(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 110012004 A
(43)申请公布日 2019.07.12

(21)申请号 201910253632.1

(22)申请日 2019.03.30

(66)本国优先权数据
201811191841.X 2018.10.12 CN

(71)申请人 王龙
地址 652803 云南省玉溪市华宁县青龙镇大村村委会者白村73号

(72)发明人 王龙

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/14(2006.01)

权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于数据暂存技术的数据防泄漏方法

(57)摘要

本发明涉及一种基于数据暂存技术的数据防泄漏方法，提供有由若干终端连接组成的局域网络，所述局域网络配置有一中心服务器，所述中心服务器连接所述局域网络内的每一终端，每一所述终端配置有存储模块用于存储数据，所述存储模块由若干存储区间组成，具体包括以下步骤：数据处理步骤；数据配置步骤；刷新暂存步骤，以所述第一加密密文所在的终端为中继终端，包括第一暂存步骤、指针加密步骤、第二暂存步骤以及地址加密步骤。通过这样设置，在局域网内建立数据共享存储的概念，通过时变和跳动的存储方式，而保证了数据的安全性。

CN 110012004 A

1.一种基于数据暂存技术的数据防泄漏方法,其特征在于:提供有由若干终端连接组成的局域网络,所述局域网络配置有一中心服务器,所述中心服务器连接所述局域网络内的每一终端,每一所述终端配置有存储模块用于存储数据,所述存储模块由若干存储区间组成,具体包括以下步骤:

数据处理步骤,以待处理数据所在的终端为初始终端,通过第一加密算法加密带处理数据以生成第一加密密文以及该第一加密密文对应的第一密钥,进入数据配置步骤;

数据配置步骤,为所述第一加密密文配置第一刷新时间以及第二刷新时间,进入刷新暂存步骤;

刷新暂存步骤,以所述第一加密密文所在的终端为中继终端,包括第一暂存步骤、指针加密步骤、第二暂存步骤以及地址加密步骤;

第一暂存步骤,配置有第一累计时间,当第一累计时间到达第一刷新时间时,在中继终端的所述存储模块随机生成一空的存储区间以存储所述第一加密密文,并获得该存储区间的存储指针信息,所述存储指针信息指向所述存储空间,重置所述第一累计时间,进入指针加密步骤;

指针加密步骤,通过第二加密算法加密所述存储指针信息以生成指针密文信息以及对应的指针密钥,保存所述指针密钥,将所述指针密文信息发送至中心服务器;

第二暂存步骤,配置第二累计时间,当第二累计时间达到第二刷新时间时,根据中继终端的所在的路由表随机生成一目的地址,将所述第一加密密文发送至该目的地址所在的终端,并重置所述第二累计时间,进入地址加密步骤;

地址加密步骤,通过第三加密算法加密所述目的地址以生成地址密文信息以及对应的地址密钥,将所述地址密文信息发送至对应的中继终端,将地址密钥发送至对应的初始终端。

2.如权利要求1所述的一种基于数据暂存技术的数据防泄漏方法,其特征在于:所述指针加密步骤中,当所述中心服务器从同一中继终端接收到一新的指针密文信息时,删除该中继终端原有的指针密文信息。

3.如权利要求2所述的一种基于数据暂存技术的数据防泄漏方法,其特征在于:所述指针加密步骤中,当所述中继终端生成一新的指针密钥时,删除该中继终端原有的指针密钥。

4.如权利要求1所述的一种基于数据暂存技术的数据防泄漏方法,其特征在于:所述第二刷新时间的时长为第一刷新时间的时长的5-20倍。

5.如权利要求1所述的一种基于数据暂存技术的数据防泄漏方法,其特征在于:所述地址加密步骤还配置有基准迁移次数,对应一第一加密密文设置有实际迁移次数,每当执行一次所述地址加密步骤所述实际迁移次数增加一个单位,当所述实际迁移次数超过所述基准迁移次数时,将所述地址密文信息发送至发送至对应的初始终端。

6.如权利要求5所述的一种基于数据暂存技术的数据防泄漏方法,其特征在于:所述基准迁移次数设置为10次。

7.如权利要求1所述的一种基于数据暂存技术的数据防泄漏方法,其特征在于:所述第一暂存步骤还包括,当所述第一加密密文被存入所述存储区间前,通过第一暂存加密算法加密所述第一加密密文以获得第一暂存加密密文;当所述第一暂存加密密文从所述存储区间被取出前,通过第一暂存解密算法解密所述第一暂存加密密文以获得第一加密密文。

8.如权利要求7所述的一种基于数据暂存技术的数据防泄漏方法，其特征在于：所述第一暂存加密密文的数据格式与其对应的第一加密密文的数据格式相同。

9.如权利要求1所述的一种基于数据暂存技术的数据防泄漏方法，其特征在于：所述第二暂存步骤还包括，当一中继终端接收所述第一加密密文时，通过第二暂存加密算法加密所述第一加密密文以获得第二暂存加密密文；当一中继终端发送所述第二暂存加密密文时，通过第二暂存解密算法解密所述第二暂存加密密文以获得第一加密密文。

10.如权利要求9所述的一种基于数据暂存技术的数据防泄漏方法，其特征在于：所述的第二暂存加密密文与所述第一加密密文的数据格式相同。

一种基于数据暂存技术的数据防泄漏方法

技术领域

[0001] 本发明涉及数据存储方法,更具体地说,涉及一种基于数据暂存技术的数据防泄漏方法。

背景技术

[0002] 数据(Data)是对事实、概念或指令的一种表达形式,可由人工或自动化装置进行处理。数据经过解释并赋予一定的意义之后,便成为信息。数据处理(data processing)是对数据的采集、存储、检索、加工、变换和传输。

[0003] 数据处理的基本目的是从大量的、可能是杂乱无章的、难以理解的数据中抽取并推导出对于某些特定的人们来说是有价值、有意义的数据。

[0004] 数据处理是系统工程和自动控制的基本环节。数据处理贯穿于社会生产和社会生活的各个领域。数据处理技术的发展及其应用的广度和深度,极大地影响着人类社会发展的进程。

[0005] 而实际使用的过程中,由于数据的存储在一个终端,而针对终端进行数据窃取的方式较多,所以只要终端被入侵,那么非常容易造成数据的泄漏,而在数据链路层实现数据窃取的实例较多,一旦数据失窃,会对用户造成巨大的损失。

发明内容

[0006] 有鉴于此,本发明目的是提供一种基于数据暂存技术的数据防泄漏方法,以解决上述问题。

[0007] 为了解决上述技术问题,本发明的技术方案是:一种基于数据暂存技术的数据防泄漏方法,提供有由若干终端连接组成的局域网络,所述局域网络配置有一中心服务器,所述中心服务器连接所述局域网络内的每一终端,每一所述终端配置有存储模块用于存储数据,所述存储模块由若干存储区间组成,具体包括以下步骤:

数据处理步骤,以待处理数据所在的终端为初始终端,通过第一加密算法加密带处理数据以生成第一加密密文以及该第一加密密文对应的第一密钥,进入数据配置步骤;

数据配置步骤,为所述第一加密密文配置第一刷新时间以及第二刷新时间,进入刷新暂存步骤;

刷新暂存步骤,以所述第一加密密文所在的终端为中继终端,包括第一暂存步骤、指针加密步骤、第二暂存步骤以及地址加密步骤;

第一暂存步骤,配置有第一累计时间,当第一累计时间到达第一刷新时间时,在中继终端的所述存储模块随机生成一空的存储区间以存储所述第一加密密文,并获得该存储区间的存储指针信息,所述存储指针信息指向所述存储空间,重置所述第一累计时间,进入指针加密步骤;

指针加密步骤,通过第二加密算法加密所述存储指针信息以生成指针密文信息以及对应的指针密钥,保存所述指针密钥,将所述指针密文信息发送至中心服务器;

第二暂存步骤，配置第二累计时间，当第二累计时间达到第二刷新时间时，根据中继终端的所在的路由表随机生成一目的地址，将所述第一加密密文发送至该目的地址所在的终端，并重置所述第二累计时间，进入地址加密步骤；

地址加密步骤，通过第三加密算法加密所述目的地址以生成地址密文信息以及对应的地址密钥，将所述地址密文信息发送至对应的中继终端，将地址密钥发送至对应的初始终端。

[0008] 进一步地：所述指针加密步骤中，当所述中心服务器从同一中继终端接收到一新的指针密文信息时，删除该中继终端原有的指针密文信息。

[0009] 进一步地：所述指针加密步骤中，当所述中继终端生成一新的指针密钥时，删除该中继终端原有的指针密钥。

[0010] 进一步地：所述第二刷新时间的时长为第一刷新时间的时长的5-20倍。

[0011] 进一步地：所述地址加密步骤还配置有基准迁移次数，对应一第一加密密文设置有实际迁移次数，每当执行一次所述地址加密步骤所述实际迁移次数增加一个单位，当所述实际迁移次数超过所述基准迁移次数时，将所述地址密文信息发送至发送至对应的初始终端。

[0012] 进一步地：所述基准迁移次数设置为10次。

[0013] 进一步地：所述第一暂存步骤还包括，当所述第一加密密文被存入所述存储区间前，通过第一暂存加密算法加密所述第一加密密文以获得第一暂存加密密文；当所述第一暂存加密密文从所述存储区间被取出前，通过第一暂存解密算法解密所述第一暂存加密密文以获得第一加密密文。

[0014] 进一步地：所述第一暂存加密密文的数据格式与其对应的第一加密密文的数据格式相同。

[0015] 进一步地：所述第二暂存步骤还包括，当一中继终端接收所述第一加密密文时，通过第二暂存加密算法加密所述第一加密密文以获得第二暂存加密密文；当一中继终端发送所述第二暂存加密密文时，通过第二暂存解密算法解密所述第二暂存加密密文以获得第一加密密文。

[0016] 进一步地：所述的第二暂存加密密文与所述第一加密密文的数据格式相同。

[0017] 本发明技术效果主要体现在以下方面：通过这样设置，在局域网内建立数据共享存储的概念，通过时变和跳动的存储方式，而保证了数据的安全性。

附图说明

[0018] 图1：本发明的基于数据暂存技术的数据防泄漏方法的步骤逻辑图；

图2：本发明的基于数据暂存技术的数据防泄漏方法的系统架构原理图；

图3：本发明的基于数据暂存技术的数据防泄漏方法的刷新暂存步骤逻辑图；

附图标记：1、初始终端；2、中继终端；3、中心服务器；10、存储模块；110、存储区间；a1、数据处理步骤；a2、数据配置步骤；a3、刷新暂存步骤；a31、第一暂存步骤；a32、指针加密步骤；a33、第二暂存步骤；a34、地址加密步骤。

具体实施方式

[0019] 以下结合附图，对本发明的具体实施方式作进一步详述，以使本发明技术方案更易于理解和掌握。

[0020] 参照图1所示，一种基于数据暂存技术的数据防泄漏方法，提供有由若干终端连接组成的局域网络，所述局域网络配置有一中心服务器3，所述中心服务器3连接所述局域网络内的每一终端，每一所述终端配置有存储模块10用于存储数据，所述存储模块10由若干存储区间110组成，首先本发明用于局域网内的数据存储，而数据存储包括两个位置，一个是数据位于的终端的位置，另一个是数据位于哪一存储区间110的位置，而需要说明的是，首先需要从终端中划分出一个独立的存储模块10，而将存储模块10划分为若干个存储区间110，存储区间110大小相同，而同样的需要保证每个待加密数据的大小小于存储空间的容量。具体包括以下步骤：

数据处理步骤a1，以待处理数据所在的终端为初始终端1，通过第一加密算法加密带处理数据以生成第一加密密文以及该第一加密密文对应的第一密钥，进入数据配置步骤a2；首先是对数据进行处理，就可以得到加密后的数据，而第一加密密文仅可以通过初始终端1才能解密，也就是说，无论第一加密密文被发送到什么位置，其使用权还是属于初始终端1，这样就可以防止数据泄露。

[0021] 数据配置步骤a2，为所述第一加密密文配置第一刷新时间以及第二刷新时间，进入刷新暂存步骤a3；而后对应每一个第一加密密文配置第一刷新时间和第二刷新时间，所述第二刷新时间的时长为第一刷新时间的时长的5-20倍。

[0022] 刷新暂存步骤a3，以所述第一加密密文所在的终端为中继终端2，包括第一暂存步骤a31、指针加密步骤a32、第二暂存步骤a33以及地址加密步骤a34；作为本发明的核心步骤，进行详述，对应一个加密密文而言，定义其所在的终端为中继终端2，例如此时中继终端2B接收到该加密密文。需要说明的是，刷新暂存步骤a3对应一个第一加密密文而言是不断重复进行执行，根据时间实际的时间进行触发，而不是根据步骤顺序触发。

[0023] 第一暂存步骤a31，配置有第一累计时间，当第一累计时间到达第一刷新时间时，在中继终端2的所述存储模块10随机生成一空的存储区间110以存储所述第一加密密文，并获得该存储区间110的存储指针信息，所述存储指针信息指向所述存储空间，重置所述第一累计时间，进入指针加密步骤a32；累计时间根据实际时间获得，可以以中继终端2接收到第一加密密文为初始时间，而例如第一刷新时间设置为60秒，也就是说，每隔60秒则为第一加密密文换一个存储空间，在另一个实施例中，当所述第一加密密文被存入所述存储区间110前，通过第一暂存加密算法加密所述第一加密密文以获得第一暂存加密密文；当所述第一暂存加密密文从所述存储区间110被取出前，通过第一暂存解密算法解密所述第一暂存加密密文以获得第一加密密文。也就是每次存入和取出分别进行一次加密和解密步骤，提高数据安全性，而存储指针信息是唯一可以获取到存储区间110的位置的信息，所以只要初始终端1获取到中继终端2的地址以及获取到存储指针信息的位置就可以获得第一加密密文，从而进行使用。所述第一暂存加密密文的数据格式与其对应的第一加密密文的数据格式相同。

[0024] 指针加密步骤a32，通过第二加密算法加密所述存储指针信息以生成指针密文信息以及对应的指针密钥，保存所述指针密钥，将所述指针密文信息发送至中心服务器3；而

指针加密步骤a32是通过第二加密算法对存储指针信息进行加密，这样一来，这个位置信息需要通过指针密钥才能进行获取。而所以如果初始终端1需要获取存储指针信息，就需要得到指针密文信息以及对应的指针密钥，而指针密文信息在中心服务器3进行统一管理，每一中继终端2不保留指针密文信息，而指针密钥则在对应的中继终端2保存，这样一来，初始终端1需要发送请求到中心服务器3，中心服务器3接收请求后找到对应的中继终端2，获取对应的指针密钥，获得存储指针信息，这样初始终端1才能完成第一加密密文的获取，更加安全可靠。所述指针加密步骤a32中，当所述中心服务器3从同一中继终端2接收到一新的指针密文信息时，删除该中继终端2原有的指针密文信息。所述指针加密步骤a32中，当所述中继终端2生成一新的指针密钥时，删除该中继终端2原有的指针密钥。

[0025] 第二暂存步骤a33，配置第二累计时间，当第二累计时间达到第二刷新时间时，根据中继终端2的所在的路由表随机生成一目的地址，将所述第一加密密文发送至该目的地址所在的终端，并重置所述第二累计时间，进入地址加密步骤a34；而这个步骤是为了将数据发出，所以通过配置第二累计时间，第二累计时间根据实际时间累计，例如设置为5分钟，当时间达到5分钟时，就可以发送到下一终端，而目的地址是根据该中继终端2路由表随机生成，不具有规律性，无法追踪。所述第二暂存步骤a33还包括，当一中继终端2接收所述第一加密密文时，通过第二暂存加密算法加密所述第一加密密文以获得第二暂存加密密文；当一中继终端2发送所述第二暂存加密密文时，通过第二暂存解密算法解密所述第二暂存加密密文以获得第一加密密文。所述的第二暂存加密密文与所述第一加密密文的数据格式相同。这样一来，提高可靠性和安全性。

[0026] 地址加密步骤a34，通过第三加密算法加密所述目的地址以生成地址密文信息以及对应的地址密钥，将所述地址密文信息发送至对应的中继终端2，将地址密钥发送至对应的初始终端1。地址加密步骤a34的设置，目的是为了加密地址，而地址密钥是发送到初始终端1的，地址密文信息发送到对应的中继终端2，也就是说，对应一个数据X，经过A-B-C-D-E终端，初始终端1A仅具有B的地址密文信息，但是初始终端1具有所有的地址密钥，所以就可以获得B的地址，而B具有C的地址密文信息，而根据B反馈得到C的地址，从而依次直至得到该第一加密数据的位置，向中心服务器3发送请求并获得对应的指针存储信息，以获得对应的第一加密数据。在另一个实施例中，所述地址加密步骤a34还配置有基准迁移次数，对应一第一加密密文设置有实际迁移次数，每当执行一次所述地址加密步骤a34所述实际迁移次数增加一个单位，当所述实际迁移次数超过所述基准迁移次数时，将所述地址密文信息发送至发送至对应的初始终端1。而需要说明的是，如果不断重复进行数据发送，那长时间形成的数据发送距离增加，而调用数据效率降低，所以配置一个次数值，例如所述基准迁移次数设置为10次。而当10次发送以后，初始终端1就可以得到目前的位置，也就是说以前的地址密钥以及地址密文信息就无效了，减少数据量。

[0027] 当然，以上只是本发明的典型实例，除此之外，本发明还可以有其它多种具体实施方式，凡采用等同替换或等效变换形成的技术方案，均落在本发明要求保护的范围之内。

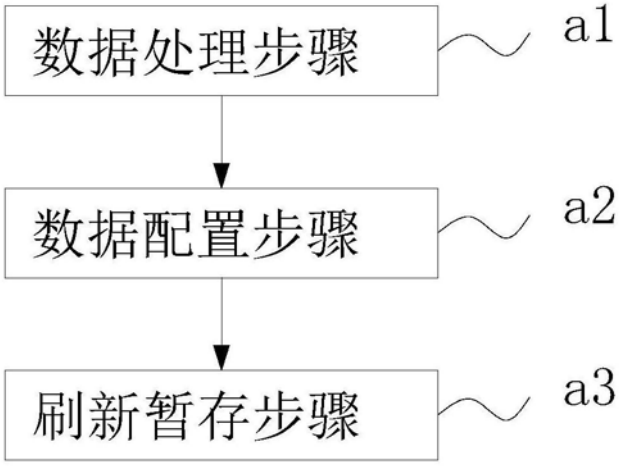
数据处理步骤
a1
数据配置步骤
a2
刷新暂存步骤
a3

图1

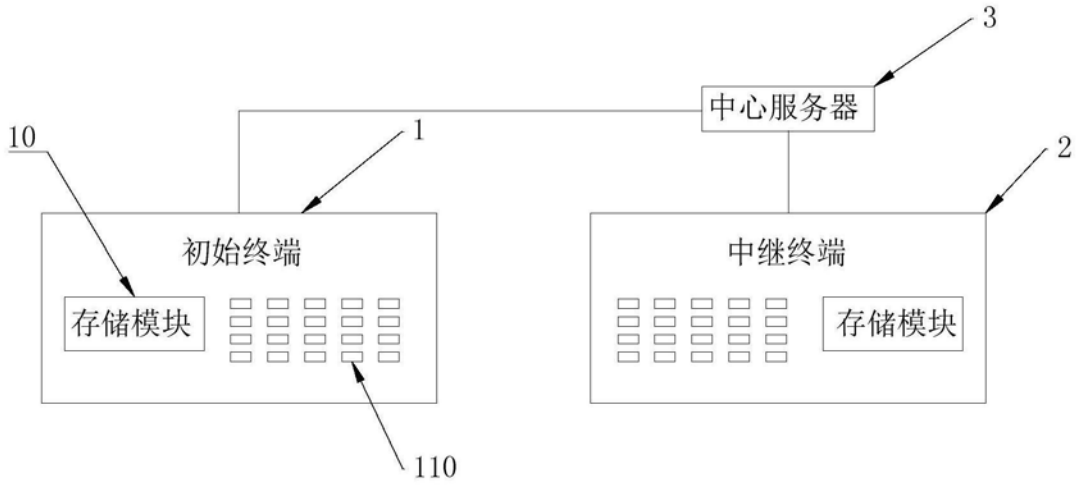
3
中心服务器
10
1
2
初始终端
存储模块
中继终端
存储模块
110

图2

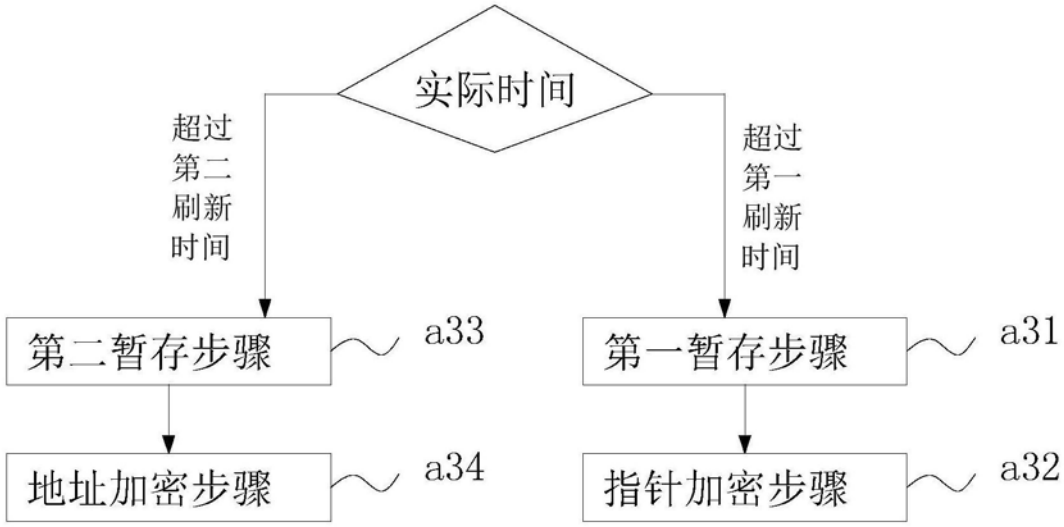
实际时间
超过第二刷新时间
超过第一刷新时间
第二暂存步骤
a33
第一暂存步骤
a31
地址加密步骤
a34
指针加密步骤
a32

图3