(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107612898 A
(43)申请公布日 2018.01.19

(21)申请号 201710803428.3

(22)申请日 2017.09.08

(71)申请人 四川省绵阳太古软件有限公司
地址 621000 四川省绵阳市科创园区创业服务中心

(72)发明人 张卫延 李辉

(74)专利代理机构 北京酷爱智慧知识产权代理有限公司 11514
代理人 安娜

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

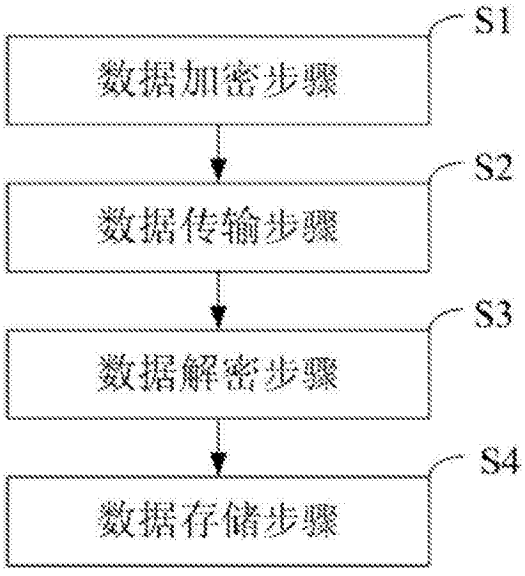
权利要求书2页 说明书8页 附图1页

(54)发明名称

物联网大数据安全传输与存储方法、系统

(57)摘要

本发明属于物联网技术领域，提供了一种物联网大数据安全传输与存储方法、系统。该方法包括采用对称算法的密钥对目标数据进行加密，生成加密数据，采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥，传输加密数据和加密密钥，采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥，根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据，检测存储器的触发模式，将解密后的原数据存储至存储器。本发明物联网大数据安全传输与存储方法、系统，能够保障数据安全传输与存储，防止数据篡改，保障数据有效存储。



CN 107612898 A

1.一种物联网大数据安全传输与存储方法，其特征在于，包括：

对待传输的数据进行加密，形成加密数据，进行传输；

对所述加密数据进行解密，获取原数据；

切换存储器的工作状态，将所述原数据存储于指定的存储器。

2.一种物联网大数据安全传输与存储方法，其特征在于，包括：

数据加密步骤：获取待传输的目标数据；

采用对称算法的密钥对所述目标数据进行加密，生成加密数据；

采用非对称算法的公钥对所述对称算法的密钥进行加密，生成加密密钥；

数据传输步骤：采用预建立的传输通道，传输所述加密数据和所述加密密钥；

数据解密步骤：采用非对称算法的私钥对所述加密密钥进行解密，获取对称算法的密钥；

根据解密获取的对称算法的密钥，对所述加密数据进行解密，获取原数据；

数据存储步骤：检测存储器的触发模式：

若为定时触发模式，则切换所述存储器至工作状态，并根据预设的时间间隔，将所述原数据存储至所述存储器；

若为侦听触发模式，则实时侦听所述通道的状态：

若所述通道存在待接收的数据，则切换所述存储器至工作状态，并将解密后的原数据存储至所述存储器。

3.根据权利要求2所述物联网大数据安全传输与存储方法，其特征在于，采用对称算法的密钥对所述目标数据进行加密，生成加密数据，具体包括：按照预设的时间间隔，更新所述对称算法的密钥；

采用更新后的对称算法的密钥对所述目标数据进行加密，生成加密数据；

采用非对称算法的公钥对所述对称算法的密钥进行加密，生成加密密钥，具体包括：

采用非对称算法的公钥对更新后的对称算法的密钥进行加密，生成加密密钥；

采用非对称算法的私钥对所述加密密钥进行解密，获取对称算法的密钥，具体包括：

采用非对称算法的私钥对所述加密密钥进行解密，获取更新后的对称算法的密钥；

根据解密获取的对称算法的密钥，对所述加密数据进行解密，获取原数据，具体包括：

根据解密获取的更新后的对称算法的密钥，对所述加密数据进行解密，获取原数据。

4.根据权利要求2所述物联网大数据安全传输与存储方法，其特征在于，获取待传输的目标数据之后，采用对称算法的密钥对所述目标数据进行加密之前，该方法还包括：

按照每条数据的属性，将所述目标数据进行分类；

采用对称算法的密钥对所述目标数据进行加密，生成加密数据，具体包括：采用对称算法的密钥分别对每种类型的目标数据进行加密，形成多个加密数据块，每个加密数据块对应一种类型的目标数据；

将所述加密数据块合成所述加密数据；

根据解密获取的对称算法的密钥，对所述加密数据进行解密，获取原数据，具体包括：

将所述加密数据进行分解，生成多个加密数据块；

根据解密获取的对称算法的密钥，分别对每个加密数据块进行解密，获取不同类型的原数据。

5.根据权利要求2所述物联网大数据安全传输与存储方法，其特征在于，采用预建立的传输通道，传输所述加密数据和所述加密密钥，具体包括：

判断所述传输通道的缓存中是否存在写空间：

若是，则将所述加密数据和所述加密密钥写入所述传输通道的缓存中。

6.一种物联网大数据安全传输与存储系统，其特征在于，包括：

数据加密模块：用于获取待传输的目标数据；采用对称算法的密钥对所述目标数据进行加密，生成加密数据；采用非对称算法的公钥对所述对称算法的密钥进行加密，生成加密密钥；

数据传输模块：用于采用预建立的传输通道，传输所述加密数据和所述加密密钥；

数据解密模块：用于采用非对称算法的私钥对所述加密密钥进行解密，获取对称算法的密钥；根据解密获取的对称算法的密钥，对所述加密数据进行解密，获取原数据；

数据存储模块：用于检测存储器的触发模式：若为定时触发模式，则切换所述存储器至工作状态，并根据预设的时间间隔，将所述原数据存储至所述存储器；若为侦听触发模式，则实时侦听所述通道的状态：若所述通道存在待接收的数据，则切换所述存储器至工作状态，并将解密后的原数据存储至所述存储器。

7.根据权利要求6所述物联网大数据安全传输与存储系统，其特征在于，所述数据加密模块，在采用对称算法的密钥对所述目标数据进行加密，生成加密数据时，具体用于：按照预设的时间间隔，更新所述对称算法的密钥；采用更新后的对称算法的密钥对所述目标数据进行加密，生成加密数据；

所述数据加密模块，在采用非对称算法的公钥对所述对称算法的密钥进行加密，生成加密密钥时，具体用于：采用非对称算法的公钥对更新后的对称算法的密钥进行加密，生成加密密钥；

所述数据解密模块，在采用非对称算法的私钥对所述加密密钥进行解密，获取对称算法的密钥时，具体用于：采用非对称算法的私钥对所述加密密钥进行解密，获取更新后的对称算法的密钥；

所述数据解密模块，在根据解密获取的对称算法的密钥，对所述加密数据进行解密，获取原数据时，具体用于：根据解密获取的更新后的对称算法的密钥，对所述加密数据进行解密，获取原数据。

8.根据权利要求6所述物联网大数据安全传输与存储系统，其特征在于，所述数据加密模块还用于：按照每条数据的属性，将所述目标数据进行分类；

所述数据加密模块，在采用对称算法的密钥对所述目标数据进行加密，生成加密数据时，具体用于：采用对称算法的密钥分别对每种类型的目标数据进行加密，形成多个加密数据块，每个加密数据块对应一种类型的目标数据；将所述加密数据块合成所述加密数据；

所述数据加密模块，在根据解密获取的对称算法的密钥，对所述加密数据进行解密，获取原数据时，具体用于：将所述加密数据进行分解，生成多个加密数据块；根据解密获取的对称算法的密钥，分别对每个加密数据块进行解密，获取不同类型的原数据。

9.根据权利要求6所述物联网大数据安全传输与存储系统，其特征在于，所述数据传输模块，具体用于：判断所述传输通道的缓存中是否存在写空间：若是，则将所述加密数据和所述加密密钥写入所述传输通道的缓存中。

物联网大数据安全传输与存储方法、系统

技术领域

[0001] 本发明涉及物联网技术领域，具体涉及一种物联网大数据安全传输与存储方法、系统。

背景技术

[0002] 目前，环境监测采集设备类型多样，环境监测设备提供商直接向客户销售环境监测设备，并可能配套一份该设备单独使用的软件，用于显示监测结果。

[0003] 但是，现有各个生态旅游目的地的环境监测数据在传输时，并没有采用加密措施，存在环境数据篡改、窃取的风险，并且，对于庞大海量的环境数据，并没有有效的存储机制，保障环境数据能够实时有效存储，尤其是物联网的存储控制系统，多是靠人工进行启闭，自动化程度低。

[0004] 如何保障数据安全传输与存储，防止数据篡改，保障数据有效存储，是本领域技术人员亟需解决的问题。

发明内容

[0005] 针对现有技术中的缺陷，本发明提供了一种物联网大数据安全传输与存储方法、系统，能够保障数据安全传输与存储，防止数据篡改，保障数据有效存储。

[0006] 第一方面，本发明提供一种物联网大数据安全传输与存储方法，该方法包括：对待传输的数据进行加密，形成加密数据，进行传输；

[0007] 对加密数据进行解密，获取原数据；

[0008] 切换存储器的工作状态，将原数据存储于指定的存储器。

[0009] 本发明提供另一种物联网大数据安全传输与存储方法，该方法包括：

[0010] 数据加密步骤：获取待传输的目标数据；

[0011] 采用对称算法的密钥对目标数据进行加密，生成加密数据；

[0012] 采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥；

[0013] 数据传输步骤：采用预建立的传输通道，传输加密数据和加密密钥；

[0014] 数据解密步骤：采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥；

[0015] 根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据；

[0016] 数据存储步骤：检测存储器的触发模式：

[0017] 若为定时触发模式，则切换存储器至工作状态，并根据预设的时间间隔，将原数据存储至存储器；

[0018] 若为侦听触发模式，则实时侦听通道的状态：

[0019] 若通道存在待接收的数据，则切换存储器至工作状态，并将解密后的原数据存储至存储器。

[0020] 进一步地，采用对称算法的密钥对目标数据进行加密，生成加密数据，具体包括：

按照预设的时间间隔，更新对称算法的密钥；

[0021] 采用更新后的对称算法的密钥对目标数据进行加密，生成加密数据；

[0022] 采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥，具体包括：

[0023] 采用非对称算法的公钥对更新后的对称算法的密钥进行加密，生成加密密钥；

[0024] 采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥，具体包括：

[0025] 采用非对称算法的私钥对加密密钥进行解密，获取更新后的对称算法的密钥；

[0026] 根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据，具体包括：

[0027] 根据解密获取的更新后的对称算法的密钥，对加密数据进行解密，获取原数据。

[0028] 基于上述任意物联网大数据安全传输与存储方法实施例，进一步地，获取待传输的目标数据之后，采用对称算法的密钥对目标数据进行加密之前，该方法还包括：

[0029] 按照每条数据的属性，将目标数据进行分类；

[0030] 采用对称算法的密钥对目标数据进行加密，生成加密数据，具体包括：采用对称算法的密钥分别对每种类型的目标数据进行加密，形成多个加密数据块，每个加密数据块对应一种类型的目标数据；

[0031] 将加密数据块合成加密数据；

[0032] 根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据，具体包括：

[0033] 将加密数据进行分解，生成多个加密数据块；

[0034] 根据解密获取的对称算法的密钥，分别对每个加密数据块进行解密，获取不同类型的原数据。

[0035] 基于上述任意物联网大数据安全传输与存储方法实施例，进一步地，采用预建立的传输通道，传输加密数据和加密密钥，具体包括：

[0036] 判断传输通道的缓存中是否存在写空间：

[0037] 若是，则将加密数据和加密密钥写入传输通道的缓存中。

[0038] 第二方面，本发明提供一种物联网大数据安全传输与存储系统，该系统包括数据加密模块、数据传输模块、数据解密模块和数据存储模块，数据加密模块用于获取待传输的目标数据；采用对称算法的密钥对目标数据进行加密，生成加密数据；采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥；数据传输模块用于采用预建立的传输通道，传输加密数据和加密密钥；数据解密模块用于采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥；根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据；数据存储模块用于检测存储器的触发模式：若为定时触发模式，则切换存储器至工作状态，并根据预设的时间间隔，将原数据存储至存储器；若为侦听触发模式，则实时侦听通道的状态：若通道存在待接收的数据，则切换存储器至工作状态，并将解密后的原数据存储至存储器。

[0039] 进一步地，数据加密模块在采用对称算法的密钥对目标数据进行加密，生成加密数据时，具体用于：按照预设的时间间隔，更新对称算法的密钥；采用更新后的对称算法的密钥对目标数据进行加密，生成加密数据；

[0040] 数据加密模块在采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥时，具体用于：采用非对称算法的公钥对更新后的对称算法的密钥进行加密，生成加密密钥；

[0041] 数据解密模块在采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥时，具体用于：采用非对称算法的私钥对加密密钥进行解密，获取更新后的对称算法的密钥；

[0042] 数据解密模块在根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据时，具体用于：根据解密获取的更新后的对称算法的密钥，对加密数据进行解密，获取原数据。

[0043] 基于上述任意物联网大数据安全传输与存储系统实施例，进一步地，数据加密模块还用于：按照每条数据的属性，将目标数据进行分类；

[0044] 数据加密模块在采用对称算法的密钥对目标数据进行加密，生成加密数据时，具体用于：采用对称算法的密钥分别对每种类型的目标数据进行加密，形成多个加密数据块，每个加密数据块对应一种类型的目标数据；将加密数据块合成加密数据；

[0045] 数据加密模块在根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据时，具体用于：将加密数据进行分解，生成多个加密数据块；根据解密获取的对称算法的密钥，分别对每个加密数据块进行解密，获取不同类型的原数据。

[0046] 基于上述任意物联网大数据安全传输与存储系统实施例，进一步地，数据传输模块，具体用于：判断传输通道的缓存中是否存在写空间：若是，则将加密数据和加密密钥写入传输通道的缓存中。

[0047] 由上述技术方案可知，本实施例提供的物联网大数据安全传输与存储方法、系统，能够采用对称算法和非对称算法进行加密，既能够实现物联网数据传输的安全性，又能够保证加密与解密运算的时效性，实现良好的加密效果。同时，该方法还能够针对存储器不同的触发方式，保障数据有效存储，避免人工切换存储器工作状态。

[0048] 因此，本实施例物联网大数据安全传输与存储方法、系统，能够保障数据安全传输与存储，防止数据篡改，保障数据有效存储。

附图说明

[0049] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍。在所有附图中，类似的元件或部分一般由类似的附图标记标识。附图中，各元件或部分并不一定按照实际的比例绘制。

[0050] 图1示出了本发明所提供的一种物联网大数据安全传输与存储方法的方法流程图；

[0051] 图2示出了本发明所提供的一种物联网大数据安全传输与存储系统的结构示意图。

具体实施方式

[0052] 下面将结合附图对本发明技术方案的实施例进行详细的描述。以下实施例仅用于更加清楚地说明本发明的技术方案，因此只是作为示例，而不能以此来限制本发明的保护范围。

[0053] 需要注意的是，除非另有说明，本申请使用的技术术语或者科学术语应当为本发明所属领域技术人员所理解的通常意义。

[0054] 第一方面，本发明实施例所提供的一种物联网大数据安全传输与存储方法，该方法包括：对待传输的数据进行加密，形成加密数据，进行传输。

[0055] 对加密数据进行解密，获取原数据。

[0056] 切换存储器的工作状态，将原数据存储于指定的存储器。

[0057] 本发明实施例所提供的另一种物联网大数据安全传输与存储方法，结合图2，该方法包括：

[0058] 数据加密步骤S1：获取待传输的目标数据。

[0059] 采用对称算法的密钥对目标数据进行加密，生成加密数据。

[0060] 采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥。

[0061] 数据传输步骤S2：采用预建立的传输通道，传输加密数据和加密密钥。

[0062] 数据解密步骤S3：采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥。

[0063] 根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据。

[0064] 数据存储步骤S4：检测存储器的触发模式：

[0065] 若为定时触发模式，则切换存储器至工作状态，并根据预设的时间间隔，将原数据存储至存储器。

[0066] 若为侦听触发模式，则实时侦听通道的状态：

[0067] 若通道存在待接收的数据，则切换存储器至工作状态，并将解密后的原数据存储至存储器。

[0068] 由上述技术方案可知，本实施例提供的物联网大数据安全传输与存储方法，能够采用对称算法和非对称算法进行加密，既能够实现物联网数据传输的安全性，又能够保证加密与解密运算的时效性，实现良好的加密效果。同时，该方法还能够针对存储器不同的触发方式，保障数据有效存储，避免人工切换存储器工作状态。

[0069] 因此，本实施例物联网大数据安全传输与存储方法，能够保障数据安全传输与存储，防止数据篡改，保障数据有效存储。

[0070] 为了进一步提高本实施例物联网大数据安全传输与存储方法的安全性，具体地，在密钥设置方面，采用对称算法的密钥对目标数据进行加密，生成加密数据时，该方法的具体实现过程如下：

[0071] 按照预设的时间间隔，更新对称算法的密钥。

[0072] 采用更新后的对称算法的密钥对目标数据进行加密，生成加密数据。

[0073] 采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥时，具体实现过程如下：

[0074] 采用非对称算法的公钥对更新后的对称算法的密钥进行加密，生成加密密钥。

[0075] 采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥时，具体实现过程如下：

[0076] 采用非对称算法的私钥对加密密钥进行解密，获取更新后的对称算法的密钥。

[0077] 根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据时，具体实现过程如下：

[0078] 根据解密获取的更新后的对称算法的密钥，对加密数据进行解密，获取原数据。

[0079] 在此，本实施例物联网大数据安全传输与存储方法能够定时更新对称算法的密钥，防止对称算法的密钥被破译，导致目标数据泄露，提高数据传输的安全性。

[0080] 为了进一步提高本实施例物联网大数据安全传输与存储方法的运算效率，具体地，在数据加密设置方面，该方法的具体实现过程如下：

[0081] 在获取待传输的目标数据之后，采用对称算法的密钥对目标数据进行加密之前，该方法还能够按照每条数据的属性，将目标数据进行分类；

[0082] 采用对称算法的密钥对目标数据进行加密，生成加密数据时，具体实现过程为：采用对称算法的密钥分别对每种类型的目标数据进行加密，形成多个加密数据块，每个加密数据块对应一种类型的目标数据。

[0083] 将加密数据块合成加密数据。

[0084] 根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据时，具体实现过程为：

[0085] 将加密数据进行分解，生成多个加密数据块。

[0086] 根据解密获取的对称算法的密钥，分别对每个加密数据块进行解密，获取不同类型的原数据。

[0087] 在此，本实施例物联网大数据安全传输与存储方法能够对目标数据进行分类，便于对不同类型的目标数据进行加密或解密运算，加快数据运算效率。

[0088] 为了进一步提高本实施例物联网大数据安全传输与存储方法在数据传输时的有效性，具体地，采用预建立的传输通道，传输加密数据和加密密钥时，具体实现过程为：判断传输通道的缓存中是否存在写空间：若是，则将加密数据和加密密钥写入传输通道的缓存中。

[0089] 在此，该方法在判断传输通道中存在写空间时，才将加密后的加密数据和加密密钥写入传输通道，防止数据拥堵，导致数据包流失，即加密数据与加密密钥丢失。

[0090] 在实际应用过程中，对于非对称算法的公钥、私钥的生成与传输，本实施例物联网大数据安全传输与存储方法的具体实现过程如下：

[0091] 采用对称算法的密钥对目标数据进行加密，生成加密数据之后，该方法还包括：

[0092] 将称算法的密钥进行分组。

[0093] 对于每组数据分别使用初始密钥进行初始加密，将初始加密后数据作为初始输入以进行多轮加密。

[0094] 在每轮加密中，将输入的数据进行加密置换，使用与本次加密轮数对应的密钥对加密置换后数据进行加密，将加密后数据作为下一轮加密的输入数据。

[0095] 将待解密的数据进行分组。

[0096] 对于每组数据分别使用与最后一轮加密对应的密钥进行初始解密，将初始解密后数据作为初始输入以进行多轮解密。

[0097] 在每轮解密中，将输入的数据进行解密置换，使用与本次解密轮数对应的密钥对解密置换后数据进行解密，将解密后数据作为下一轮解密输入数据，最终获取称算法的密钥。

[0098] 在此，该方法将待加密的称算法的密钥进行分组，对于每组数据分别使用初始密钥进行初始加密，将初始加密后数据作为初始输入以进行多轮加密；在每轮加密中，将输入

的数据进行加密置换，使用与本次加密轮数对应的密钥对加密置换后数据进行加密，将加密后数据作为下一轮加密的输入数据，以便于获取对称算法的密钥，减少运算量，提高安全性能，又能够及时对加密数据进行解密。

[0099] 第二方面，本发明实施例所提供的一种物联网大数据安全传输与存储系统，结合图2，该系统包括数据加密模块1、数据传输模块2、数据解密模块3和数据存储模块4，数据加密模块1用于获取待传输的目标数据；采用对称算法的密钥对目标数据进行加密，生成加密数据；采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥；数据传输模块2用于采用预建立的传输通道，传输加密数据和加密密钥；数据解密模块3用于采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥；根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据；数据存储模块4用于检测存储器的触发模式：若为定时触发模式，则切换存储器至工作状态，并根据预设的时间间隔，将原数据存储至存储器；若为侦听触发模式，则实时侦听通道的状态：若通道存在待接收的数据，则切换存储器至工作状态，并将解密后的原数据存储至存储器。

[0100] 由上述技术方案可知，本实施例提供的物联网大数据安全传输与存储系统，能够采用对称算法和非对称算法进行加密，既能够实现物联网数据传输的安全性，又能够保证加密与解密运算的时效性，实现良好的加密效果。同时，该系统还能够针对存储器不同的触发方式，保障数据有效存储，避免人工切换存储器工作状态。

[0101] 因此，本实施例物联网大数据安全传输与存储系统，能够保障数据安全传输与存储，防止数据篡改，保障数据有效存储。

[0102] 为了进一步提高本实施例物联网大数据安全传输与存储系统的安全性，具体地，在密钥设置方面，该系统能够定时更细密钥，即数据加密模块1在采用对称算法的密钥对目标数据进行加密，生成加密数据时，具体用于：按照预设的时间间隔，更新对称算法的密钥；采用更新后的对称算法的密钥对目标数据进行加密，生成加密数据。数据加密模块1在采用非对称算法的公钥对对称算法的密钥进行加密，生成加密密钥时，具体用于：采用非对称算法的公钥对更新后的对称算法的密钥进行加密，生成加密密钥。数据解密模块3在采用非对称算法的私钥对加密密钥进行解密，获取对称算法的密钥时，具体用于：采用非对称算法的私钥对加密密钥进行解密，获取更新后的对称算法的密钥。数据解密模块3在根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据时，具体用于：根据解密获取的更新后的对称算法的密钥，对加密数据进行解密，获取原数据。

[0103] 在此，本实施例物联网大数据安全传输与存储系统能够定时更新对称算法的密钥，防止对称算法的密钥被破译，导致目标数据泄露，提高数据传输的安全性。

[0104] 为了进一步提高本实施例物联网大数据安全传输与存储系统的运算效率，具体地，在数据加密设置方面，数据加密模块1还用于：按照每条数据的属性，将目标数据进行分类。数据加密模块1在采用对称算法的密钥对目标数据进行加密，生成加密数据时，具体用于：采用对称算法的密钥分别对每种类型的目标数据进行加密，形成多个加密数据块，每个加密数据块对应一种类型的目标数据；将加密数据块合成加密数据。数据加密模块1在根据解密获取的对称算法的密钥，对加密数据进行解密，获取原数据时，具体用于：将加密数据进行分解，生成多个加密数据块；根据解密获取的对称算法的密钥，分别对每个加密数据块进行解密，获取不同类型的原数据。

[0105] 在此，本实施例物联网大数据安全传输与存储系统能够对目标数据进行分类，便于对不同类型的目标数据进行加密或解密运算，加快数据运算效率。

[0106] 为了进一步提高本实施例物联网大数据安全传输与存储系统在数据传输时的有效性，具体地，数据传输模块2具体用于：判断传输通道的缓存中是否存在写空间：若是，则将加密数据和加密密钥写入传输通道的缓存中。

[0107] 在此，该系统在判断传输通道中存在写空间时，才将加密后的加密数据和加密密钥写入传输通道，防止数据拥堵，导致数据包流失，即加密数据与加密密钥丢失。

[0108] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0109] 需要说明的是，附图中的流程图和框图显示了根据本发明的多个实施例的服务器、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的服务器来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0110] 本发明实施例所提供的配置装置可以是计算机程序产品，包括存储了程序代码的计算机可读存储介质，所述程序代码包括的指令可用于执行前面方法实施例中所述的方法，具体实现可参见方法实施例，在此不再赘述。

[0111] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的服务器、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0112] 在本申请所提供的几个实施例中，应该理解到，所揭露的服务器、装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个服务器，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0113] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以发布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0114] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以

是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0115] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-OnlyMemory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0116] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围，其均应涵盖在本发明的权利要求和说明书的范围当中。

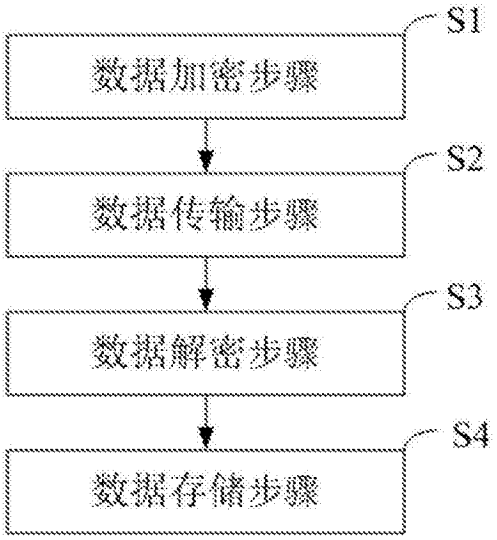

S1
数据加密步骤
S2
数据传输步骤
S3
数据解密步骤
S4
数据存储步骤

图1

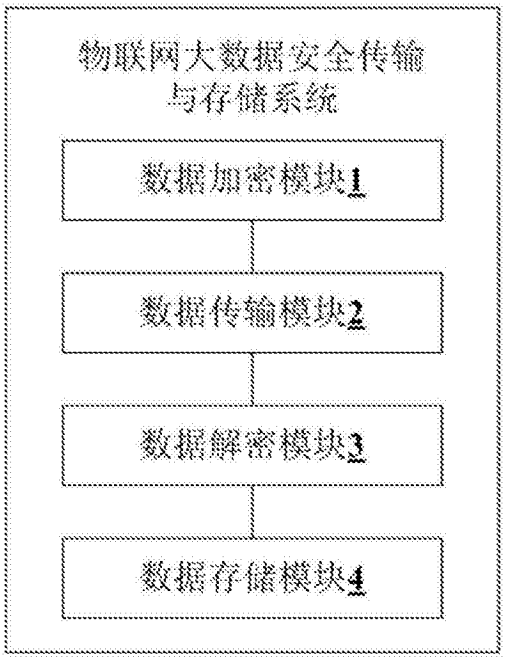

物联网大数据安全传输
与存储系统
数据加密模块1
数据传输模块2
数据解密模块3
数据存储模块4

图2