(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106534176 B
(45)授权公告日 2019.06.14

(21)申请号 201611121134.4

(22)申请日 2016.12.08

(65)同一申请的已公布的文献号
申请公布号 CN 106534176 A

(43)申请公布日 2017.03.22

(73)专利权人 西安交大捷普网络科技有限公司
地址 710075 陕西省西安市高新区科技二路72号

(72)发明人 陈晓兵 陈宏伟 焦小涛 何建锋 同元峰

(74)专利代理机构 西安新思维专利商标事务所有限公司 61114
代理人 黄秦芳

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 103391197 A,2013.11.13,
CN 104852961 A,2015.08.19,
CN 105099672 A,2015.11.25,
CN 106130958 A,2016.11.16,

审查员 肖敬伟

权利要求书1页 说明书3页

(54)发明名称

一种云环境下数据安全存储方法

(57)摘要

本发明公开了一种云环境下数据加密方法，发送端根据加密算法对预先生成的动态令牌进行加密，加密的结果作为密钥，根据所述密钥对数据进行AES对称加密形成加密数据部分，对所述动态令牌进行异或、置换、代换和移位与加密数据部分进行拼接，根据拼接后的数据计算校验码和加密数据部分拼接后进行传输；具有与接收端相同动态令牌和密钥的接收端对数据接收后进行拆包获得待验证的校验码和加密数据部分，对加密数据部分计算获得校验码，将该校验码与待验证的校验码进行对比，如果相同则为正确的数据，对所述加密数据部分进行存储或其他加工处理，反之，则为不正确，视为数据被篡改丢弃该数据。本发明能够防泄漏、防篡改，性能消耗小。

CN 106534176 B

1.一种云环境下数据加密方法,其特征在于,该方法为发送端根据加密算法对预先生成的动态令牌进行加密,加密的结果作为数据传输前加密的密钥,根据所述密钥对数据进行AES对称加密形成加密数据部分,对所述动态令牌进行异或、置换、代换和移位与加密数据部分进行拼接,根据拼接后的数据计算校验码和对拼接后的加密数据部分进行传输;

具有与发送端相同动态令牌和密钥的接收端对数据接收后进行拆包获得待验证的校验码和加密数据部分,对加密数据部分计算获得校验码,将该校验码与待验证的校验码进行对比,如果相同则为正确的数据,对所述加密数据部分进行存储或其他加工处理,反之,则为不正确,视为数据被篡改丢弃该数据。

2.根据权利要求1所述的云环境下数据加密方法,其特征在于,该方法还包括:对正确的数据进行数据分离,根据分离出来的动态令牌进行移位、代换、置换和异或反解出令牌信息,再使用解密后的令牌信息对数据段里面的数据使用AES进行解密,解密后的数据与令牌信息分别进行存储。

3.根据权利要求1或2所述的云环境下数据加密方法,其特征在于,该方法还包括:对数据进行检索浏览时,检索到的数据使用令牌信息进行加密,令牌信息进行AES加密后结果作为密钥,根据密钥再对数据部分进行加密,加密后数据做一下移位、代换、置换和异或整理后的数据作为发送数据发送到设备端;所述设备端对数据进行异或、置换、代换和移位反解,根据自己的设备令牌信息对解密数据进行解密,如果解密失败说明数据传输中被篡改直接丢弃,解密成功后对数据进行展现。

4.根据权利要求3所述的云环境下数据加密方法,其特征在于,所述对加密数据部分计算获得校验码,具体为:对数据做校验和时抽取数据长度开始位置8字节,1/3位置、1/5位置、1/7位置、1/9位置偏移8个字节,结束位置向前偏移8个字节,对取到的6处48字节数据进行或运算得到的和作为校验码;其中若偏移不够8字节的用0填充。

5.根据权利要求4所述的云环境下数据加密方法,其特征在于,该方法中加密过程为:当前加密模块首先从操作系统底层接口获取硬件令牌信息,对获取的令牌信息使用常规的AES算法进行加密,加密形成的令牌数据作为后续数据加密的密钥,使用此密钥对业务数据使用进行加密,加密的结果数据与密钥数据进行组合即数据内容进行偏移移位、移位后的数据前128字节和后128字节进行基于可见字符特征的数据字典替换、置换、异或;将加密数据与校验和按次序组装起来,进行传输。

6.根据权利要求5所述的云环境下数据加密方法,其特征在于,该方法中解密过程为:对接收数据进行校验和、密钥分离,分离出的数据计算出校验码与传输数据中的校验码进行比较,不一致认为已篡改或泄漏直接丢弃,校验码正确后对数据做解密,根据分离出来的密钥数据对数据部分进行反异或、反置换和替换最后进行移位得出原始数据进行后续处理。

一种云环境下数据安全存储方法

技术领域

[0001] 本发明属于云环境下数据安全技术领域，具体涉及一种云环境下数据加密方法。

背景技术

[0002] 云环境下数据集中后的安全问题显现。一是传统的网络中各种应用服务的标准流量和突发流量有迹可循，流量模型设计相对较为规范、简单，对安全设备的处理能力没有太高的要求。而在云计算环境下，同类型存储或者应用服务器的规模增长迅猛，动辄以万为单位进行扩展，并且不能分而治之，必须依托统一架构的基础网络来承载。与传统网络环境相比，这就对安全设备本身的性能指标提出了更高的要求。二是用户的数据存储、处理、网络传输等都与云计算系统有关。如何避免多用户共存带来的潜在风险；如何保证云服务的身份鉴别、认证管理和访问控制等数据或控制命令下发的安全需求成为云计算环境所面临的安全挑战之一。云环境下安全设备进行数据上报、策略下发、配置/日志存储越来越多，在网络环境中很容易出现数据篡改、泄漏等数据存储安全问题，此方法可以解决上述数据泄漏问题。

发明内容

[0003] 有鉴于此，本发明的主要目的在于提供一种云环境下数据加密方法。

[0004] 为达到上述目的，本发明的技术方案是这样实现的：

[0005] 本发明实施例提供一种云环境下数据加密方法，该方法为发送端根据加密算法对预先生成的动态令牌进行加密，加密的结果作为数据传输前加密的密钥，根据所述密钥对数据进行AES对称加密形成加密数据部分，对所述动态令牌进行异或、置换、代换和移位与加密数据部分进行拼接，根据拼接后的数据计算校验码和加密数据部分拼接后进行传输；

[0006] 具有与接收端相同动态令牌和密钥的接收端对数据接收后进行拆包获得待验证的校验码和加密数据部分，对加密数据部分计算获得校验码，将该校验码与待验证的校验码进行对比，如果相同则为正确的数据，对所述加密数据部分进行存储或其他加工处理，反之，则为不正确，视为数据被篡改丢弃该数据。

[0007] 上述方案中，该方法还包括：对正确的数据进行数据分离，根据分离出来的动态令牌进行移位、代换、置换和异或反解出令牌信息，再对动态令牌信息进行AES加密使用解密后的令牌信息对数据段里面的数据使用AES进行解密，解密后的数据与令牌信息分别进行存储。

[0008] 上述方案中，该方法还包括：对数据进行检索浏览时，检索到的数据使用令牌信息进行加密，令牌信息进行AES加密加密后结果作为密钥，根据密钥再对数据部分进行加密，加密后数据做一下移位、代换、置换和异或整理后的数据作为发送数据发送到设备端；所述设备端对数据进行异或、置换、代换和移位反解，根据自己的设备令牌信息对解密数据进行解密，如果解密失败说明数据传输中被篡改直接丢弃，解密成功后对数据进行展现。

[0009] 上述方案中，所述对加密数据部分计算获得校验码，具体为：对数据做校验和时抽

取数据长度开始位置8字节，1/3位置、1/5位置、1/7位置、1/9位置偏移8个字节，结束位置向前偏移8个字节，对取到的6处48字节数据进行或运算得到的和作为校验码；其中若偏移不够8字节的用0填充。

[0010] 上述方案中，该方法中加密过程为：当前加密模块首先从操作系统底层接口获取硬件令牌信息，对获取的令牌信息使用常规的AES算法进行加密，加密形成的令牌数据作为后续数据加密的密钥，使用此密钥对业务数据使用进行加密，加密的结果数据与密钥数据进行组合即数据内容进行偏移移位、移位后的数据前128字节和后128字节进行基于可见字符特征的数据字典替换、置换、异或；将加密数据与校验和按次序组装起来，进行传输。

[0011] 上述方案中，该方法中解密过程为：对接收数据进行校验和、密钥分离，分离出的数据计算出校验与传输数据中的校验和进行比较，不一致认为已篡改或泄漏直接丢弃，校验和正确后对数据做解密，根据分离出来的密钥数据对数据部分进行反异或、反置换和替换最后进行移位得出原始数据进行后续处理。

[0012] 与现有技术相比，本发明的有益效果：

[0013] 本发明能够增强和避免数据传输、存储时的数据安全，防泄漏、防篡改，性能消耗小。

具体实施方式

[0014] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0015] 本发明实施例提供一种云环境下数据加密方法，该方法为发送端根据加密算法对预先生成的动态令牌进行加密，加密的结果作为数据传输前加密的密钥，根据所述密钥对数据进行AES对称加密形成加密数据部分，对所述动态令牌进行异或、置换、代换、移位与加密数据部分进行拼接，根据拼接后的数据计算校验码和加密数据部分拼接后进行传输；

[0016] 具有与接收端相同动态令牌和密钥的接收端对数据接收后进行拆包获得待验证的校验码和加密数据部分，对加密数据部分计算获得校验码，将该校验码与待验证的校验码进行对比，如果相同则为正确的数据，对所述加密数据部分进行存储或其他加工处理，反之，则为不正确，视为数据被篡改丢弃该数据。

[0017] 该方法还包括：对正确的数据进行数据分离，根据分离出来的动态令牌进行移位、代换、置换、异或反解出令牌信息，再对动态令牌信息进行AES加密使用解密后的令牌信息对数据段里面的数据使用AES进行解密，解密后的数据与令牌信息分别进行存储。

[0018] 该方法还包括：对数据进行检索浏览时，检索到的数据使用令牌信息进行加密，令牌信息进行AES加密加密后结果作为密钥，根据密钥再对数据部分进行加密，加密后数据做一下移位、代换、置换、异或整理后的数据作为发送数据发送到设备端；所述设备端对数据进行异或、置换、代换、移位反解，根据自己的设备令牌信息对解密数据进行解密，如果解密失败说明数据传输中被篡改直接丢弃，解密成功后对数据进行展现。

[0019] 加密过程为：从操作系统底层接口获取硬件令牌信息(此信息每设备唯一)，对获取的令牌信息使用常规的AES算法进行加密，加密形成的令牌数据作为后续数据加密的密钥。使用此密钥对程序中的业务数据使用进行加密，加密的结果数据与密钥数据进行组合

(数据内容进行偏移移位、移位后的数据前128字节和后128字节进行基于可见字符特征的数据字典(相当一个密码本)替换、置换、异或)。对加密好的数据计算出校验,为提升算法效率对数据做校验和时抽取数据长度开始位置8字节,1/3位置、1/5位置、1/7位置、1/9位置偏移8个字节,结束位置向前偏移8个字节6段数据,对取到的6端共48字节数据进行或运算得到的和作为校验码。(偏移不够8字节的用0填充)。将加密数据与校验和按次序组装起来,进行传输。

[0020] 解密过程为:首先对接收数据进行校验和、密钥分离,分离出的数据计算出校验和(计算过程与加密时处理一致)与传输数据中的校验和进行比较,不一致认为已篡改或泄漏直接丢弃,校验和正确后对数据做解密,解密过程是加密过程的逆过程,需要用分离出来的密钥数据对数据部分进行反异或、反置换和替换最后进行移位得出原始数据进行后续处理。

[0021] 所述对加密数据部分计算获得校验码,具体为对数据做校验和时抽取数据长度开始位置8字节,1/3位置、1/5位置、1/7位置、1/9位置偏移8个字节,结束位置向前偏移8个字节,对取到的6处48字节数据进行或运算得到的和作为校验码。(偏移不够8字节的用0填充)。

[0022] 本发明能够有效防止数据传输时篡改和存储数据的泄露。

[0023] 本发明的主要思路是在设备到存储之前将设备上的硬件令牌信息与密钥结合进行一定的加密,对端或数据存储端收到数据后进行相应的解密;从设备上请求时存储端要将数据按令牌信息密钥进行加密,设备收到数据后用自己的硬件令牌信息进行解密。

[0024] 以上所述,仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。