**现有H5安全方案**

H5客户端随机生成一个密钥key。

再使用非对称加密算法RSA对密钥key进行加密。

将业务数据以随机key使用AES对称加密算法进行加密。

将获取的token和其他逻辑数据和加密过的业务数据以及加密过的key进行MD5加签。

再将加签的签值放进逻辑数据中并发送到服务器。

可能的不足之处：数据被抓包篡改，但能被篡改的只有外层逻辑数据，如果AES加密的数据被解密盗窃，那也无能为力。所以最可能被篡改的是token，但是外层数据都参与了加签，被篡改的话，后台能通过验签来验证数据是否改变，如果篡改人将签值也篡改，那么外层数据就会被其任意修改，但只要篡改人不能破解RSA拿不到随机密钥，就不可能对业务有破坏，所以其实这个方案的安全性已经很高了。