views for users and admins.

- **PlanCard.vue**: Displays plan details with dynamic pricing from Stripe.
- **JsonPlansEditor.vue**: Admin-only JSON editor for plan management.

User Subscription View

For users with active subscriptions, the view displays:

- Subscription period (start/end dates)
- Quota allocation (batch and live processing)
- Usage progress with color-coded indicators
- Cancel/Resume subscription controls

```

1 calculateUsagePercent(used, quota) {
2   if (quota === -1) return 0      // Unlimited
3   if (quota === 0) return 100
4   return Math.min((used / quota) * 100, 100)
5 }
6
7 getUsageColor(used, quota) {
8   if (quota === -1) return 'success'
9   const percent = (used / quota) * 100
10  if (percent >= 90) return 'error'
11  if (percent >= 75) return 'warning'
12  return 'success'
13 }
```

Listing 4.21: Usage Percentage Calculation

PlanCard Component

The PlanCard fetches pricing from Stripe and displays plan features:

Prop	Type	Description
plan	Object	Plan data (id, name, features, priceId)
disabled	Boolean	Disable subscribe button (for admins)

Table 4.4: PlanCard Component Props

```

1 async fetchPriceInfo() {
2   if (!this.plan.priceId) return
3
4   try {
5     this.loadingPrice = true
6     this.priceInfo = await stripeService.getPriceInfo(
7       this.plan.priceId
8     )
9   }
```

```

9  } catch (error) {
10    this.priceError = 'Failed to load price'
11  } finally {
12    this.loadingPrice = false
13  }
14}

15 // Computed property for display
16 get formattedPrice() {
17   if (!this.priceInfo) return 'Loading...'
18   const amount = this.priceInfo.unit_amount / 100
19   return `$$${amount.toFixed(2)}`
20 }
21

```

Listing 4.22: PlanCard Price Fetching

Stripe Checkout Integration

When a user subscribes, the frontend initiates Stripe Checkout:

```

1  async handleSubscribe(priceId) {
2    try {
3      const data = await stripeService.createCheckoutSession(
4        priceId
5      )
6
7      if (data?.url) {
8        window.location.href = data.url
9      } else {
10        this.showError('Failed to redirect. Please try again.')
11      }
12    } catch (err) {
13      console.error('Subscription error', err)
14      this.showError('An error occurred during checkout.')
15    }
16  }

```

Listing 4.23: Checkout Session Creation

Cancel and Resume Subscription

Users can manage their subscription lifecycle:

```

1  async handleCancelSubscription() {
2    if (!confirm('Are you sure you want to cancel?')) {
3      return
4    }
5
6    try {
7      this.cancellingSubscription = true
8      await stripeService.cancelSubscription(
9        this.subscription.stripeSubscriptionId
10       )

```

```

11 |     await this.checkStripeSubscriptionStatus(
12 |       this.subscription.stripeSubscriptionId
13 |     )
14 |
15 |     this.showSuccess('Subscription scheduled for cancellation.')
16 |   } catch (err) {
17 |     this.showError('Failed to cancel subscription.')
18 |   } finally {
19 |     this.cancellingSubscription = false
20 |   }
21 |

```

Listing 4.24: Cancel Subscription

Admin Plans Editor

Administrators access a JSON editor for managing plans:

- Live JSON validation with syntax highlighting
- Stripe price ID validation before publishing
- Diff comparison with current version
- Version history tracking

The editor validates each plan's `priceId` against Stripe before allowing publication, ensuring only valid pricing configurations are saved.

Chapter 5

Conclusion and Future Work

This chapter summarizes the project achievements, draws conclusions from the implementation, and outlines directions for future work.

5.1 Project Summary

This project successfully designed and implemented a comprehensive **Gateway Dashboard** system to address the challenges faced by the Speech Gateway API ecosystem. The project delivered the following key components:

5.1.1 Authentication System

A robust authentication module was implemented supporting three authentication methods:

- **Email/Password Authentication:** Traditional credential-based login with password hashing using bcrypt.
- **Google OAuth 2.0:** Redirect-based OAuth flow for seamless Google account integration.
- **Apple Sign-In:** SDK-based authentication supporting Apple's privacy-focused identity system.

The authentication system includes advanced security features such as JWT token management, automatic token refresh, token blacklisting using Redis, and session security with device fingerprinting.

5.1.2 Payment and Subscription System

A complete payment processing infrastructure was developed using Stripe, consisting of:

- **Plan Module:** Versioned pricing plans with Redis caching and cache penetration protection.
- **Stripe Integration:** Checkout session creation, webhook handling, and subscription lifecycle management.
- **Subscription Module:** Quota tracking for batch and live processing with automatic access control.

5.1.3 Frontend Dashboard

A Vue.js 2 web application was developed with Vuetify providing:

- Intuitive user interface for subscription and service management.
- Admin portal with JSON-based plans editor and validation.
- Secure navigation guards and HTTP interceptors for token management.
- Responsive design supporting multiple device form factors.

5.2 Conclusions

The Gateway Dashboard project has successfully achieved all stated objectives:

1. **Web-based Dashboard:** A fully functional Vue.js application provides an intuitive interface for users and administrators, eliminating the need for direct API interaction.
2. **Secure Authentication:** The multi-provider SSO system enables seamless user onboarding while maintaining security through industry-standard protocols (OAuth 2.0, JWT, HTTPS).
3. **Subscription Infrastructure:** The Stripe integration enables automated billing, subscription management, and tiered access control, establishing the commercial viability of the Speech Gateway services.
4. **Administrative Tools:** The admin portal with RBAC provides efficient management of users, plans, and system monitoring without manual database intervention.
5. **Enhanced Security:** Token blacklisting, automatic refresh, and session management using Redis provide robust protection against unauthorized access.

The modular architecture adopted in this project promotes maintainability and extensibility. The separation between frontend and backend, combined with the service-oriented design in NestJS, allows for independent scaling and future enhancements.

5.3 Future Work

While the current implementation addresses the core requirements, several areas present opportunities for future development:

5.3.1 Technical Enhancements

- **Multi-language Support:** Implement internationalization (i18n) in the frontend to support multiple languages.
- **Real-time Usage Monitoring:** Add WebSocket-based real-time updates for quota usage and system status.
- **Enhanced Analytics:** Implement comprehensive usage analytics dashboard for administrators.

- **Mobile Application:** Develop native mobile applications for iOS and Android to complement the web dashboard.

5.3.2 Business Features

- **Team/Organization Accounts:** Support for enterprise customers with multiple users under a shared subscription.
- **Usage-based Billing:** Implement pay-as-you-go pricing model in addition to subscription plans.
- **Invoice Management:** Generate downloadable PDF invoices for accounting purposes.
- **Promotional Codes:** Support for discount codes and promotional campaigns.

5.3.3 Infrastructure Improvements

- **Containerization:** Docker containerization for easier deployment and scaling.
- **CI/CD Pipeline:** Automated testing and deployment pipelines for continuous integration.
- **Monitoring and Alerting:** Integration with tools like Prometheus and Grafana for production monitoring.

5.4 Final Remarks

The Gateway Dashboard project demonstrates how modern web technologies can be leveraged to create a comprehensive management system for API-based services. The combination of Vue.js, NestJS, MongoDB, and Redis provides a solid foundation for building scalable, maintainable, and secure web applications.

The project not only addresses the immediate needs of the Speech Gateway ecosystem but also establishes patterns and practices that can be applied to similar enterprise applications. The modular design ensures that the system can evolve to meet future requirements while maintaining backward compatibility.

Bibliography

- [1] Apple Inc. *Apple Platform Security*. <https://support.apple.com/guide/security>. 2023.
- [2] Apple Inc. *Sign in with Apple REST API*. https://developer.apple.com/documentation/sign_in_with_apple. 2023.
- [3] Apple Inc. *Sign in with Apple: Technical Overview*. <https://developer.apple.com/sign-in-with-apple>. 2019.
- [4] Kyle Banker. *MongoDB in action*. Manning Publications, 2011.
- [5] Adam Barth, Collin Jackson, and John C Mitchell. “Securing frame communication in browsers”. In: *17th USENIX Security Symposium*. 2008, pp. 17–30.
- [6] Baymard Institute. *E-Commerce Checkout Usability: An Original Research Study*. <https://baymard.com/checkout-usability>. 2020.
- [7] Gavin Bierman, Martín Abadi, and Mads Torgersen. “Understanding TypeScript”. In: *European Conference on Object-Oriented Programming*. 2014, pp. 257–281.
- [8] Josiah L Carlson. *Redis in Action*. Manning Publications, 2013.
- [9] Kristina Chodorow. *MongoDB: the definitive guide*. O'Reilly Media, 2013.
- [10] Chee Yong Chong and Sai Peck Lee. “Component-based software engineering: Technologies, development frameworks, and quality assurance schemes”. In: *Information and Software Technology* 107 (2019), pp. 70–86.
- [11] Roy Thomas Fielding. “Architectural styles and the design of network-based software architectures”. PhD thesis. University of California, Irvine, 2000.
- [12] Martin Fowler. *Patterns of enterprise application architecture*. Addison-Wesley, 2003.
- [13] Zheng Gao, Christian Bird, and Earl T Barr. “Type systems for JavaScript: A survey”. In: *Software Engineering at Google* (2017), pp. 1–27.
- [14] Gartner Inc. *Market Guide for Cloud Workspace Productivity Suites*. 2023.
- [15] Annabelle Gawer and Michael A Cusumano. *Platform leadership: How Intel, Microsoft, and Cisco drive industry innovation*. Harvard Business School Press, 2014.
- [16] GitHub Inc. *GitHub Annual Report 2023*. <https://github.com/about>. 2023.
- [17] Google Inc. *Google Account Security Features*. <https://safety.google/authentication>. 2023.
- [18] Google Inc. *Google Services: Active User Statistics 2023*. <https://about.google>. 2023.
- [19] Google Inc. *Material Design Guidelines*. <https://material.io/design>. 2014.
- [20] Google Inc. *Using OAuth 2.0 to Access Google APIs*. <https://developers.google.com/identity/protocols/oauth2>. 2023.

- [21] Wenjuan Guo et al. “Freemium as an optimal strategy for market dominant firms”. In: *Marketing Science* 38.1 (2019), pp. 150–169.
- [22] Rahul Gupta. *Stripe integration: A comprehensive guide for developers*. 2020.
- [23] Dick Hardt. *The OAuth 2.0 authorization framework*. Tech. rep. RFC 6749, 2012.
- [24] Amir Herzberg and Ahmad Jbara. “Payment system integration: A comparative study of Stripe and PayPal”. In: *Journal of Electronic Commerce Research* 20.3 (2019), pp. 145–162.
- [25] Jim Isaak and Mina J Hanna. “User data privacy: Facebook, Cambridge Analytica, and privacy protection”. In: *Computer* 51.8 (2018), pp. 56–59.
- [26] Michael Jones, John Bradley, and Nat Sakimura. *JSON web token (JWT)*. Tech. rep. RFC 7519, 2015.
- [27] Neal Leavitt. “Will NoSQL databases live up to their promise?” In: *Computer* 43.2 (2010), pp. 12–14.
- [28] Cheng Li et al. “Building reliable distributed systems using message queues”. In: *Proceedings of the 25th Symposium on Operating Systems Principles*. 2015, pp. 239–254.
- [29] Torsten Lodderstedt, Mark McGloin, and Phil Hunt. “OAuth 2.0 threat model and security considerations”. In: *RFC 6819* (2013).
- [30] Callum Macrae. *Vue.js: Up and Running*. O’Reilly Media, 2018.
- [31] Mark Masse. *REST API design rulebook*. O’Reilly Media, 2011.
- [32] Microsoft Corporation. *Microsoft Identity Platform Documentation*. <https://docs.microsoft.com/azure/active-directory>. 2023.
- [33] Michael S Mikowski and Josh C Powell. *Single Page Web Applications: JavaScript end-to-end*. Manning Publications, 2013.
- [34] Sam Newman. *Building microservices: designing fine-grained systems*. O’Reilly Media, 2015.
- [35] Addy Osmani. *A comparison of JavaScript frameworks*. 2017.
- [36] Addy Osmani. *Web performance optimization*. 2017.
- [37] OWASP Foundation. *OWASP Top 10 - 2021: The Ten Most Critical Web Application Security Risks*. Tech. rep. OWASP, 2021.
- [38] Suhas Pai et al. “SoK: Systematization of knowledge on web single sign-on systems”. In: *2011 IEEE Symposium on Security and Privacy*. IEEE. 2011, pp. 232–246.
- [39] Cesare Pautasso, Olaf Zimmermann, and Frank Leymann. “RESTful web services vs. “big” web services: making the right architectural decision”. In: *Proceedings of the 17th international conference on World Wide Web* (2008), pp. 805–814.
- [40] PayPal Holdings Inc. *PayPal Q4 2023 Earnings Report*. <https://investor.paypal-corp.com>. 2023.
- [41] Ken Peffers, Charles E Gengler, and Tuure Tuunanen. “Electronic payment systems: an analysis and comparison of types”. In: *IEEE Transactions on Engineering Management* 50.3 (2003), pp. 296–304.
- [42] Tomas Petricek, Gustavo Guerra, and Don Syme. “Types from data: Making structured data first-class citizens in F#”. In: *ACM SIGPLAN Notices* 51.6 (2016), pp. 477–490.

- [43] Chris Richardson. *Microservices patterns: with examples in Java*. Manning Publications, 2018.
- [44] Carlos Rodriguez et al. “RESTful web services: A study and comparison of tools”. In: *Service Oriented Computing and Applications* 10 (2016), pp. 435–450.
- [45] Nat Sakimura, John Bradley, and Naveen Agarwal. *Proof Key for Code Exchange by OAuth Public Clients*. Tech. rep. RFC 7636, 2015.
- [46] Günther Schuh, Michael Riesener, and Christof Mattern. “Subscription business models: Growth and profitability”. In: *Production Engineering* 7 (2013), pp. 385–392.
- [47] Prabath Siriwardena. *Advanced API security: OAuth 2.0 and beyond*. Apress, 2020.
- [48] S Mahbub Sohan. “A pattern language for webhooks”. In: *PLoP’17: 24th Conference on Pattern Languages of Programs* (2017).
- [49] StatCounter Global Stats. *Mobile Operating System Market Share Worldwide*. <https://gs.statcounter.com>. 2023.
- [50] Statista Research Department. *Most popular online accounts worldwide 2023*. <https://www.statista.com>. 2023.
- [51] Stripe Inc. *Stripe API Documentation*. <https://stripe.com/docs/api>. 2023.
- [52] Stripe Inc. *Stripe Billing Documentation*. <https://stripe.com/docs/billing>. 2023.
- [53] Stripe Inc. *Stripe Security and Compliance*. <https://stripe.com/docs/security>. 2023.
- [54] Yi Sun et al. “Understanding user adoption of single sign-on systems”. In: *Computers & Security* 83 (2019), pp. 143–154.
- [55] Yuhui Sun, Yan Zhang, and Wei Peng. “Security and privacy for web databases and services”. In: *Web Database Systems: Technologies and Applications* (2010), pp. 15–37.

Appendix A

Proof

A long proof that you expect no one will read