-Structure:

+)Gồm 3 phần:Header,Payload,Signature.

+)Header: Thường bao gồm 2 phần là type of token và thuật toán đang được sử dụng là HMAC SHA256 hoặc RSA.

+)Payload:

+)Chứa các Claims -> là thông tin về entity,xác định các quyền truy cập của nó và cung câp thông tin bổ sung như là thời gian hết hạn,…

+)Có 3 loại claims chính là:

+)Registed claims: Là claims được tiêu chuẩn hóa , và nó có bộ khung mặc định như là iss(issuer->Người đăng ký),sub(subject),aud(audience),exp(expiration time),nbf(not before time), iat(issued at -> Thời gian hết hạn) và jti(JWT ID).

+)Public claims: Là các claims được cộng đồng sử dụng rộng rãi gồm các claims như role,permission.

+)private claims: Là các claims được chúng ta tự định nghĩa sử dụng cho mục đích riêng.

+)Signature:

+)Là phần chứa giữ liệu được mã hóa từ phần header và phần payload của token và được mã hóa bằng 1 secret\_key.

+)Khi mà giải mã để thấy được sự toàn vẹn của token thì nó sẽ trải qua 4 bước sau:

+) Đầu tiên là sẽ giải mã token với secret\_key để lấy 3 phần của token.

+) Tiếp theo là sẽ mã hóa phần signature của token để lấy là dữ liệu header+payload đã được mã hóa khi tạo token trước đó.

+) Tiếp theo là sẽ kết hợp header+payload của token để mã hóa chúng lại với nhau.

+) So sánh phần signature của token đã được mã hóa với phần header+payload đã được mã hóa xem có trùng khớp với nhau hay không.