JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. JWT is typically used to authenticate a user and securely exchange information between a client and a server, or multiple applications. It is composed of three parts: header, payload, and signature.

The HEADER contains information about the type of token and the cryptographic algorithm used to sign the token. The PAYLOAD contains the claims, which are the information related to the user or the application that is being shared. The SIGNATURE is a cryptographic verification of the data in the header and payload.

The main benefits of using JWT are authentication, authorization, and scalability.

Authentication is the process of confirming the identity of a user. JWT is used to authenticate a user in an API-based system. When a user attempts to log in with their credentials, the server will generate a token and send it back to the user. The user then sends this token with each request, and the server can validate the token to authenticate the user.

Authorization is the process of determining whether a user has access to a certain resource. With JWT, authorization can be done on the server side. When a user makes a request, the server will use the information in the token to determine if the user has the necessary permissions to access the resource.

Scalability is an important factor when designing an API based system. JWT is a lightweight, stateless protocol that makes it easy to scale the system, as no session state needs to be stored on the server. This also reduces the amount of data that needs to be sent with each request, improving performance.

In conclusion, JWT is an open standard that provides secure authentication and authorization, as well as scalability. It is a lightweight, stateless protocol that makes it easy to scale the system. JWT is used by many companies, including Google, Microsoft, and Facebook, to secure their web applications.

Proof of benefits of JWT are:

1**. Security:** JWT tokens are digitally signed, which means that the server can verify that the token has not been tampered with. The signature also ensures that only the intended party can access the data contained within the token.

2. **Ease of Use:** JWT tokens are self-contained, meaning that all the necessary information is contained within the token itself. This means that the server does not have to look up user information in a database, which can reduce the amount of time and resources needed to process a request.

3. **Scalability:** JWT tokens are stateless, meaning that they do not need to be stored on the server. This makes them easier to scale, as the server does not have to keep track of which tokens are valid and which ones have been revoked.