JWT（JSON Web Token）的原理基于加密和签名机制，其工作流程如下：

**认证过程**：当用户通过认证机制登录后，服务器会生成一个JWT并将其作为身份验证令牌发送给客户端。

**令牌生成**：JWT由三部分组成：头部（Header）、载荷（Payload）和签名（Signature）。服务器将头部和载荷信息以及密钥结合起来，并使用指定的加密算法生成签名。最终，将头部、载荷和签名拼接起来形成一个JWT。

**令牌传输**：客户端收到JWT后，通常会将其存储在本地（如LocalStorage或Cookie）以备后续使用。客户端在每次向服务器发起请求时，都会将JWT作为请求的一部分发送给服务器。

令牌验证：服务器接收到JWT后，首先会验证JWT的签名是否有效。服务器通过解密JWT的签名得到原始的头部和载荷信息，再根据头部中指定的算法和密钥对头部和载荷进行签名，然后将生成的签名与JWT中的签名进行对比。如果两者一致，则说明JWT的完整性未被篡改。

**载荷解析**：如果JWT的签名有效，服务器会解析载荷信息，获取其中的用户身份和权限等信息，以便进行后续的业务逻辑处理。

**权限控制**：服务器根据解析出的用户信息进行权限控制，验证用户是否具有访问资源的权限。如果验证通过，则服务器会响应请求并提供相应的服务；如果验证失败，则服务器会返回相应的错误信息或拒绝访问请求。

通过这样的流程，JWT实现了基于令牌的身份验证和授权，提供了一种简单、安全、可扩展的认证机制，适用于各种网络应用场景。