(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 108363929 A
(43)申请公布日 2018.08.03

(21)申请号 201810134242.8

(22)申请日 2018.02.09

(71)申请人 广州旭能信息科技有限公司
地址 510000 广东省广州市白云区京溪桥东侧广州新百佳小商品城A12285之一号

(72)发明人 许瑞本 艾歆 邓本瑜

(74)专利代理机构 广州市越秀区海心联合专利代理事务所(普通合伙) 44295
代理人 王洪娟 蔡国

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06F 21/78(2013.01)

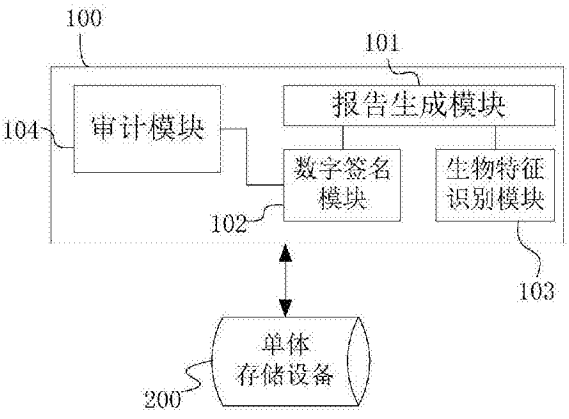
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种存储设备信息消除报告生成和防篡改系统及方法

(57)摘要

本发明公开了一种存储设备信息消除报告生成和防篡改系统及方法,包括报告生成模块,用于利用多层级报告内嵌及各层级对应的具有唯一性的摘要讯息生成防篡改报告;数字签名模块,用于获取全球唯一地址编码以及进行加密签名;生物特征识别模块,用于生物特征。其优点在于,通过唯一对应的摘要讯息与JSON报告相结合得到多层级的防篡改报告,其中只要任一层级发生数据变化,即被篡改时,对应的摘要讯息自然与原内嵌的摘要讯息不一致。



CN 108363929 A

1.一种存储设备信息消除报告生成和防篡改系统,其特征在于,包括:

报告生成模块(101),用于收集和记录信息消除过程的信息数据,并利用多层级报告内嵌及各层级对应的具有唯一性的摘要讯息生成防篡改报告;

数字签名模块(102),用于获取全球唯一地址编码并输入至报告生成模块(101),以及对报告生成模块(101)指定的数据进行加密签名并将加密签名内容反馈至报告生成模块(101);

生物特征识别模块(103),用于获取操作人员的生物特征并将操作人员信息反馈至报告生成模块(101)。

2.根据权利要求1所述存储设备信息消除报告生成和防篡改系统,其特征在于,所述的数字签名模块(102)利用非对称数据加密引擎引用私钥对指定的数据进行加密签名。

3.根据权利要求1所述存储设备信息消除报告生成和防篡改系统,其特征在于,所述的报告生成模块(101)收集和记录信息数据后首先生成源报告,然后对源报告输出唯一对应的第一摘要讯息,并利用数字签名模块(102)将第一摘要讯息加密签名为加密讯息;然后将加密讯息写入源报告得到签名报告,对签名报告输出唯一对应的第二摘要讯息;最后将第二摘要讯息写入签名报告得到防篡改报告。

4.根据权利要求3所述存储设备信息消除报告生成和防篡改系统,其特征在于,所述的报告生成模块(101)利用Hash算法输出各报告对应的摘要讯息。

5.根据权利要求3所述存储设备信息消除报告生成和防篡改系统,其特征在于,所述的源报告、签名报告和防篡改报告为JSON格式。

6.根据权利要求1所述存储设备信息消除报告生成和防篡改系统,其特征在于,将防篡改报告写入对应单体存储设备(200)的指定位置。

7.根据权利要求1所述存储设备信息消除报告生成和防篡改系统,其特征在于,还包括审计模块(104),用于对防篡改报告进行逐层级审计。

8.根据权利要求7所述存储设备信息消除报告生成和防篡改系统,其特征在于,所述的审计模块(104)在对应的单体存储设备(200)指定位置读取防篡改报告,并拆分为签名报告和第二摘要讯息;进行第一次校验,算出签名报告的唯一摘要讯息与第二摘要讯息比对,摘要讯息全文一致为校验通过;将签名报告拆分为源报告和加密讯息;进行第二次校验,算出源报告的唯一摘要讯息并与加密讯息解密后的摘要讯息进行全文校验,全文一致为校验通过;再进行第三次校验,从源报告解析出记录的单体存储设备(200)基本信息与当前被审计的单体存储设备(200)基本信息进行一致性校验;第三次校验通过后审计结束。

9.根据权利要求1-8任一所述存储设备信息消除报告生成和防篡改方法,其特征在于,包括如下步骤:

S11、对单体存储设备(200)进行信息消除并收集和记录信息消除过程的信息数据;

S12、生成包括了时间戳、UUID和操作人员讯息的JSON格式的源报告;

S13、利用Hash算法对源报告输出唯一对应的第一摘要讯息,并利用非对称数据加密引擎引用私钥对第一摘要讯息加密签名得到加密讯息;

S14、将加密讯息写入源报告得到签名报告;

S15、利用Hash算法对签名报告输出唯一对应的第二摘要讯息;

S16、将第二摘要讯息写入签名报告得到防篡改报告;

S17、将防篡改报告写入单体存储设备(200)指定位置。

10.根据权利要求9所述存储设备信息消除报告生成和防篡改方法，其特征在于，包括如下步骤：

S21、在单体存储设备(200)指定位置读取防篡改报告；

S22、将防篡改报告拆分为签名报告和第二摘要讯息；

S23、进行第一次校验：利用Hash算法算出签名报告的唯一摘要讯息与第二摘要讯息比对，摘要讯息全文一致为校验通过；

S24、将签名报告拆分为源报告和加密讯息；

S25、进行第二次校验：利用Hash算法算出源报告的唯一摘要讯息并与加密讯息解密后的摘要讯息进行全文校验，全文一致为校验通过；

S26、进行第三次校验：从源报告解析出记录的单体存储设备(200)基本信息与当前被审计的单体存储设备(200)基本信息进行一致性校验，校验通过后进行下一步；

S27，解析源报告，得到正确的操作人员信息、时间戳、UUID。

一种存储设备信息消除报告生成和防篡改系统及方法

技术领域

[0001] 本发明涉及一种计算机领域的存储信息消除系统及方法，尤其涉及一种存储设备信息消除报告生成和防篡改系统及方法。

背景技术

[0002] 随着计算机和通信技术的发展和规模应用，大量的电子数据需要进行有效可靠的存储和管理，存储设备是电子信息的存储载体。对过期数据信息或者不可公开数据信息进行信息消除，是电子数据管理工作中的重要一环。

[0003] 在对存储设备进行信息消除的过程中，需要对存储设备的基本信息、读写日志、消除流程、执行消除的时间等信息进行汇总并形成信息消除报告。现有的信息消除工具对信息消除报告的生成和审计管理方法方式存在以下缺点：

[0004] 1.对生成报告的操作人员没有有效验证。

[0005] 2.对生成报告的消除设备没有有效验证。

[0006] 3.对生成报告的时间没有有效验证。

[0007] 4.对生成报告的内容没有有效的防篡改保护和验证。

发明内容

[0008] 为了解决上述现有技术存在的问题，本发明目的在于提供一种有效防止消除报告被篡改和对消除操作的人员和设备均具有有效验证的存储设备信息消除报告生成和防篡改系统及方法。

[0009] 本发明所述的一种存储设备信息消除报告生成和防篡改系统，包括：

[0010] 报告生成模块，用于收集和记录信息消除过程的信息数据，并利用多层级报告内嵌及各层级对应的具有唯一性的摘要讯息生成防篡改报告；

[0011] 数字签名模块，用于获取全球唯一地址编码并输入至报告生成模块，以及对报告生成模块指定的数据进行加密签名并将加密签名内容反馈至报告生成模块；

[0012] 生物特征识别模块，用于获取操作人员的生物特征并将操作人员信息反馈至报告生成模块。

[0013] 优选地，所述的数字签名模块利用非对称数据加密引擎引用私钥对指定的数据进行加密签名。

[0014] 优选地，所述的报告生成模块收集和记录信息数据后首先生成源报告，然后对源报告输出唯一对应的第一摘要讯息，并利用数字签名模块将第一摘要讯息加密签名为加密讯息；然后将加密讯息写入源报告得到签名报告，对签名报告输出唯一对应的第二摘要讯息；最后将第二摘要讯息写入签名报告得到防篡改报告。

[0015] 优选地，所述的报告生成模块利用Hash算法输出各报告对应的摘要讯息。

[0016] 优选地，所述的源报告、签名报告和防篡改报告为JSON格式。

[0017] 优选地，所述的存储设备信息消除报告生成和防篡改系统，将防篡改报告写入对

应单体存储设备的指定位置。

[0018] 优选地，所述的存储设备信息消除报告生成和防篡改系统，还包括审计模块，用于对防篡改报告进行逐层级审计。

[0019] 优选地，所述的审计模块在对应的单体存储设备指定位置读取防篡改报告，并拆分为签名报告和第二摘要讯息；进行第一次校验，算出签名报告的唯一摘要讯息与第二摘要讯息比对，摘要讯息全文一致为校验通过；将签名报告拆分为源报告和加密讯息；进行第二次校验，算出源报告的唯一摘要讯息并与加密讯息解密后的摘要讯息进行全文校验，全文一致为校验通过；再进行第三次校验，从源报告解析出记录的单体存储设备基本信息与当前被审计的单体存储设备基本信息进行一致性校验；第三次校验通过后审计结束。

[0020] 一种基于所述存储设备信息消除报告生成和防篡改系统的报告生成方法，包括如下步骤：

[0021] S11、对单体存储设备进行信息消除并收集和记录信息消除过程的信息数据；

[0022] S12、生成包括了时间戳、UUID和操作人员讯息的JSON格式的源报告；

[0023] S13、利用Hash算法对源报告输出唯一对应的第一摘要讯息，并利用非对称数据加密引擎引用私钥对第一摘要讯息加密签名得到加密讯息；

[0024] S14、将加密讯息写入源报告得到签名报告；

[0025] S15、利用Hash算法对签名报告输出唯一对应的第二摘要讯息；

[0026] S16、将第二摘要讯息写入签名报告得到防篡改报告；

[0027] S17、将防篡改报告写入单体存储设备指定位置。

[0028] 一种基于所述存储设备信息消除报告生成和防篡改方法的审计解析方法，包括如下步骤：

[0029] S21、在单体存储设备指定位置读取防篡改报告；

[0030] S22、将防篡改报告拆分为签名报告和第二摘要讯息；

[0031] S23、进行第一次校验：利用Hash算法算出签名报告的唯一摘要讯息与第二摘要讯息比对，摘要讯息全文一致为校验通过；

[0032] S24、将签名报告拆分为源报告和加密讯息；

[0033] S25、进行第二次校验：利用Hash算法算出源报告的唯一摘要讯息并与加密讯息解密后的摘要讯息进行全文校验，全文一致为校验通过；

[0034] S26、进行第三次校验：从源报告解析出记录的单体存储设备基本信息与当前被审计的单体存储设备基本信息进行一致性校验，校验通过后进行下一步；

[0035] S27，解析源报告，得到正确的操作人员信息、时间戳、UUID。

[0036] 本发明所述的一种存储设备信息消除报告生成和防篡改系统及方法，其优点在于，通过唯一对应的摘要讯息与JSON报告相结合得到多层级的防篡改报告，其中只要任一层级发生数据变化，即被篡改时，对应的摘要讯息自然与原内嵌的摘要讯息不一致。而其中一层级的摘要讯息被作为加密的对象由数字签名模块加密签名后插入至对应的报告中，杜绝了数据被逐个层级破解的可能性。可以在一个防篡改报告内一次性记录了进行消除操作的操作人员信息、时间戳以及UUID，对信息消除的单体存储设备进行有效管理和审计。最后将生成的防篡改报告写入至单体存储设备指定的位置，由于所述的指定位置并不对外公开，因此从篡改的最初步骤即产生隐藏的技术效果，进一步提高了防篡改的作用。

附图说明

[0037] 图1是本发明所述存储设备信息消除报告生成和防篡改系统的结构示意图；

[0038] 图2是本发明所述存储设备信息消除报告生成和防篡改方法的报告生成流程图；

[0039] 图3是本发明所述存储设备信息消除报告生成和防篡改方法的审计解析流程图。

具体实施方式

[0040] 如图1所示，本发明所述的一种存储设备信息消除报告生成和防篡改系统，包括直接对单体存储设备200进行信息消除操作的消除设备100，所述的消除设备100还包括了报告生成模块101、数字签名模块102、生物特征识别模块103和审计模块104。

[0041] 其中所述的报告生成模块101收集和记录信息数据后首先生成源报告，然后对源报告输出唯一对应的第一摘要讯息，并利用数字签名模块102将第一摘要讯息加密签名为加密讯息；然后将加密讯息写入源报告得到签名报告，对签名报告输出唯一对应的第二摘要讯息；最后将第二摘要讯息写入签名报告得到防篡改报告。所述的数字签名模块102获取属于消除设备100的全球唯一地址编码(UUID，Universally UniqueIdentifier)，并将UUID输入至消除设备100。在报告生成模块101需要对指定数据进行加密签名时，利用非对称数据加密引擎RSA引用私钥完成。最后消除设备100将防篡改报告写入对应单体存储设备200的指定位置，完成整个完整的防篡改报告生成过程。

[0042] 所述的生物特征识别模块103所采集的生物特征包括但不限定于指纹、人脸信息，生物特征识别模块103启用前先采集操作人员的生物特征并保存。

[0043] 在需要对单体存储设备200进行审计时，所述的审计模块104在对应的单体存储设备200指定位置读取防篡改报告，并拆分为签名报告和第二摘要讯息。进行第一次校验，算出签名报告的唯一摘要讯息与第二摘要讯息比对，摘要讯息全文一致为校验通过。将签名报告拆分为源报告和加密讯息，行第二次校验，算出源报告的唯一摘要讯息并与加密讯息解密后的摘要讯息进行全文校验，全文一致为校验通过。再进行第三次校验，从源报告解析出记录的单体存储设备200基本信息与当前被审计的单体存储设备200基本信息进行一致性校验；第三次校验通过后审计结束。

[0044] 所述存储设备信息消除报告生成和防篡改系统的工作原理和生成/审计方法如图2、3所示。

[0045] 在生成防篡改报告时，进行以下步骤：

[0046] S11、对单体存储设备200进行信息消除并收集和记录信息消除过程的信息数据；

[0047] S12、生成包括了时间戳、UUID和操作人员讯息的JSON格式的源报告J1；

[0048] S13、利用Hash算法对源报告J1输出唯一对应的第一摘要讯息Z1，并利用非对称数据加密引擎引用私钥对第一摘要讯息Z1加密签名得到加密讯息Z1m；

[0049] S14、将加密讯息Z1m写入源报告J1得到签名报告J2；

[0050] S15、利用Hash算法对签名报告J2输出唯一对应的第二摘要讯息Z2；

[0051] S16、将第二摘要讯息Z2写入签名报告J2得到防篡改报告J3；

[0052] S17、将防篡改报告J3写入单体存储设备200指定位置；完成整个防篡改报告J3生成流程。

[0053] 在需要对单体存储设备200中的防篡改报告J3进行审计和解析记载内容时，进行以下步骤：

[0054] S21、在单体存储设备200指定位置读取防篡改报告J3；

[0055] S22、将防篡改报告J3拆分为签名报告J2和第二摘要讯息Z2；

[0056] S23、进行第一次校验：利用Hash算法算出签名报告J2的唯一摘要讯息与第二摘要讯息Z2比对，摘要讯息全文一致为校验通过；

[0057] S24、将签名报告J2拆分为源报告J1和加密讯息Z1m；

[0058] S25、进行第二次校验：利用Hash算法算出源报告J1的唯一摘要讯息并与加密讯息Z1m解密后的摘要讯息进行全文校验，全文一致为校验通过；

[0059] 其中所述的解密过程是从数字签名模块102读出公钥，利用与生成报告时所用的非对称数据加密算法对加密讯息Z1m进行解密并输出解密后的摘要信息。

[0060] S26、进行第三次校验：从源报告J1解析出记录的单体存储设备200基本信息与当前被审计的单体存储设备200基本信息进行一致性校验，校验通过后进行下一步；

[0061] S27，最后在经过三次检验均获得通过后，对源报告J1进行最终解析，得到正确的操作人员信息、时间戳、UUID等在先记录的完整信息，完成整个防篡改报告的审计解析流程。

[0062] 对于本领域的技术人员来说，可根据以上描述的技术方案以及构思，做出其它各种相应的改变以及形变，而所有的这些改变以及形变都应该属于本发明权利要求的保护范围之内。

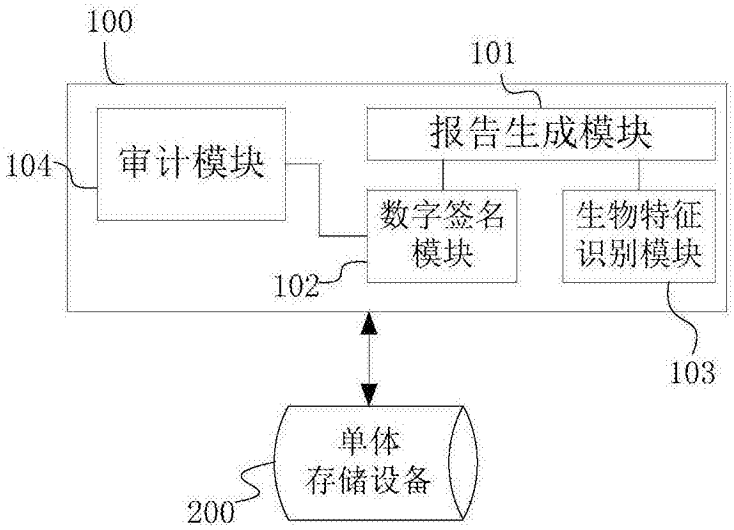

100
101
报告生成模块
104
审计模块
数字签名模块
生物特征识别模块
102
103
单体存储设备
200

图1


S11
开始，对单体存储设备进行信息消除，并收集和记录单体存储设备的信息数据
S12
生成包括了时间戳、UUID和操作人员讯息的JSON格式的源报告J1
S13
利用Hash算法对源报告J1输出唯一对应的第一摘要讯息Z1，并加密签名得到加密讯息Z1m
S14
将加密讯息Z1m写入源报告J1得到签名报告J2
S15
利用Hash算法对签名报告J2输出唯一对应的第二摘要讯息Z2
S16
将第二摘要讯息Z2写入签名报告J2得到防篡改报告J3
S17
将防篡改报告J3写入单体存储设备指定位置，结束

图2

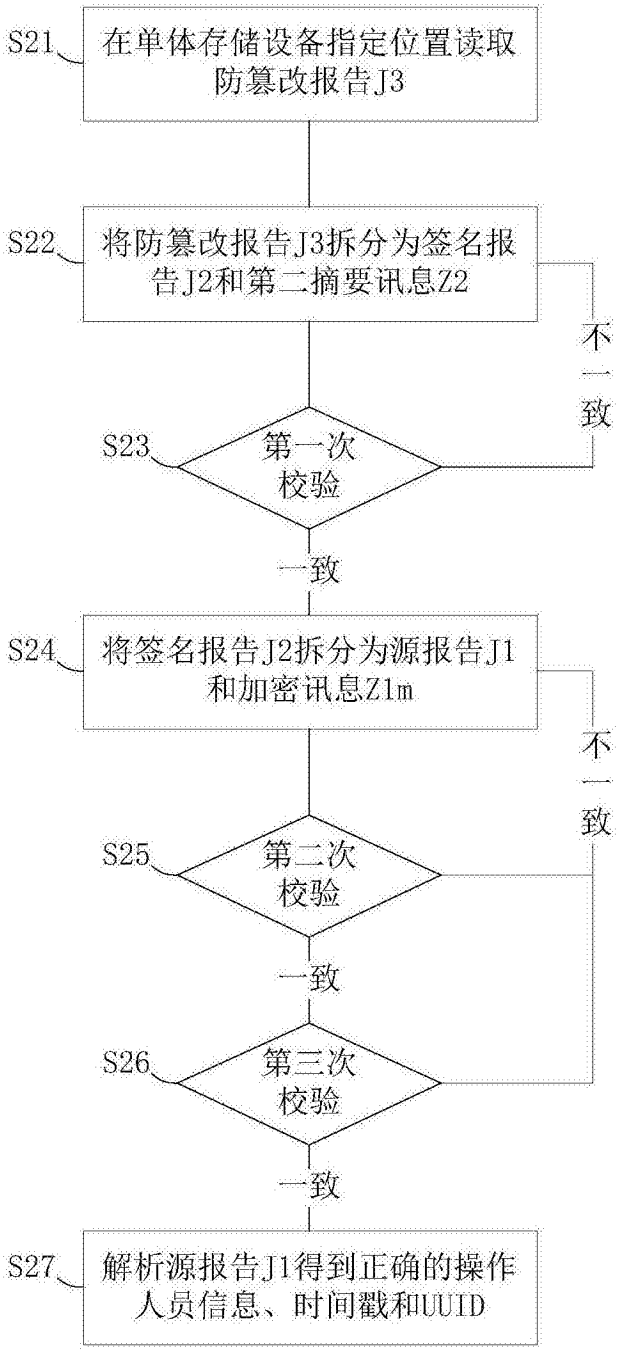

S21
在单体存储设备指定位置读取防篡改报告J3
S22
将防篡改报告J3拆分为签名报告J2和第二摘要讯息Z2
不一致
S23
第一次校验
一致
S24
将签名报告J2拆分为源报告J1和加密讯息Z1m
不一致
S25
第二次校验
一致
S26
第三次校验
一致
S27
解析源报告J1得到正确的操作人员信息、时间戳和UUID

图3