(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 102831529 A
(43)申请公布日 2012.12.19

(21)申请号 201210290889.2

(22)申请日 2012.08.15

(71)申请人 天长市浩云电子科技有限公司
地址 239300 安徽省滁州市天长市经济开发区经三路高新技术创业服务中心

(72)发明人 梁浩

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 杨小双

(51)Int.Cl.
G06Q 30/00(2012.01)
G06K 17/00(2006.01)
H04L 29/08(2006.01)

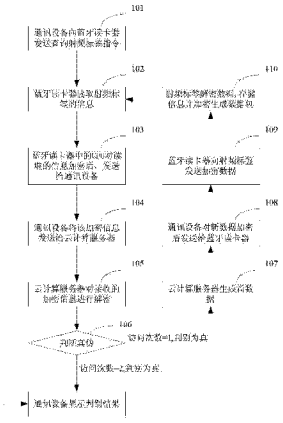
权利要求书 2 页 说明书 4 页 附图 3 页

(54)发明名称

一种基于射频的商品信息识别方法及系统

(57)摘要

本发明公开了一种基于射频的商品信息识别方法及系统，该方法包括以下步骤：所述通讯设备向所述蓝牙读卡器发送查询所述射频标签的指令，所述指令中包括需要查询的商品类别；所述蓝牙读卡器根据所述商品类别读取所述射频标签的防伪信息，所述防伪信息包括商品信息动态代码、访问次数信息码、UID号、中央处理单元CPU运算代码和随机代码；所述蓝牙读卡器将所述防伪信息加密后，通过所述通讯设备发送给所述云计算服务器；所述云计算服务器对所述加密的防伪信息进行解密，将解密后的防伪信息与本地存储的防伪信息进行比较，判断所述射频标签的真伪，并通知所述通讯设备。本发明由于防伪信息是动态生成的，不易仿造，因此，提高了防伪检验的安全性。



CN 102831529 A

1. 一种基于射频的商品信息识别方法，应用于包括射频标签、蓝牙读卡器、通讯设备和云计算服务器的系统中，其特征在于，所述方法包括以下步骤：

所述通讯设备向所述蓝牙读卡器发送查询所述射频标签的指令，所述指令中包括需要查询的商品类别；

所述蓝牙读卡器根据所述商品类别读取所述射频标签的防伪信息，所述防伪信息包括商品信息动态代码、访问次数信息码、UID 号、中央处理单元 CPU 运算代码和随机代码；

所述蓝牙读卡器将所述防伪信息加密后，通过所述通讯设备发送给所述云计算服务器；

所述云计算服务器对所述加密的防伪信息进行解密，将解密后的防伪信息与本地存储的防伪信息进行比较，判断所述射频标签的真伪，并通知所述通讯设备。

2. 如权利要求 1 所述的基于射频的商品信息识别方法，其特征在于，还包括：

所述云计算服务器判断所述射频标签为真后，动态生成新的防伪信息，并通过所述通讯设备和蓝牙读卡器发送给所述射频标签；

所述射频标签将所述新的防伪信息进行存储。

3. 如权利要求 1 所述的基于射频的商品信息识别方法，其特征在于，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签的真伪，具体包括：

判断 CPU 运算代码结构数据是否被篡改，如果没有被篡改，则射频标签为真；或

判断访问次数信息码中的访问次数与云计算服务器记录的访问次数是否相符，如果相符，则射频标签为真。

4. 如权利要求 1 所述的基于射频的商品信息识别方法，其特征在于，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签为真后，还包括：

当首次验证射频标签为真后，如果后续验证出现序号小于云计算服务器存储的序号，则判定该射频标签为假。

5. 如权利要求 1 所述的基于射频的商品信息识别方法，其特征在于，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签为真后，还包括：

连续成功查询预定次数后，暂停预定时间访问。

6. 如权利要求 1 所述的基于射频的商品信息识别方法，其特征在于，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签为假后，还包括：

记录所有错误访问的 IP。

7. 一种基于射频的商品信息识别系统，其特征在于，包括：云计算服务器、通讯设备、蓝牙读卡器和射频标签；

所述通讯设备，用于向所述蓝牙读卡器发送某一类商品查询请求，并将所述蓝牙读卡器获取的加密的防伪信息发送给所述云计算服务器；

所述蓝牙读卡器，用于调用其存储的该类商品射频标签的识别码，根据该识别码与所述射频标签通信，获取射频标签中的防伪信息并加密，所述防伪信息包括商品信息动态代码、访问次数信息码、UID 号、中央处理单元 CPU 运算代码和随机代码；

所述云计算服务器，用于对上述加密的防伪信息进行解密后，将解密后的防伪信息与本地存储的防伪信息进行比较，判断该射频标签的真伪，将最终判断结果通知通讯设备。

8. 如权利要求 7 所述的基于射频的商品信息识别系统，其特征在于，所述蓝牙读卡器

包括：

蓝牙部分，用于接收通讯设备发送的信息并传输到射频读卡器部分，并将射频读卡器部分的信息通过蓝牙天线发送通讯设备；

射频读卡器部分，存储防伪商品单位允许的标签识别码、读写密码，根据通讯设备发送的商品类别，调用的相应读写密码和标签识别码进行正常的读写操作。

9. 如权利要求 7 所述的基于射频的商品信息识别系统，其特征在于，

所述云计算服务器，还用于确定射频标签为真时，动态生成新的防伪信息并加密后，返回给所述射频标签；

所述射频标签，还用于解密获得所述新的防伪信息，并存储。

一种基于射频的商品信息识别方法及系统

技术领域

[0001] 本发明涉及防伪技术领域，具体涉及一种基于射频的商品信息识别方法及系统。

背景技术

[0002] 防伪标签学名防伪标识，又名防伪商标，是能粘贴、印刷、转移在标的物表面，或标的物包装上，或标的物附属物，如商品挂牌、名片以及防伪证卡上，具有防伪作用的标识。

[0003] 防伪标签是品牌性用户保护自己品牌的方案和有效手段，目前具有多种防伪技术，例如二维码、条形码和激光防伪码等，但这些防伪技术容易被仿冒，安全性依然不高，有待解决。

发明内容

[0004] 针对上述缺陷，本发明目的在于提出了一种基于射频的商品信息识别方法及系统，以提高现有防伪技术的安全性。

[0005] 为实现上述目的，本发明通过以下技术方案实现：

[0006] 一种基于射频的商品信息识别方法，应用于包括射频标签、蓝牙读卡器、通讯设备和云计算服务器的系统中，所述方法包括以下步骤：

[0007] 所述通讯设备向所述蓝牙读卡器发送查询所述射频标签的指令，所述指令中包括需要查询的商品类别；

[0008] 所述蓝牙读卡器根据所述商品类别读取所述射频标签的防伪信息，所述防伪信息包括商品信息动态代码、访问次数信息码、UID 号、中央处理单元 CPU 运算代码和随机代码；

[0009] 所述蓝牙读卡器将所述防伪信息加密后，通过所述通讯设备发送给所述云计算服务器；

[0010] 所述云计算服务器对所述加密的防伪信息进行解密，将解密后的防伪信息与本地存储的防伪信息进行比较，判断所述射频标签的真伪，并通知所述通讯设备。

[0011] 优选地，还包括：

[0012] 所述云计算服务器判断所述射频标签为真后，动态生成新的防伪信息，并通过所述通讯设备和蓝牙读卡器发送给所述射频标签；

[0013] 所述射频标签将所述新的防伪信息进行存储。

[0014] 优选地，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签的真伪，具体包括：

[0015] 判断 CPU 运算代码结构数据是否被篡改，如果没有被篡改，则射频标签为真；或

[0016] 判断访问次数信息码中的访问次数与云计算服务器记录的访问次数是否相符，如果相符，则射频标签为真。

[0017] 优选地，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签为真后，还包括：

[0018] 当首次验证射频标签为真后，如果后续验证出现序号小于云计算服务器存储的序

号，则判定该射频标签为假。

[0019] 优选地，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签为真后，还包括：

[0020] 连续成功查询预定次数后，暂停预定时间访问。

[0021] 优选地，所述将解密后的防伪信息与本地的防伪信息进行比较，判断所述射频标签为假后，还包括：

[0022] 记录所有错误访问的 IP。

[0023] 本发明提供了一种基于射频的商品信息识别系统，包括：云计算服务器、通讯设备、蓝牙读卡器和射频标签；

[0024] 所述通讯设备，用于向所述蓝牙读卡器发送某一类商品查询请求，并将所述蓝牙读卡器获取的加密的防伪信息发送给所述云计算服务器；

[0025] 所述蓝牙读卡器，用于调用其存储的该类商品射频标签的识别码，根据该识别码与所述射频标签通信，获取射频标签中的防伪信息并加密，所述防伪信息包括商品信息动态代码、访问次数信息码、UID 号、中央处理单元 CPU 运算代码和随机代码；

[0026] 所述云计算服务器，用于对上述加密的防伪信息进行解密后，将解密后的防伪信息与本地存储的防伪信息进行比较，判断该射频标签的真伪，将最终判断结果通知通讯设备。

[0027] 优选地，所述蓝牙读卡器包括：

[0028] 蓝牙部分，用于接收通讯设备发送的信息并传输到射频读卡器部分，并将射频读卡器部分的信息通过蓝牙天线发送通讯设备；

[0029] 射频读卡器部分，存储防伪商品单位允许的标签识别码、读写密码，根据通讯设备发送的商品类别，调用的相应读写密码和标签识别码进行正常的读写操作。

[0030] 优选地，所述云计算服务器，还用于确定射频标签为真时，动态生成新的防伪信息并加密后，返回给所述射频标签；

[0031] 所述射频标签，还用于解密获得所述新的防伪信息，并存储。

[0032] 与现有技术相比，本发明具有以下有益效果：

[0033] 在本发明使用射频标签替代传统标签，通讯设备通过蓝牙读卡器与射频标签通信，获取射频标签中加密的防伪信息，并将该加密的防伪信息发送至云计算服务器进行真伪识别，云计算服务器将识别结果通知通讯设备；并且云计算服务器在每次识别后，重新生成动态防伪信息，发送给射频标签进行存储。由于防伪信息是动态生成的，不易仿造，因此，提高了防伪检验的安全性。

附图说明

[0034] 下面根据实施例和附图对本发明作进一步详细说明。

[0035] 图 1 为本发明实施例 1 的一种基于射频的商品信息识别系统结构图；

[0036] 图 2 为本发明实施例 1 的射频标签结构示意图；

[0037] 图 3 为本发明实施例 1 的蓝牙读卡器结构示意图；

[0038] 图 4 为本发明实施例 2 的一种基于射频的商品信息识别方法流程图。

[0039] 附图说明：

[0040] 其中，10、云计算服务器；20、通讯设备；30、蓝牙读卡器；40、射频标签。

具体实施方式

[0041] 本发明实施例 1 的一种基于射频的商品信息识别系统，如图 1 所示，包括云计算服务器 10、通讯设备 20、蓝牙读卡器 30 和射频标签 40。通讯设备 20 向蓝牙读卡器 30 发送某一类商品查询请求，蓝牙读卡器 30 调用其存储的该类商品射频标签的识别码，根据该识别码与射频标签 40 通信，获取射频标签 40 中加密的防伪信息，并通过通讯设备 20 发送到云计算服务器 10，由云计算服务器 10 对上述加密的防伪信息进行解密后，判断射频标签的真伪，将最终判断结果通知通讯设备 20。

[0042] 其中，通讯设备 20 是可以进行无线通信的移动设备，例如手机或 PDA（Personal Digital Assistant，个人数字助理）等。

[0043] 射频标签 40 为射频智能卡无源标签（例如工作于 13.56M 赫兹频率），如图 2 所示，包括：天线、射频模块、CPU（Central Processing Unit，中央处理单元）、ROM（Read-Only Memory，只读存储器）、RAM（Random Access Memory，随机存储器）、EEPROM（Electrically Erasable Programmable Read-Only Memory，电可擦可编程只读存储器）等。CPU 与 ROM、RAM、EEPROM 和射频模块连接，进行通信控制；射频模块通过天线与通讯设备 20 通信。其中，EEPROM 中存储的防伪信息包括：UID（User Identification，用户身份证明）号，为只读；商品信息动态代码，是经过云计算服务器 10 加密后生成的，每次读取后由云计算服务器 10 提供新号，重新存入；访问次数信息码，为每次访问云计算服务器后递增的顺序号，如 1、2、3、…．、n，并将顺序号经加密，生成访问次数信息码；CPU 运算代码，为 CPU 运算程序中部分关键代码，由云计算服务器每次动态提供；随机代码，由云计算服务器每次动态提供。每次读取操作时，CPU 根据 ROM 中程序的命令，将以上相关数据进行运算加密，通过蓝牙读卡器 30 和通讯设备 20 发送给云计算服务器 10。射频标签 40 通常安装于商品的开启处，商品启用时，射频标签 40 将销毁。

[0044] 蓝牙读卡器 30 如图 3 所示，包括：射频读卡器部分 31 和蓝牙部分 32，可以看成通用型 RFID（Radio Frequency Identification，射频标识）读卡器和蓝牙适配器的结合体。其中，射频读卡器部分 31 中的 ROM 存储防伪商品单位允许的 RFID 标签的识别码、读写密码，射频读卡器部分 31 根据通讯设备 20 发送的商品类别，调用该标签的相应读写密码和 RFID 标签识别码进行正常的读写操作。蓝牙部分 32，用于接收通讯设备 20 发送的信息并传输到射频读卡器部分 31，并能将射频读卡器部分 31 的信息通过蓝牙天线发送通讯设备 20。

[0045] 本发明实施例 2 的一种基于射频的商品信息识别方法，如图 4 所示，包括以下步骤：

[0046] 步骤 101，通讯设备向蓝牙读卡器发送查询射频标签指令，该指令中包括需要查询的商品类别。具体为：蓝牙读卡器中的蓝牙模块接收来自通讯设备的指令，发送到射频读卡器，射频读卡器中的 ROM 存储防伪商品单位允许的 RFID 标签识别码、读写密码；射频读卡器根据通讯设备 20 发送的商品类别，调用相应的读写密码和 RFID 标签识别码，与射频标签进行正常的读写操作。

[0047] 步骤 102，蓝牙读卡器读取射频标签中 ROM 的程序信息、EEPROM 中防伪信息，读取

的防伪信息包括：蓝牙标签的 UID、商品信息动态代码、访问次数信息码、CPU 运算代码和随机代码。其中，访问次数信息码为该射频标签出厂后，每访问一次，云计算服务器中的访问次数记录递增，经特别加密运算后得到访问次数信息，和自然地 1、2、3、…、n 是一一对应，但经过加密运算；CPU 运算代码是 CPU 运算程序中部分关键代码，包括指定读取射频标签 UID 中某些字符的代码，每次读取后由云计算服务器重新生成。

[0048] 步骤 103，蓝牙读卡器中的 CPU 对读取的防伪信息进行加密后，发送给通讯设备。

[0049] 步骤 104，通讯设备将该加密的防伪信息发送给云计算服务器。

[0050] 步骤 105，云计算服务器对接收的加密的防伪信息进行解密，获得商品信息动态代码、访问次数信息码、CPU 运算代码和随机代码。同时自动记录每次访问的 IP 地址，根据判别的假产品，根据 IP 地址，可追查造假根源。

[0051] 步骤 106，云计算服务器通过上述解密获得的防伪信息与存储的该射频标签对应的防伪信息进行比较，判断该射频标签的真伪，如果为假，则通知通讯设备，在通讯设备上显示检测结果为假；如果访问次数为 2，则在通讯设备上显示检测结果为真；如果访问次数为 1，则转 107。

[0052] 判断真伪具体包括：通过通讯设备传送的 CPU 运算代码（ROM 中存放的 COS）结构数据，判断是否被篡改，如果被篡改则为假；另外，还可以根据访问次数信息码判断射频标签的真伪，由于每次读取射频标签的防伪信息传到云计算服务器后，访问次数应该加一，如果射频标签的访问次数和云计算服务器记录的访问次数不符，则判别射频标签为假。另外，某个批号数据连续访问 n 次都错误后，暂停该射频标签的访问，并向通讯设备回复：“请与厂家联系”。另外，当首次验证判定射频标签为真后，如果后续验证出现序号小于云计算服务器存储的序号，则判定该射频标签为假。

[0053] 步骤 107，云计算服务器根据接收的分类信息，经不同的加密算法，生成新的以下数据：重新加密生成的商品信息动态码；访问次数信息码（此信息为每次访问服务器后递增的顺序号，如 1、2、3、….、n…，并将顺序号经加密，生成新访问次数信息码；CPU 运算代码（CPU 运算程序中部分关键代码，包括指定读取射频标签 UID 中某些字符的代码，每次读取后由云计算服务器重新生成；随机代码（由云计算服务器每次动态提供，每次读取后由云计算服务器重新生成。云计算服务器存储防伪信息并加密生成数据包，发送给通讯设备；

[0054] 步骤 108，通讯设备将加密数据包发送给蓝牙读卡器；

[0055] 步骤 109，蓝牙读卡器将加密数据包发送给射频标签；

[0056] 步骤 110，射频标签解密防伪信息，存储该防伪信息后，加密生成数据包（包括新防伪信息），存储到 EEPROM 中。

[0057] 上述一个查询过程完成后，可以继续进行多次查询，但如果连续成功查询 n 次后，暂停一段时间访问；如果连续 n 次查询失败后，提示为假，停止该标签的数据核对，记录所有错误访问的 IP，以后再访问，不显示结果，记录 IP。

[0058] 上面结合附图对本发明进行了示例性的描述，显然本发明的实现并不受上述方式的限制，只要采用了本发明的方法构思和技术方案进行的各种改进，或未经改进将本发明的构思和技术方案直接应用于其它场合的，均在本发明的保护范围内。

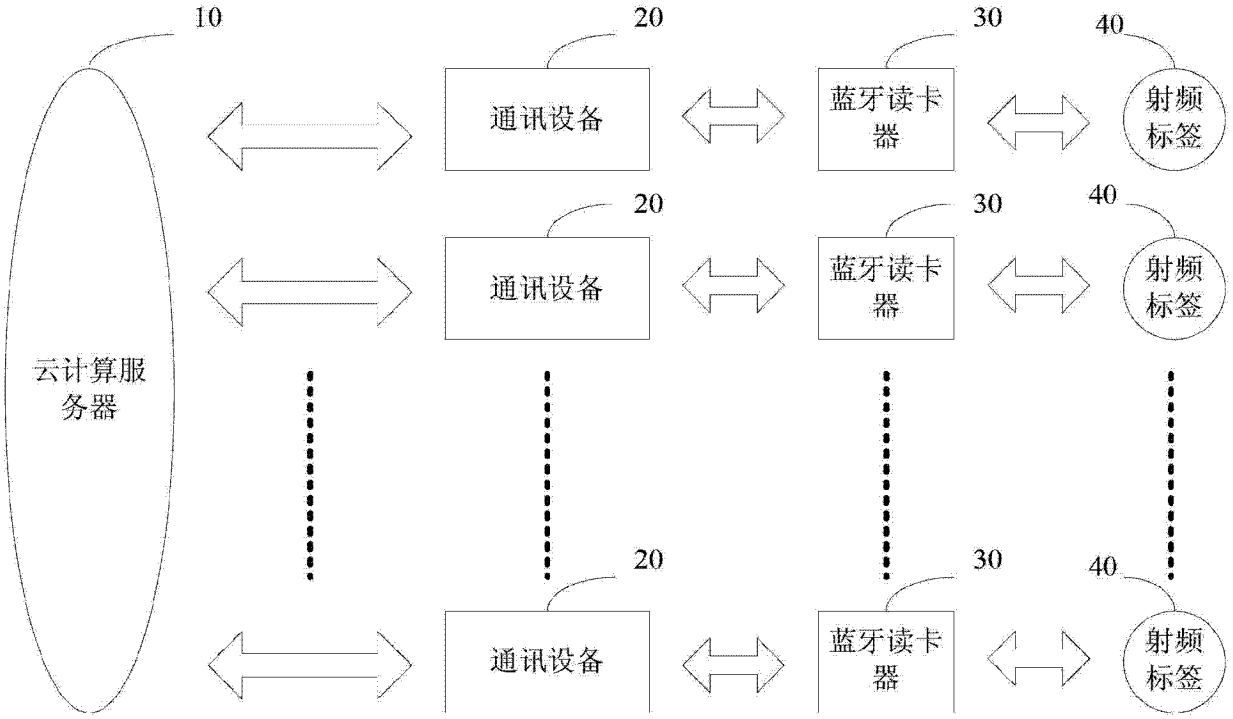

10
20
30
40
云计算服务器
通讯设备
蓝牙读卡器
射频标签
通讯设备
蓝牙读卡器
射频标签
通讯设备
蓝牙读卡器
射频标签

图 1

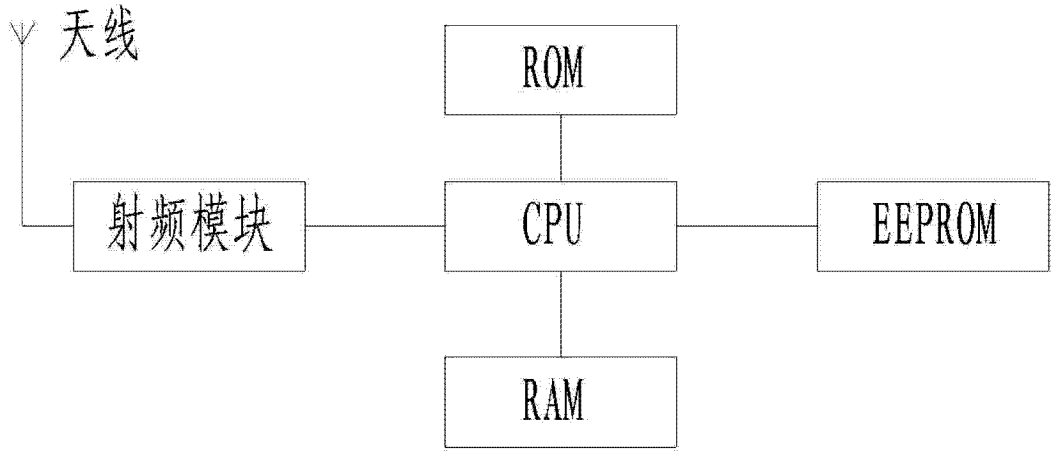

天线
ROM
射频模块
CPU
EEPROM
RAM

图 2

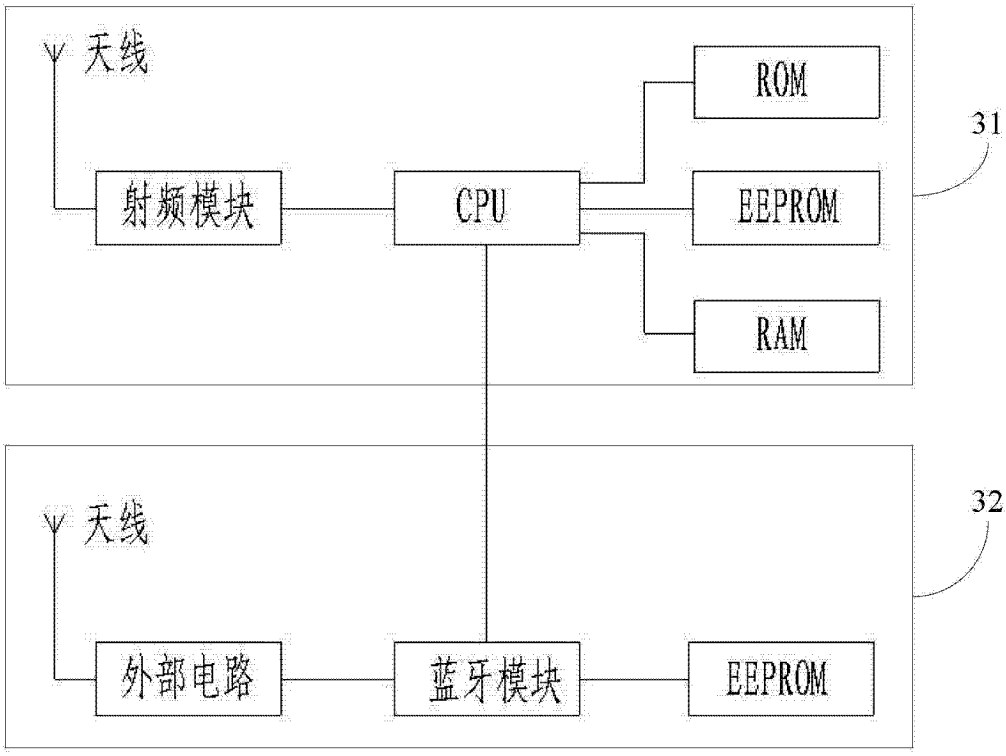


图 3

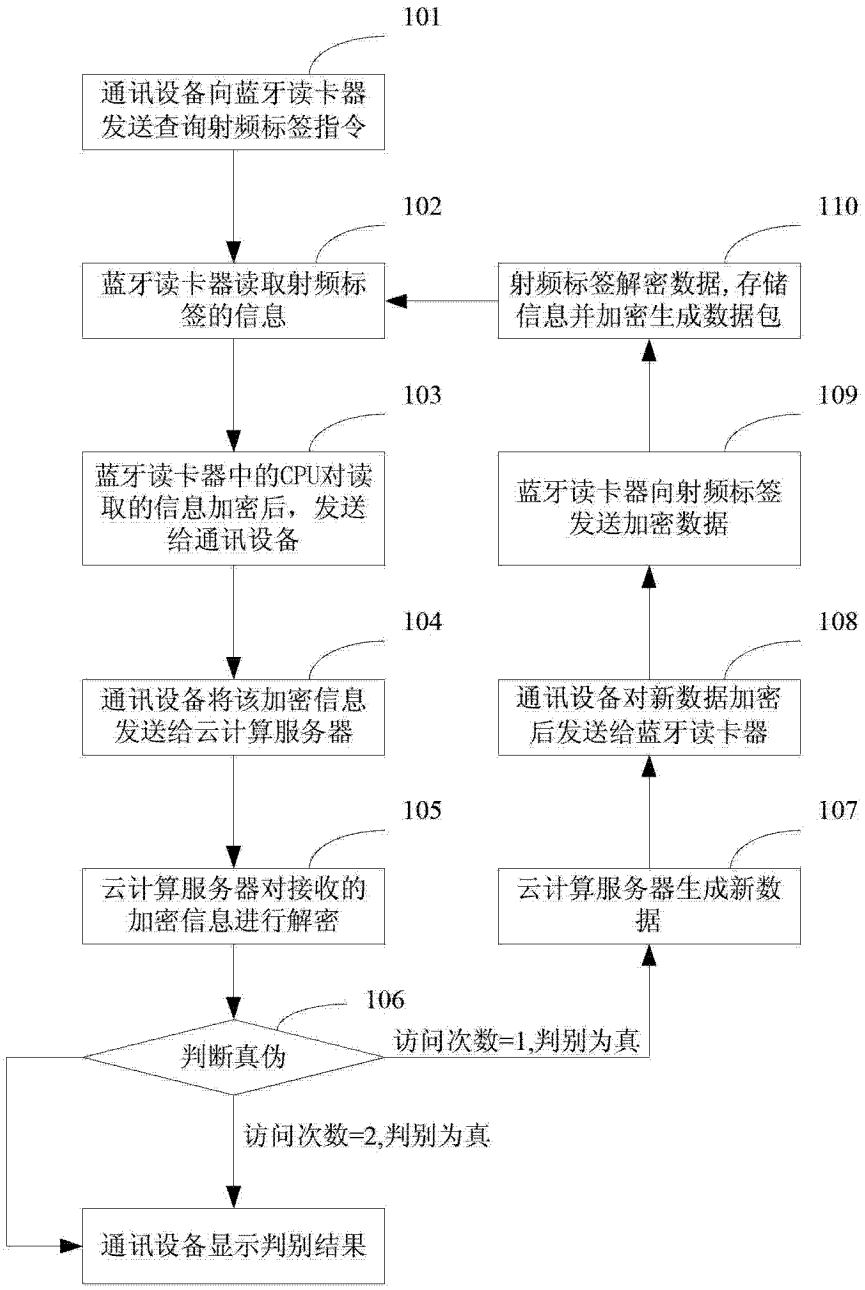

101
通讯设备向蓝牙读卡器发送查询射频标签指令
102
蓝牙读卡器读取射频标签的信息
103
蓝牙读卡器中的CPU对读取的信息加密后，发送给通讯设备
104
通讯设备将该加密信息发送给云计算服务器
105
云计算服务器对接收的加密信息进行解密
106
判断真伪
访问次数=1,判别为真
访问次数=2,判别为真
通讯设备显示判别结果
107
云计算服务器生成新数据
108
通讯设备对新数据加密后发送给蓝牙读卡器
109
蓝牙读卡器向射频标签发送加密数据
110
射频标签解密数据，存储信息并加密生成数据包

图 4