**Significant Security Risks/Assumptions**

APIs have different security risks like

* Excessive data exposure (DDoS attacks)
* Broken authentication and authorization
* Security misconfiguration
* Insufficient logging and monitoring

**How to prevent attacks**

* APIs are a prime target for DDoS attacks. To avoid DDoS attacks, as well as API spikes and other issues that affect performance and security, place rate limits on how and how often your API can be called.
* Proper authentication and authorization by providing token-based authorization.
* Data encryption For example by using methods such as Transport Layer Security (TLS), that data can be decrypt and modify data by legitimate user after authorization by signature.
* By using API gateway.

Fast API has built-in data validation, makes it an ideal candidate for the backend side of our web application. Fast API validates the developer’s data type even in deeply nested JSON requests. Fast API is built on standards like JSON Schema, OAuth 2.0, and OpenAPI. OpenAPI has a way to define multiple security "schemes".