JWT Payload Structure – CRM Project

The JWT payload determines the claims that hold the authenticated user's identity and authorization scope in the CRM platform. The payload is sent in every request to authenticate APIs and is utilized for role-based access control (RBAC), team-level data filtering, and session expiration management.

Payload Fields

| Field Name | Type | Description | Example |
| --- | --- | --- | --- |
| user\_id | Integer | Unique identifier of the authenticated user from the Users table in the database. Used to fetch user-specific data without additional lookups. | 101 |
| role | String | The user’s role in the system. Determines module access and permissions according to the RBAC matrix (e.g., Admin, Manager, Sales, Marketing, Support, Viewer). | "Manager" |
| team\_id | Integer | ID of the team to which the user belongs. Used for filtering records (Leads, Deals, Campaigns) relevant to the team. | 5 |
| email | String | User’s registered email address for quick UI reference and verification purposes. | "manager@company.com" |
| exp | Integer (Unix Timestamp) | Expiration time of the token in seconds since Unix epoch. The token becomes invalid after this timestamp, requiring re-authentication. | 1723564800 |

Security Considerations

* Sensitive credentials (e.g., passwords, refresh tokens) are never stored in the payload.
* Tokens are server-side signed with a secure secret (HS256 algorithm suggested).
* exp provides automatic invalidation after a specified session duration (e.g., 1 hour).
* Role and team-based filtering is done server-side after the token is decoded.
* The payload should be kept minimal to minimize size and exposure.

Usage in System

1. Login API creates the JWT upon successful validation of credentials.
2. Frontend stores the JWT securely (e.g., httpOnly cookie or secure storage).
3. All API Requests pass the JWT in the Authorization header.
4. Backend Middleware extracts the token, adds the payload to the request context (req.user), allowing access to user\_id, role, and team\_id for authorization checks.
5. Access Control is enforced for role and team\_id.