(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 105871855 B
(45)授权公告日 2019.09.13

(21)申请号 201610221608.6

(22)申请日 2016.04.11

(65)同一申请的已公布的文献号
申请公布号 CN 105871855 A

(43)申请公布日 2016.08.17

(73)专利权人 杨鹏
地址 430030 湖北省武汉市硚口区建设大道384-58号29栋

(72)发明人 杨鹏

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 陈卫

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

(56)对比文件
CN 104794626 A,2015.07.22,
CN 103023876 A,2013.04.03,
CN 102208043 A,2011.10.05,
WO 2015/028824 A1,2015.03.05,
US 2016/0080379 A1,2016.03.17,
CN 105303097 A,2016.02.03,
CN 104794626 A,2015.07.22,
CN 103646044 A,2014.03.19,
CN 104821986 A,2015.08.05,
CN 103136678 A,2013.06.05,
CN 103177367 A,2013.06.26,
CN 105205365 A,2015.12.30,
CN 105184587 A,2015.12.23,

审查员 徐苏宁

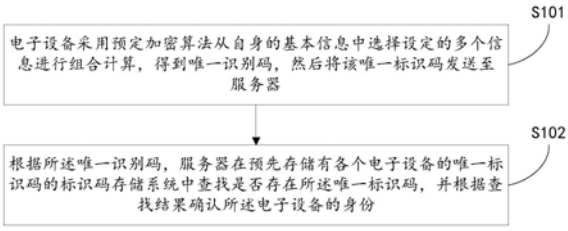
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种电子设备标识码生成、存储和识别的方法及系统

(57)摘要

本发明公开了一种电子设备标识码生成、存储和识别的方法及系统，其中，所述方法包括：电子设备采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，得到唯一识别码，然后将该唯一标识码发送至服务器；根据所述唯一识别码，服务器在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码，并根据查找结果确认所述电子设备的身份。本发明能够选择电子设备的基本信息中设定的多个信息进行组合计算得到电子设备的唯一标识码，并将其存储至由多个互为备份的分布式区块链数据库组成的标识码存储系统中，避免被黑客攻击篡改数据，能安全的对电子设备的身份进行识别，还可用于防伪，实用性较强。



CN 105871855 B

1.一种电子设备标识码生成、存储和识别的方法,其特征在于,所述方法包括:

S101、电子设备采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算,得到唯一标识码,然后将该唯一标识码发送至服务器;

S102、根据所述唯一标识码,服务器在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码,并根据查找结果确认所述电子设备的身份;

所述标识码存储系统由分布式区块链数据库组成,每一个区块链数据库均存储有各个电子设备的唯一标识码,且每一个区块链数据库互为备份;

当所述服务器为电子设备生产厂家服务器时,所述S102具体包括:

电子设备生产厂家服务器在标识码存储系统中查找是否存在所述电子设备发送的唯一标识码,若存在,则确认所述电子设备为正品,并将确认结果反馈至所述电子设备,否则,确认所述电子设备为仿造品,并将确认结果反馈至所述电子设备,同时将该唯一标识码存储至仿造品标识码存储系统;

当所述服务器为第三方服务器,则所述S102具体包括:

第三方服务器在标识码存储系统中查找是否存在所述电子设备发送的唯一标识码,若存在,则确认所述电子设备为老用户,并将确认结果反馈至所述电子设备,否则,确认所述电子设备为新用户,并将确认结果反馈至所述电子设备,同时将该唯一标识码存储至所述标识码存储系统。

2.如权利要求1所述的一种电子设备标识码生成、存储和识别的方法,其特征在于,所述基本信息具体包括:电子设备的CPU信息,GPU信息,存储芯片序列号,wifi的MAC地址,IMEI码,MEID码,ESN码,进网许可证编号,蓝牙MAC地址,制造商信息,Sim序列号,NFC识别码,及采集的指纹特征码,虹膜特征码,声纹特征码以及步态特征码。

3.如权利要求2所述的一种电子设备标识码生成、存储和识别的方法,其特征在于,所述S102之前还包括:

服务器对各个电子设备的所述基本信息进行采集,并采用与S101中相同的预定加密算法从所述基本信息中选择与S101中相同的所述设定的多个信息进行组合计算,得到每个电子设备的唯一标识码,并将各个电子设备的唯一标识码存储至所述标识码存储系统。

4.一种电子设备标识码生成、存储和识别的系统,其特征在于,所述系统包括电子设备和服务器;

所述电子设备,用于采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算,得到唯一标识码,然后将该唯一标识码发送至服务器;

所述服务器包括:

查找单元,用于根据所述唯一标识码,在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码;

确认单元,用于根据所述查找单元的查找结果确认所述电子设备的身份;

所述标识码存储系统由分布式区块链数据库组成,每一个区块链数据库均存储有各个电子设备的唯一标识码,且每一个区块链数据库互为备份;

所述服务器具体为电子设备生产厂家服务器或者第三方服务器;

当所述服务器为电子设备生产厂家服务器时,所述确认单元具体用于:

若标识码存储系统中存在所述电子设备发送的唯一标识码,则确认所述电子设备为正

品，并将确认结果反馈至所述电子设备，否则，确认所述电子设备为仿造品，并将确认结果反馈至所述电子设备，同时将该唯一标识码存储至仿造品标识码存储系统；

当所述服务器为第三方服务器时，所述确认单元具体用于：

若标识码存储系统中存在所述电子设备发送的唯一标识码，则确认所述电子设备为老用户，并将确认结果反馈至所述电子设备，否则，确认所述电子设备为新用户，并将确认结果反馈至所述电子设备，同时将该唯一标识码存储至所述标识码存储系统。

5.如权利要求4所述的一种电子设备标识码生成、存储和识别的系统，其特征在于，所述基本信息具体包括：电子设备的CPU信息，GPU信息，存储芯片序列号，wifi的MAC地址，IMEI码，MEID码，ESN码，进网许可证编号，蓝牙MAC地址，制造商信息，Sim序列号，NFC识别码，及采集的指纹特征码，虹膜特征码，声纹特征码以及步态特征码。

6.如权利要求5所述的一种电子设备标识码生成、存储和识别的系统，其特征在于，所述服务器还包括：

采集计算单元，用于对各个电子设备的所述基本信息进行采集，并采用与所述电子设备中相同的预定加密算法从所述基本信息中选择与所述电子设备中相同的所述设定的多个信息进行组合计算，得到每个电子设备的唯一标识码；

存储单元，用于将所述采集计算单元得到的各个电子设备的唯一标识码存储至所述标识码存储系统。

一种电子设备标识码生成、存储和识别的方法及系统

技术领域

[0001] 本发明涉及电子技术领域，具体涉及一种电子设备标识码生成、存储和识别的方法及系统。

背景技术

[0002] 当前电子设备的身份识别和防伪是业界难题，目前主流的身份识别和防伪是通过存储有电子设备的相关信息的非区块链模式的数据库来校验身份信息。当前技术主要存在的缺点是：1、如果数据库存储的电子设备的相关信息泄露，就可以根据泄露的电子设备的相关信息伪造出对应的电子设备；2、如果存储有电子设备相关信息的数据库被侵入，则数据库中存储的该电子设备的相关信息就存在被篡改的风险。

发明内容

[0003] 本发明所要解决的技术问题是提供一种电子设备标识码生成、存储和识别的方法及系统，根据电子设备的多个基本信息计算得到电子设备的唯一标识码，并将其存储在由分布式区块链数据库组成标识码存储系统中，能够在分布式区块链数据库被侵入时防止电子设备的基本信息被泄露，进而防止发生利用电子设备的基本信息伪造出对应的电子设备的可能，并避免存储所述唯一标识码的数据库中的数据被篡改。

[0004] 本发明解决上述技术问题的技术方案如下：

[0005] 依据本发明的一个方面，提供了一种电子设备标识码生成、存储和识别的方法，所述方法包括：

[0006] S101、电子设备采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，得到唯一标识码，然后将该唯一标识码发送至服务器；

[0007] S102、根据所述唯一标识码，服务器在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码，并根据查找结果确认所述电子设备的身份。

[0008] 依据本发明的另一个方面，提供了一种电子设备标识码生成、存储和识别的系统，所述系统包括电子设备和服务器；

[0009] 所述电子设备，用于采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，得到唯一标识码，然后将该唯一标识码发送至服务器；

[0010] 所述服务器包括：

[0011] 查找单元，用于根据所述唯一标识码，在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码；

[0012] 确认单元，用于根据所述查找单元的查找结果确认所述电子设备的身份。

[0013] 本发明的有益效果：服务器能够采用预定加密算法从各个电子设备的基本信息中选择设定的多个信息进行组合计算，得到每个电子设备独有的唯一标识码，然后将各个电子设备的唯一标识码存储至标识码存储系统中；所述唯一标识码是根据电子设备独有的多

个基本信息计算得到的，因此是电子设备独有的唯一标识码，无法伪造；所述标识码存储系统是由分布式区块链数据库组成，每一个区块链数据库均存储有各个电子设备的唯一标识码，且每一个区块链数据库互为备份，黑客即使攻击破坏篡改了一个分布式区块链数据库，也会因为其他备份的分布式区块链数据库的存在，而无法破坏整个分布式区块链数据库系统，备份的分布式区块链数据库越多，所述标识码存储系统中的数据就越安全；因为所述标识码存储系统中只存储了电子设备的唯一标识码，并没有存储电子设备的基本信息，所以即使黑客入侵了所述标识码存储系统中的分布式区块链数据库也无法获取电子设备的基本信息，也就不存在根据泄露的电子设备的唯一标识码制造出相同的设备的可能；因此能安全方便的对电子设备的身份进行识别。本发明能够解决电子设备的身份识别问题以及电子设备的防伪问题，安全方便，实用性较强。

附图说明

[0014] 图1为本发明实施例一的一种电子设备标识码生成、存储和识别的方法流程图；

[0015] 图2为本发明实施例二的一种电子设备标识码生成、存储和识别的系统示意图。

具体实施方式

[0016] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0017] 实施例一、一种电子设备标识码生成、存储和识别的方法。下面结合图 1对本实施例提供的方法进行详细说明。

[0018] 参见图1，S101、电子设备采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，得到唯一标识码，然后将该唯一标识码发送至服务器。

[0019] 具体的，电子设备采用预定加密算法从自身独有的基本信息中选择设定类别的多个信息，进行组合计算得到自身独有的唯一标识码，并将所述唯一标识码发送至服务器。所述基本信息具体包括电子设备的CPU信息，GPU信息，存储芯片序列号，wifi的MAC地址，IMEI码，MEID码，ESN码，进网许可证编号，蓝牙MAC地址，制造商信息，Sim序列号，NFC识别码，及采集的指纹特征码，虹膜特征码，声纹特征码以及步态特征码，所述基本信息包含的内容并不限于上述列举出的内容，因为每个电子设备包含的基本信息种类并不相同；所述预定加密算法采用特定通用的加密算法，根据设定的规则从所述基本信息中选择设定种类的信息进行组合计算以满足不同的需求。

[0020] 例如，若选择的电子设备的信息中包括Sim序列号，指纹特征码，虹膜特征码，声纹特征码或者步态特征码等可变更的基本信息，则表示所述电子设备的对应的唯一标识码对电子设备的使用环境有要求；若选择的电子设备的信息中只包括电子设备的CPU信息，GPU信息等电子设备固有的不可变更的基本信息，则表示所述电子设备对应的唯一标识码只对电子设备本身有要求，不随使用环境变化而变化。例如，若服务器中存储有根据电子设备基本信息中固有的不可变更的多个设定种类的信息进行组合计算得到唯一标识码，以及根据该电子设备基本信息中可变更的多个设定种类的信息进行组合计算得到的唯一标识码；那么，在电子设备将固有的不可变更的多个设定种类的信息对应的唯一标识码，以及可变更的多个设定种类的信息对应的唯一标识码，发送给服务器进行验证时；服务器在确认所述

电子设备身份的同时，还可以判断电子设备的使用环境是否发生变化。

[0021] 采用预定加密算法根据设定的规则从电子设备的基本信息中选择设定的多个基本信息进行组合计算得到的唯一标识码，是电子设备在该设定规则下独有的唯一的标识码，无法伪造，并且电子设备只是将唯一标识码发送至服务器进行验证，不需要采用电子设备的基本信息进行验证，更加方便安全，避免信息泄露。

[0022] S102、根据所述唯一识别码，服务器在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码，并根据查找结果确认所述电子设备的身份。

[0023] 具体的，根据所述电子设备发送的唯一识别码，服务器在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述电子设备发送的所述唯一标识码，并根据查找结果确认所述电子设备的身份。

[0024] 在步骤S102之前还包括，服务器对各个电子设备的所述基本信息进行采集，并采用与S101中相同的预定加密算法从所述基本信息中选择与S101 中相同的所述设定的多个信息进行组合计算，得到每个电子设备的唯一标识码，并将各个电子设备的唯一标识码存储至所述标识码存储系统。

[0025] 具体的，服务器采用与所述电子设备中使用的相同的设定规则从各个电子设备的所述基本信息中选择设定的种类的信息进行组合计算，并采用与 S101中相同的预定加密算法对多个设定的种类的信息进行组合计算，进而得到每个电子设备的唯一标识码，并将各个电子设备的唯一标识码存储至所述标识码存储系统。

[0026] 所述标识码存储系统具体是由分布式区块链数据库组成，每一个区块链数据库均存储有各个电子设备的唯一标识码，且每一个区块链数据库互为备份。黑客即使攻击破坏篡改了一个分布式区块链数据库，也会因为其他备份的分布式区块链数据库的存在，而无法破坏整个分布式区块链数据库系统，备份的分布式区块链数据库越多，所述标识码存储系统中的数据就越安全。另外，因为所述标识码存储系统中只存储了电子设备的唯一标识码，并没有存储电子设备的基本信息，所以即使黑客入侵了所述标识码存储系统中的分布式区块链数据库也无法获取电子设备的基本信息，也就不存在根据泄露的电子设备的唯一标识码制造出相同的设备的可能。

[0027] 另外，电子设备在设定规则下从所述基本信息中选择的信息类别都是特定的，因此，电子设备采用预定加密算法计算得到的自身独有的唯一标识码，与服务器采用预定加密算法在该设定规则下对电子设备设定类别的信息进行组合计算得到的唯一标识码相同，因此才可以进行验证确定电子设备的身份。

[0028] 所述服务器具体可为电子设备生产厂家服务器或者第三方服务器。

[0029] 当所述服务器为电子设备生产厂家服务器时，电子设备生产厂家服务器在所述标识码存储系统中查找是否存在电子设备发送的唯一标识码，若存在，则确认所述电子设备为正品，并将确认结果反馈至所述电子设备，否则确认所述电子设备为仿造品，并将确认结果反馈至所述电子设备，同时将该唯一标识码存储至仿造品标识码存储系统；

[0030] 具体的，当所述服务器为电子设备生产厂家服务器时，电子设备生产厂家服务器在电子设备生产之后，就在厂家设定规则下采集电子设备的基本信息，并从中选择设定类别的多个信息，然后采用所述预定加密算法进行组合计算，进而得到电子设备的唯一标识

码，然后存储至标识码存储系统中。用于防伪，只存储电子设备的唯一标识码，并不存储电子设备的基本信息，更加安全。厂家生产的电子设备中设置有所述厂家设定规则，便于电子设备验证真伪，并且每一个电子设备中除了设置有厂家设定规则外，还设置有设备设定规则，所述设备设定规则是电子设备自身带有的规则。

[0031] 客户在购买电子设备时，当不确定电子设备是否为正品时，可将电子设备在所述厂家设定规则下采用预定加密算法从自身的基本信息中选择设定类别的多个信息进行组合计算得到唯一标识码，发送至电子设备生产厂家服务器进行验证；若电子设备生产厂家服务器在所述标识码存储系统中查找到所述电子设备发送的唯一标识码，则确认所述电子设备为正品，并将确认结果反馈至所述电子设备以告知客户，客户即可放心购买；若电子设备生产厂家服务器在所述标识码存储系统中查找不到所述电子设备的唯一标识码，则确认所述电子设备为仿造品，并将结果反馈告知客户，客户不可购买，以防被骗，同时将仿造的电子设备标识码存储至仿造品标识码存储系统中，以便在打假时提供帮助。所述仿造品标识码存储系统同样是由分布式区块链数据库组成，每一个区块链数据库均存储有仿造的电子设备的唯一标识码，且每一个区块链数据库互为备份。

[0032] 因为所述标识码存储系统中只存储了电子设备的唯一标识码，并没有存储电子设备的基本信息，所以即使黑客入侵了所述标识码存储系统中的分布式区块链数据库也无法获取电子设备的基本信息，也就不存在根据泄露的电子设备的唯一标识码制造出相同的设备的可能，因而能对电子设备的进行防伪，避免客户被骗。

[0033] 当所述服务器为第三方服务器时，第三方服务器在标识码存储系统中查找是否存在电子设备发送的唯一标识码，若存在，则确认所述电子设备为老用户，并将确认结果反馈至所述电子设备，否则，确认所述电子设备为新用户，并将确认结果反馈至所述电子设备，同时将该唯一标识码存储至所述标识码存储系统。

[0034] 具体的，当所述服务器为第三方服务器时，电子设备在使用第三方生产的某种软件时，若第三方服务器设置有第三方设定规则，则第三方服务器获取电子设备的所述基本信息，然后在所述第三方设定规则下采用所述预定加密算法从采集的电子设备的所述基本信息中选择设定种类的多个信息进行组合计算，进而得到电子设备的唯一标识码，并将电子设备的唯一标识码存储至标识码存储系统中。

[0035] 当第三方服务器需要判断安装第三方生产的某种软件的电子设备是否为新用户时，电子设备获取所述第三方设定规则，并在所述第三方设定规则下从自身的基本信息中选择设定类别的多个信息进行组合计算得到的唯一标识码，并发送至第三方服务器，第三方服务器在所述标识码存储系统中查找是否存在所述电子设备的唯一标识码，若存在，则确认此电子设备为老客户，并将确认结果反馈至所述电子设备，若不存在，则第三方服务器判断此电子设备为新用户，并将确认结果反馈至所述电子设备，同时将所述唯一标识码存储至所述标识码存储系统，以便日后继续进行新老用户的识别。

[0036] 或者当第三方服务器需要判断安装第三方生产的某种软件的电子设备是否为新用户时，也可以第三方服务器自己采集获取电子设备的基本信息，然后在所述第三方设定规则下采用所述预定加密算法从采集的电子设备的基本信息中选择设定类别的多个信息进行组合计算，得到电子设备的唯一标识码，从而在所述标识码存储系统中进行查找，进而确定电子设备是否为老用户。

[0037] 另外，在电子设备不允许第三方服务器获取电子设备的基本信息时，由电子设备在自身带有的所述设备设定规则下，采用所述预定加密算法从自身的基本信息中采集设定种类的多个信息进行组合计算得到的唯一标识码发送给所述第三方服务器，以便第三方服务器将唯一标识码存储至标识码存储系统中进行记录，以及进行身份验证。

[0038] 因为第三方服务器的所述标识码存储系统中只存储了电子设备的唯一标识码，并没有存储电子设备的基本信息，所以即使黑客入侵了所述标识码存储系统中的分布式区块链数据库也无法获取电子设备的基本信息，也就不存在根据泄露的电子设备的唯一标识码制造出相同的设备的可能，因而能安全的对电子设备的身份进行识别。

[0039] 厂家设定规则对应的从电子设备的基本信息中选择的设定的多个信息的种类是固定的，在验证的时候，电子设备根据存储在电子设备内部的厂家设定规则得到对应于厂家服务器的唯一标识码；若第三方服务器设置有第三方设定规则，其对应的从电子设备的基本信息中选择的设定的多个信息的种类也是固定的，在验证的时候，电子设备从第三方服务器中获取所述第三方设定规则，进而得到对应于第三方服务器的唯一标识码；或者第三方服务器从电子设备中采集电子设备的基本信息，并从中选择多个设定的信息，进而得到对应于所述第三方设定规则的唯一标识码；若第三方服务器没有设置第三方设定规则或者电子设备不允许第三方采集自身的基本信息，由电子设备根据自身的所述设备设定规则得到唯一标识码，并发送至第三方服务器进行存储以及验证。在每个设定规则下，电子设备对应的唯一标识码是独有并唯一的。

[0040] 实施例二、一种电子设备标识码生成、存储和识别的系统。下面结合图 2对本实施例提供的系统进行详细说明。

[0041] 参见图2，本实施例提供的系统包括服务器和电子设备。

[0042] 所述电子设备，用于采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，得到唯一标识码，然后将该唯一标识码发送至服务器。

[0043] 具体的，所述电子设备采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，进而得到自身独有的唯一标识码，并将所述唯一标识码发送至服务器。所述基本信息具体包括电子设备的CPU信息，GPU信息，存储芯片序列号，wifi的MAC地址，IMEI码，MEID码，ESN码，进网许可证编号，蓝牙MAC地址，制造商信息，Sim序列号，NFC识别码，及采集的指纹特征码，虹膜特征码，声纹特征码以及步态特征码，所述基本信息包含的内容不限于上述列举出的内容，因为每个电子设备包含的基本信息种类并不相同；所述预定加密算法采用特定通用的加密算法，根据设定的规则从所述基本信息中选择设定种类的信息进行组合计算以满足不同的需求。

[0044] 例如，若选择的电子设备的信息中包括Sim序列号，指纹特征码，虹膜特征码，声纹特征码或者步态特征码等可变更的基本信息，则表示所述电子设备的对应的唯一标识码对电子设备的使用环境有要求；若选择的电子设备的信息中只包括电子设备的CPU信息，GPU信息等电子设备固有的不可变更的基本信息，则表示所述电子设备对应的唯一标识码只对电子设备本身有要求，不随使用环境变化而变化。例如，若服务器中存储有根据电子设备基本信息中固有的不可变更的多个设定种类的信息进行组合计算得到唯一标识码，以及根据该电子设备基本信息中可变更的多个设定种类的信息进行组合计算得到的唯一标识码；那么，在电子设备将固有的不可变更的多个设定种类的信息对应的唯一标识码，以及可变更

的多个设定种类的信息对应的唯一标识码，发送给服务器进行验证时；服务器在确认所述电子设备身份的同时，还可以判断电子设备的使用环境是否发生变化。

[0045] 采用预定加密算法根据设定的规则从电子设备的基本信息中选择设定种类的多个基本信息进行组合计算得到的唯一标识码，是电子设备在该设定规则下独有的唯一的标识码，无法伪造，并且电子设备只是将唯一标识码发送至服务器进行验证，不需要采用电子设备的基本信息进行验证，更加方便安全，避免信息泄露。

[0046] 所述服务器具体包括查找单元以及确认单元。

[0047] 所述查找单元，用于根据所述唯一标识码，在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码；

[0048] 所述确认单元，用于根据所述查找单元的查找结果确认所述电子设备的身份。

[0049] 所述服务器还包括采集计算单元以及存储单元；

[0050] 采集计算单元，用于对各个电子设备的所述基本信息进行采集，并采用与所述电子设备中相同的预定加密算法从所述基本信息中选择与所述电子设备中相同的所述设定的多个信息进行组合计算，得到每个电子设备的唯一标识码；

[0051] 存储单元，用于将所述采集计算单元得到的各个电子设备的唯一标识码存储至所述标识码存储系统。

[0052] 具体的，所述采集计算单元采用的与所述电子设备中使用的相同的设定规则从各个电子设备的所述基本信息中选择设定的种类的信息进行组合计算，并采用与所述电子设备中使用的相同的所述预定加密算法对多个设定的种类的信息进行组合计算，进而得到每个电子设备的唯一标识码。所述存储单元将得到的各个电子设备的唯一标识码存储至所述标识码存储系统。所述标识码存储系统由分布式区块链数据库组成，每一个区块链数据库均存储有各个电子设备的唯一标识码，且每一个区块链数据库互为备份。黑客即使攻击破坏篡改了一个分布式区块链数据库，也会因为其他备份的分布式区块链数据库的存在，而无法破坏整个分布式区块链数据库系统，备份的分布式区块链数据库越多，所述标识码存储系统中的数据就越安全。另外，因为所述标识码存储系统中只存储了电子设备的唯一标识码，并没有存储电子设备的基本信息，所以即使黑客入侵了所述标识码存储系统中的分布式区块链数据库也无法获取电子设备的基本信息，也就不存在根据泄露的电子设备的唯一标识码制造出相同的设备的可能。

[0053] 具体的，采集计算单元采用预定加密算法从各个电子设备的基本信息中选择设定的多个信息进行组合计算，得到每个电子设备的唯一标识码，所述存储单元将各个电子设备的唯一标识码存储至标识码存储系统；电子设备采用预定加密算法从自身的所述基本信息中选择设定的多个信息进行组合计算，得到唯一标识码，然后将其发送至服务器；所述查找单元在所述标识码存储系统中查找是否存在所述电子设备发送的所述唯一标识码；所述确认单元根据查找结果确认所述电子设备的身份。

[0054] 所述服务器具体为电子设备生产厂家服务器或者第三方服务器。

[0055] 具体的，当所述服务器为电子设备生产厂家服务器时，所述电子设备生产厂家服务器在所述标识码存储系统中查找是否存在所述电子设备发送的唯一标识码，若存在，则确认所述电子设备为正品，并将确认结果反馈至所述电子设备，否则，确认所述电子设备为仿造品，并将确认结果反馈至所述电子设备，同时将该唯一标识码存储至仿造品标识码存

储系统，以便在防伪打假时提供帮助，其中，所述仿造品标识码存储系统同样是由分布式区块链数据库组成，每一个区块链数据库均存储有各个电子设备的唯一标识码，且每一个区块链数据库互为备份。

[0056] 具体的，当所述服务器为第三方服务器时，所述第三方服务器在标识码存储系统中查找是否存在所述电子设备发送的唯一标识码，若存在，则确认所述电子设备为老用户，并将确认结果反馈至所述电子设备，否则，确认所述电子设备为新用户，并将确认结果反馈至所述电子设备，同时将该唯一标识码存储至所述标识码存储系统中，以便日后继续进行新老用户的识别。

[0057] 本发明提供的一种电子设备标识码生成、存储和识别的方法及系统，服务器采用预定加密算法从各个电子设备的基本信息中选择设定的多个信息进行组合计算，得到每个电子设备的唯一标识码，然后将各个电子设备的唯一标识码存储至标识码存储系统中；所述唯一标识码是根据电子设备的多个基本信息计算得到的因此是电子设备自身独有的唯一标识码，无法伪造；所述标识码存储系统是由分布式区块链数据库组成，每一个区块链数据库均存储有各个电子设备的唯一标识码，且每一个区块链数据库互为备份，黑客即使攻击破坏篡改了一个分布式区块链数据库，也会因为其他备份的分布式区块链数据库的存在，而无法破坏整个分布式区块链数据库系统，备份的分布式区块链数据库越多，所述标识码存储系统中的数据就越安全；因为所述标识码存储系统中只存储了电子设备的唯一标识码，并没有存储电子设备的基本信息，所以即使黑客入侵了所述标识码存储系统中的分布式区块链数据库也无法获取电子设备的基本信息，也就不存在根据泄露的电子设备的唯一标识码制造出相同的设备的可能；因此能够方便安全的对电子设备的身份进行识别。本发明能够解决电子设备的身份识别以及防伪问题，安全方便，实用性较强。

[0058] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

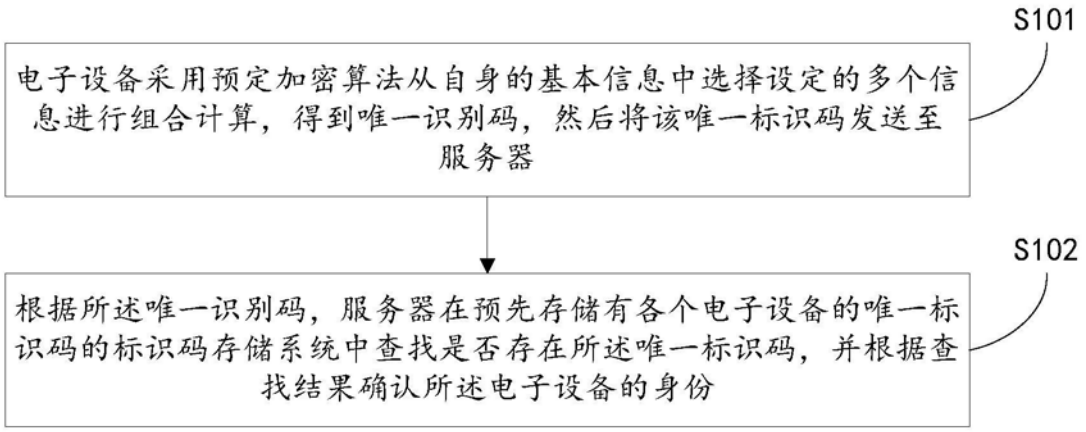

S101
电子设备采用预定加密算法从自身的基本信息中选择设定的多个信息进行组合计算，得到唯一识别码，然后将该唯一标识码发送至服务器
S102
根据所述唯一识别码，服务器在预先存储有各个电子设备的唯一标识码的标识码存储系统中查找是否存在所述唯一标识码，并根据查找结果确认所述电子设备的身份

图1

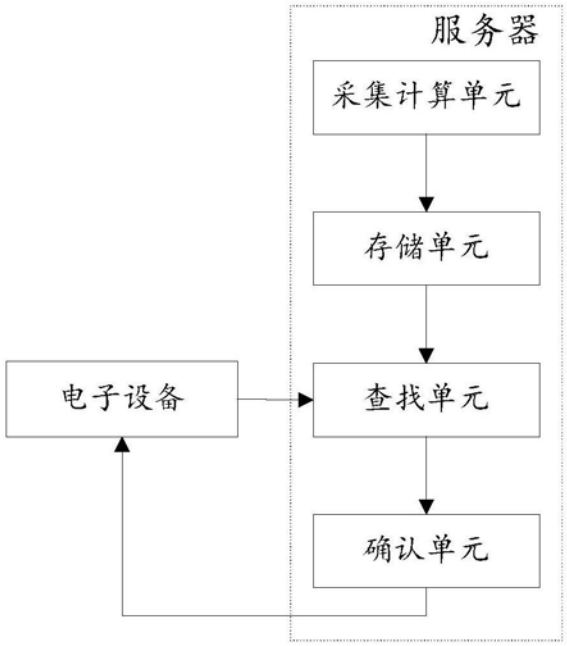

服务器
采集计算单元
存储单元
电子设备
查找单元
确认单元

图2