Real-Time Vehicle Tracking System
Authentication Module

1. Introduction

Authentication is a critical component of the Real-Time Vehicle Tracking System. It ensures that only authorized users and devices can access system resources and data.

2. Types of Authentication

• User Authentication (Admin, Manager, Driver)
• Device Authentication (GPS devices)
• API Authentication using JWT tokens

3. Authentication Flow

1. User submits login credentials.
2. Backend validates credentials from database.
3. Server generates JWT token.
4. Token is sent to client.
5. Client includes token in API requests.

4. Login API

Method	Endpoint	Description
POST	/auth/login	Authenticate user and generate token

Sample Login Request

```
{
  "username": "admin",
  "password": "admin123"
}
```

Sample Login Response

```
{
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
  "expiresIn": "24h"
}
```

5. Token Validation

JWT token is validated on every API request. If the token is expired or invalid, the server rejects the request with an unauthorized error.

6. Role-Based Access Control (RBAC)

• Admin: Full system access
• Manager: Vehicle and report access
• Driver: View assigned vehicle only

7. Security Measures

• Password hashing (bcrypt)
• HTTPS communication
• Token expiration and refresh
• Account lock after failed attempts

8. Authentication Error Codes

Code	Description
401	Unauthorized – Invalid credentials
403	Forbidden – Access denied
408	Session expired

9. Conclusion

The authentication module ensures secure access to the Real-Time Vehicle Tracking System by verifying users, devices, and API requests using modern security standards.