(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 11 月 16 日 (16.11.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/193750 A1

(51) 国际专利分类号:
G06F 21/55 (2013.01)

(21) 国际申请号: PCT/CN2017/080006

(22) 国际申请日: 2017 年 4 月 11 日 (11.04.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610318168.6 2016年5月13日 (13.05.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人; 及

(71) 申请人 (仅对 *US*): 李小峰 (LI, Xiaofeng) [CN/CN]; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲2号渔阳置业大厦B座605, Beijing 100029 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY,

WO 2017/193750 A1

(54) **Title:** PROCESSING METHOD FOR PRESENTING COPY ATTACK, AND SERVER AND CLIENT

(54) **发明名称:** 一种防止拷贝攻击的处理方法、服务器及客户端

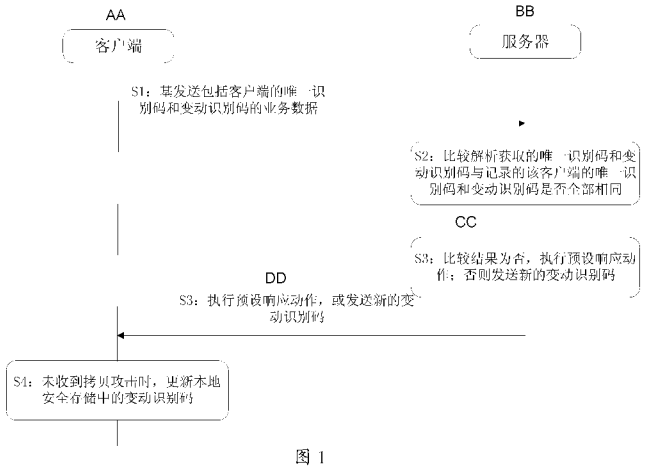

图 1

S1 Sending service data comprising a unique identification code and a variable identification code of a client to a server
S2 Comparing whether the unique identification code and the variable identification code which are acquired by means of parsing are completely the same as a recorded unique identification code and variable identification code of the client
S4 When no copy attack is received, updating the variable identification code in local secure storage
AA Client
BB Server
CC If the comparison result is not the same, executing a pre-set response action; otherwise, sending a new variable identification code
DD Executing a pre-set response action, or sending a new variable identification code

(57) **Abstract:** A processing method for presenting a copy attack, and a server and a client. The method comprises: a client sending service data comprising a unique identification code and a variable identification code of the client to a server (S1); the server comparing whether the unique identification code and the variable identification code which are acquired by means of parsing are completely the same as a unique identification code and a variable identification code of the client which are recorded by the server (S2); if the comparison result is not the same, then the server determining that local secure storage of the client is suffering from a copy attack and

[见续页]

MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：
— 包括国际检索报告(条约第21条(3))。

executing a pre-set response action; otherwise, the server sending a new variable identification code to the client (S3); and the client updating the received new variable identification code to the local secure storage (S4). By means of the method, the difficulty in copy attacks can be increased, and the harmfulness from the implementation of copy attacks can be reduced, thereby increasing the security of application data storage in a terminal device, reducing the loss of the user property, and protecting the security of the user property.

(57) 摘要：一种防止拷贝攻击的处理方法、服务器及客户端。所述方法包括：客户端向服务器发送包括客户端的唯一识别码和变动识别码的业务数据（S1）；服务器比较解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码是否全部相同（S2）；若所述比较结果为否，则所述服务器判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，所述服务器向所述客户端发送新的变动识别码（S3）；所述客户端将接收到的新的变动识别码更新至所述本地安全存储中（S4）。利用所述方法，可以加大拷贝攻击难度，降低拷贝攻击实施的危害性，提高终端设备中应用数据存储的安全性，降低用户财产损失，保护用户财产安全。

一种防止拷贝攻击的处理方法、服务器及客户端

技术领域

本申请属于安全认证信息数据处理技术领域，尤其涉及一种防止拷贝攻击的处理方法、服务器及客户端。

背景技术

随着互联网和信息技术的迅速发展，在日常生活中，人们对手机、平板等移动终端设备的依赖性越来越强。用户的移动终端中常常安装有与用户财产相关的APP，如手机钱包、手机银行、投资或理财应用等，如何降低用户终端设备被黑客攻破而导致用户财产损失、有效提高用户财产安全性已成为目前终端信息安全的一项重要课题。

目前移动终端的APP对数据安全存储方式通常采用软安全存储。所述的软安全存储通常是指为运行在设备系统上的一个软件，如运行在Android上的一个APP，通过增加反破解的手段来提供数据本地安全存储的安全性，黑客一般很难破解该软件存储的数据和算法。但正因如此，目前黑客很容易想到采用拷贝攻击的方式进行攻击，即黑客将用户的数据和环境拷贝过来，直接模拟用户设备，就可以很容易用设备上用户的数据来伪造用户，从而能够窃取用户的信息。通过拷贝攻击，黑客能够直接在黑客的机器上运行用户的账户，而不用去强力破解软件内部的数据和算法。而目前防止拷贝攻击的方式，都是和用户设备的信息进行绑定，如果判断不是原先绑定的设备，就认为不安全。但现有的这种方式可以很容易被黑客攻破，因为这些设备环境信息都是通过系统的api去获取的，黑客可以采用更为精密的算法通过hook（钩子）调用到系统的api，来获取设备环境信息，利用这些api从而模拟设备信息，让软件误以为是原先绑定的设备，从而攻破设备

绑定这一层保护，达到可以进入用户账户的目的。

因此，现有技术中客户端单一的数据软安全存储的安全性仍然较低，难以防止拷贝攻击，用户绑定的设备信息通常是内置固有的，攻击者（如黑客）一旦实施拷贝攻击成功，将会对用户造成难以估计的损失。

发明内容

本申请目的在于提供一种防止拷贝攻击的处理方法、服务器及客户端，可以加大拷贝攻击难度，降低拷贝攻击实施的危害性，提高终端设备中应用数据存储的安全性，降低用户财产损失，保护用户财产安全。

本申请提供的一种防止拷贝攻击的处理方法、服务器及客户端是这样实现的:

一种防止拷贝攻击的处理方法，所述方法包括:

客户端向服务器发送业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

所述服务器解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码是否全部相同;

若所述比较结果为否，则所述服务器判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，所述服务器向所述客户端发送新的变动识别码;

所述客户端将接收到的新的变动识别码更新至所述本地安全存储中。

一种防止拷贝攻击的处理方法，所述方法包括:

接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较

解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同;

若所述比较结果为否，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，向所述客户端发送新的变动识别码。

一种防止拷贝攻击的处理方法，所述方法包括:

在本地安全存储初始化时存储由服务器发送来的唯一识别码和变动识别码;

向服务器发送业务数据，所述业务数据包括本地安全存储的唯一识别码和变动识别码;

接收服务器发送的新的变动识别码，所述新的变动识别码为服务器比较客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码为全部相同时发送的变动识别码;

将接收到的所述新的变动识别码更新至所述本地安全存储中。

一种防止拷贝攻击的服务器，所述服务器包括:

数据接收模块，用于接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

比较模块，用于解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同;

处理模块，用于若所述比较模块的比较结果为否时，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，向所述客户端发送新的变动识别码。

一种防止拷贝攻击的客户端，所述客户端包括:

安全存储模块，用于在本地安全存储初始化时存储由服务器发送来的

唯一识别码和变动识别码;

数据发送模块，用于向服务器发送业务数据，所述业务数据包括所述安全存储模块存储的唯一识别码和变动识别码;

第一接收模块，用于接收服务器发送的新的变动识别码，所述新的变动识别码为服务器比较客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码为全部相同时发送的变动识别码;

更新模块，用于将接收到的所述新的变动识别码更新至所述本地安全存储中。

本申请提供的一种防止拷贝攻击的处理方法、服务器及客户端，可以在防止攻击者拷贝攻击常规的设备绑定之外，还采用了远程服务器端进行判断，识别验证客户端中应用的本地安全存储是否经过拷贝攻击。在真实的使用环境中，一般攻击者通过拿到设备数据并且部署环境进行攻击通常是滞后于用户再次使用终端应用的，本申请提供的实施方案通过设置存储的数据的时效性来保障攻击者拷贝攻击窃取的信息数据很容易过时，并且由服务器端来判断是否进行拷贝攻击，而服务器端通常数据的存储和计算安全性大于客户端一侧，攻击者很难绕过服务器端验证这一层防护。这样，可以加大拷贝攻击难度，整体降低拷贝攻击实施的危害性，提高终端设备中应用数据存储的安全性，降低用户财产损失，保护用户财产安全。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得

其他的附图。

图1是本申请提供的一种防止拷贝攻击的处理方法一种实施例的方法流程图;

图2是本申请实施方案中客户端软安全存储初始化的一种应用场景示意图;

图3是本申请提供的一种防止拷贝攻击的处理方法另一种实施例的方法流程图;

图4是本申请提供的一种防止拷贝攻击的处理方法另一种实施例的方法流程图;

图5是本申请提供的一种防止拷贝攻击的服务器一种实施例的模块结构示意图;

图6是本申请提供的一种防止拷贝攻击的服务器另一种实施例的模块结构示意图;

图7是本申请提供的一种防止拷贝攻击的客户端一种实施例的模块结构示意图;

图8是本申请提供的一种防止拷贝攻击的客户端另一种实施例的模块结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

图 1 是本申请所述一种防止拷贝攻击的处理方法一种实施例的方法流

程图。虽然本申请提供了如下述实施例或附图所示的方法操作步骤或装置结构，但基于常规或者无需创造性的劳动在所述方法或装置中可以包括更多或者更少的操作步骤或模块结构。在逻辑性上不存在必要因果关系的步骤或结构中，这些步骤的执行顺序或装置的模块结构不限于本申请实施例提供的执行顺序或模块结构。所述的方法或模块结构的在实际中的装置或终端产品应用时，可以按照实施例或者附图所示的方法或模块结构进行顺序执行或者并行执行（例如并行处理器或者多线程处理甚至分布式处理的环境）。

具体的如图 1 所述，本申请一种实施例提供的一种防止拷贝攻击的处理方法可以包括:

S1：客户端向服务器发送业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码。

客户端在与服务器进行信息交互，向服务器发送业务数据时，可以同时将客户端本地安全存储的唯一识别码和变动识别码一起发送给服务器。所述的客户端本地安全存储可以包括客户端中某个应用软安全存储，一般的客户端中安装的应用进行本地安全存储初始化时可以向服务器申请用于识别该客户端的唯一识别码和此次初始化的变动随机码。一般的，所述唯一识别码用户标记客户端身份，通常情况下在判断客户端未受到拷贝攻击时可以不发生变化，而所述变动随机码可以设置为在每一次客户端触发使用本地安全存储相关的业务时均会更新变化。本申请中所述的唯一识别码和变动随机码具体的数据格式可以根据实际的应用场景进行设计，例如本实施例中所述唯一识别码可以包括根据客户端设备信息演化生成的唯一 ID，所述的变动识别码可以为服务器每次随机生成的随机数，如 6 位数字或者字母、符合组合等。

本申请所述方法的另一种实施例中，所述客户端发送给服务器的唯一

识别码和变动识别码可以经过加密处理，这样可以进一步增强数据存储安全性，提高数据破解难度，如数据通信过程可以采用公钥和私钥的 RSA 非对称加密、AES 对称加密等。当然，服务器下发给客户端的唯一识别码或者变动识别码也可以采用对称或非对称加密，提高客户端与服务器之间通信的安全性。因此，本申请所述防止拷贝攻击的处理方法的另一种实施例中，所述客户端与服务器之间所述唯一识别和变动识别码的信息交互可以采用使用非对称加密、对称加密中的任意一种加密方式实现。

当然，客户端在接收服务器发送的唯一识别码或变动识别码时可以采用相应的解密算法进行解码，获取唯一识别码或变动识别码后进行本地安全存储。图 2 是本申请实施方案中客户端软安全存储初始化的一种应用场景示意图。在图 2 中，客户端软安全存储初始化时向服务器一侧的安全服务申请唯一 ID 和初始化随机数，服务器生成该客户端的唯一 ID 和初始化随机数，加密后下发给客户端。客户端解密后安全保持唯一 ID 和初始化随机数。

需要说明的是，本实施例中所述的业务数据包括客户端本地安全存储的服务器发送所述给客户端的唯一识别码和变动识别码具体的实施场景可以包括将客户端触发的包括业务数据、唯一识别码、变动识别码等的信息作为此次发送给服务器的一个整体业务数据，如新增业务数据的某些字段，这些字段包括所述唯一识别码和变动识别码，或者，其他的应用场景中也可以包括将业务数据唯一识别码、变动识别码分别作为单独的数据，此次将这三个数据一起发送给服务器。当然，所述的业务数据也可以是具体的业务操作，也可以为客户端的验证请求之类的消息信息。因此，一定程度上可以理解为客户端向服务器发送的消息中包含了客户的唯一识别码和变动识别码，对具体的实现方式不做限定。

本申请实施例中，使用客户端本地安全存储相关的业务向服务器发送

业务数据时，所述的业务数据可以包括客户端本地安全存储的服务器发送给所述客户端的唯一识别码和变动识别码。

S2：所述服务器解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码是否全部相同。

本实施例中，所述服务器接收到客户端发送的业务数据后，可以解析所述业务数据，获取客户端上传来的业务数据中的唯一识别码和变动识别码。由于服务器预先存储了分配给客户端的唯一识别码和上次的变动识别码，因此，所述服务器可以比较解析获取的唯一识别码和变动识别码与服务器存储记录的该客户端的唯一识别码和变动识别码是否全部相同。当然，如前所述，如果客户端上传来的唯一识别码和变动识别码是经过加密处理的，则服务器一侧相应的采用域加密处理对应的解密方式进行解密处理后获取唯一识别码和变动识别码。

所述服务器接收客户端发送的业务数据，获取客户端的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码是否全部相同。

S3：若所述比较结果为否，则所述服务器判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，所述服务器向所述客户端发送新的变动识别码。

服务器对解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码进行比较，如果比较结果为其中有至少一项不相同，则可以表示发送该业务数据的客户端未存在异常，尤其是变动识别码，如本实施例中的随机数不相同时，表明该客户端应用相应的软安全存储很有可能是经过拷贝攻击并运行该应用，触发到了软安全存储的相

关业务。因此，本申请实施例，服务器基于对解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码的比较结果为否，可以判断客户端的本地安全存储受到拷贝攻击，进一步的可以做出预先设置的响应动作，具体的响应动作可以根据实际情况预先进行设定，如强迫下线、禁止用户账户资金操作、密保验证等等。

当然，如果服务器比较解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码全部相同，则可以认为发送该业务请求的客户端为用户真实的客户端，可以允许业务接入，进一步进行操作，然后，所述服务器可以为该客户端生成一个新的变动识别码，然后将所述新的变动识别码发送给客户端。如本实施例中服务器判断客户上传来的唯一 ID 和随机数与存储记录的该客户端的唯一 ID 和上一次发送的随机数一致，则客户端的身份认证通过，则服务器此时再生成一个新的随机数发送给客户端。

S4：所述客户端将接收到的新的变动识别码更新至所述本地安全存储中。

如前所述，服务器在判断客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码全部相同时会向客户端发送一个新的变动识别码，客户端可将新的变动识别码更新至客户端本地安全存储中，以供下一次发送业务数据时使用。

本申请提供的一种防止拷贝攻击的处理方，可以在防止攻击者拷贝攻击常规的设备绑定之外，还采用了远程服务器端进行判断，识别验证客户端中应用的本地安全存储是否经过拷贝攻击。在真实的使用环境中，一般攻击者通过拿到设备数据并且部署环境进行攻击通常是滞后于用户再次使用终端应用的，本申请提供的实施方案通过设置存储的数据的时效性来

保障攻击者拷贝攻击窃取的信息数据很容易过时，并且由服务器端来判断是否进行拷贝攻击，而服务器端通常数据的存储和计算安全性大于客户端一侧，攻击者很难绕过服务器端验证这一层防护。这样，可以加大拷贝攻击难度，整体降低拷贝攻击实施的危害性，提高终端设备中应用数据存储的安全性，降低用户财产损失，保护用户财产安全。

当然，如前所述，如果所述比较结果为否，即服务器对解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码的比较结果为其中至少一项不相同，可以认为客户端的本地安全存储受到拷贝攻击，进一步的可以做出响应动作。本申请具体的响应动作可以根据实际情况进行设定，如强迫下线、禁止用户账户资金操作、密保验证等等。本申请所述方法提供一种在判断客户端的本地安全存储为受到拷贝攻击时的处理方法，具体的，本申请所述一种防止拷贝攻击的处理方法的另一种实施例中，所述预设响应动作可以包括:

S301: 所述服务器下发要求所述业务数据对应的用户进行身份验证的消息，并在身份验证通过后向用户的客户端发送重新分配的唯一识别码和变动识别码。

相应的，所述用户的客户端基于接收到的身份验证消息进行身份验证，如密码登录、指纹登录、人脸登录等。用户在自己的客户端上身份验证通过后，则可以根据接收到的服务器为所述用户的客户端重新分配的唯一识别码和变动识别码初始化本地安全存储。

本申请中所述的变动识别码可以采用数据、字母、符合等的一种或多种组合。具体的本申请提供的一种变动识别码的实施方式中，可以采用整数一直累加的方式来实现变动识别码（如随机整数）的时效性。因此，本申请所述方法的一种实施例中，所述变动识别码被设置成采用整数逐次累

加的方式生成。

具体的应用场景中，所述客户端 C1 变动识别码采用初始化随机 6 位整数 013579，每次安全存储的业务触发更新变动识别码时都会在上一次的变动识别码数值上累加 1 生成，如在初始化变动识别码 013579 服务器下一次生成要发给客户端 C1 的变动识别码为 013580，再下一次为 013581，以此类推。当然，服务器可以为不同的客户端随机生成不同的初始化随机 6 位整数。

上述所述的防止拷贝攻击的处理方法可以应用于安全认证的服务器一侧，通过给数据设置时效性来保证黑客窃取的数据很容易过时的，并且由服务器端判断客户端是否被拷贝攻击，以达到增加拷贝攻击难度，降低拷贝攻击危害，提高客户端应用数据安全存储的目的。因此，本申请基于上述所述还提供一种可以应用服务器一侧的防止拷贝攻击的处理方法，具体的，所述方法可以包括：

S201：接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码；

S202：解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同；

S203：若所述比较结果为否，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，向所述客户端发送新的变动识别码。

图 3 是本申请提供的一种防止拷贝攻击的处理方法一种实施例的方法流程图。具体的应用场景中，用户在使用软安全存储相关的业务过程中，客户端都会将软安全存储中的唯一 id 和随机数加密和业务数据一起发送给服务端，服务端解密唯一 id 和随机数，和服务端保存的唯一 id 和随机

数一致，则说明该软安全存储没有被拷贝过，则更新一个新的随机数给该软安全存储，软安全存储更新本地的随机数。

另一种具体的应用场景中，如果服务器发现客户端上传上来的随机数和服务端记录的不同，则可以表示该软安全存储是经过拷贝攻击，并运行过。这样服务器就可以重新让该账户的用户进行身份验证并初始化。因此，本申请所述方法的另一种实施例中，服务器判断客户端的本地安全存储为受到拷贝攻击时，所述预设响应动作可以包括:

下发要求所述业务数据对应的用户进行身份验证的消息，并在身份验证通过后向用户的客户端发送重新分配的唯一识别码和变动识别码。

当然，所述变动识别码也可以被设置成采用整数逐次累加的方式生成，以及其他的实施例中客户端与服务器之间所述唯一识别和变动识别码的信息交互采用使用非对称加密、对称加密中的任意一种加密方式实现。具体的数据设置、生成、交互方式可以参照本申请其他实施例所述，在此不做赘述。

本申请提供一种可以应用服务器一侧的防止拷贝攻击的处理方法，可以实现服务器一侧验证客户端是否经过拷贝攻击，在根据判断结果执行相应的东西，最大化的是黑客窃取的用户数据容易过时，进而提高客户端的数据存储的安全性，提供一种可以防止拷贝攻击、降低拷贝攻击对用户造成的损失的处理方法。

当前，本申请上述所述防止拷贝攻击的处理方法可以适用于客户端一侧，由客户端本地安全存储服务器为客户端配置的唯一识别码和每次业务操作都会更新的变动识别码。在客户端与服务器进行交互时，客户端将本地识别码和变动识别码一同发给服务器，由然后根据服务器的判断结果相应的执行本地操作，如账户身份验证、软安全存储初始化、更新随机数等。

具体的，本申请提供一种可以用于客户端一侧的防止拷贝攻击的处理方法，所述方法可以包括:

S301: 在本地安全存储初始化时存储由服务器发送来的唯一识别码和变动识别码;

S302: 向服务器发送业务数据，所述业务数据包括本地安全存储的唯一识别码和变动识别码;

S303: 接收服务器发送的新的变动识别码，所述新的变动识别码为服务器比较客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码为全部相同时发送的变动识别码;

S304: 将接收到的所述新的变动识别码更新至所述本地安全存储中。

图 4 是本申请提供的一种防止拷贝攻击的处理方法另一种实施例的方法流程图。当然，其他的实施例中，上述所述可以用于客户端一侧的防止拷贝攻击的处理方法所述方法还包括:

基于接收到的身份验证消息进行身份验证; 并在所述身份验证通过后，根据接收到的服务器重新分配的唯一识别码和变动识别码初始化本地安全存储。

上述各个实施例提供的客户端、服务器以及双方交互的防止拷贝攻击的处理方法，可以在防止攻击者拷贝攻击常规的设备绑定之外，还采用了远程服务器端进行判断，识别验证客户端中应用的本地安全存储是否经过拷贝攻击。在真实的使用环境中，一般攻击者通过拿到设备数据并且部署环境进行攻击通常是滞后于用户再次使用终端应用的，本申请提供的实施方案通过设置存储的数据的时效性来保障攻击者拷贝攻击窃取的信息数据很容易过时，并且由服务器端来判断是否进行拷贝攻击，而服务器端通常数据的存储和计算安全性大于客户端一侧，攻击者很难绕过服务器端验证这一层防护。这样，可以加大拷贝攻击难度，整体降低拷贝攻击实施的

危害性，提高终端设备中应用数据存储的安全性，降低用户财产损失，保护用户财产安全。

基于上述实施例所述的防止拷贝攻击的处理方法，本申请还提供一种防止拷贝攻击的处理装置，所述装置可以用于客户端应用安全服务的服务器及系统中。图 5 是本申请提供的一种防止拷贝攻击的服务器一种实施例的模块结构示意图，如图 5 所示，所述服务器可以包括:

数据接收模块 101，可以用于接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

比较模块 102，可以用于解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同;

处理模块 103，可以用于若所述比较模块 102 的比较结果为否时，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作; 否则，向所述客户端发送新的变动识别码。

所述的预设响应动作可以根据具体的应用场景进行设定。本申请提供的一种实施例中，若判断客户端的本地安全存储为受到拷贝攻击，则可以让用户重新进行身份验证，并初始化本地安全存储。图 6 是本申请提供的一种防止拷贝攻击的处理服务器另一种实施例的模块结构示意图，如图 6 所示，所述处理模块 103 可以包括:

第一处理模块 1031，可以用于在判断客户端的本地安全存储为受到拷贝攻击时下发要求所述业务数据对应的用户进行身份验证的消息，并在身份验证通过后向用户的客户端发送重新分配的唯一识别码和变动识别码;

第二处理模块 1032，可以用于在判断客户端的本地安全存储为未受到

拷贝攻击时所述服务器向所述客户端发送新的变动识别码。

如前所述，本申请所述装置的另一种实施例中，所述变动识别码被设置成采用整数逐次累加的方式生成。以及，客户端与服务器之间所述唯一识别和变动识别码的信息交互采用使用非对称加密、对称加密中的任意一种加密方式实现。具体的可以参考本申请其他实施例相关描述，在此不做赘述。

上述所述的防止拷贝攻击的处理服务器可以识别验证客户端中应用的本地安全存储是否经过拷贝攻击。在真实的使用环境中，一般攻击者通过拿到设备数据并且部署环境进行攻击通常是滞后于用户再次使用终端应用的，本申请提供的实施方案通过设置存储的数据的时效性来保障攻击者拷贝攻击窃取的信息数据很容易过时，并且由服务器端来判断是否进行拷贝攻击，而服务器端通常数据的存储和计算安全性大于客户端一侧，攻击者很难绕过服务器端验证这一层防护。这样，可以加大拷贝攻击难度，整体降低拷贝攻击实施的危害性，提高终端设备中应用数据存储的安全性，降低用户财产损失，保护用户财产安全。

本申请还提供一种防止拷贝攻击的客户端，可以基于服务器分配的唯一识别码和变动识别码与服务器进行信息交互的过程中验证失败客户端的本地安全存储是否受到拷贝攻击，通过变更随机数等方式使黑客拷贝攻击窃取的数据很容易过时，并且在服务器端实现判断客户端是否拷贝攻击的验证，达到有效保护客户端本地安全存储的数据，提高数据存储的安全性，增加拷贝攻击难度。图 7 是本申请提供的一种防止拷贝攻击的客户端一种实施例的模块结构示意图，如图 7 所示，所述客户端可以包括:

安全存储模块 201，可以用于在本地安全存储初始化时存储由服务器发送来的唯一识别码和变动识别码;

数据发送模块 202，可以用于向服务器发送业务数据，所述业务数据包括所述安全存储模块 201 存储的唯一识别码和变动识别码；

第一接收模块 203，可以用于接收服务器发送的新的变动识别码，所述新的变动识别码为服务器比较客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码为全部相同时发送的变动识别码；

更新模块 204，可以用于将接收到的所述新的变动识别码更新至所述本地安全存储中。

图 8 是本申请提供的一种防止拷贝攻击的客户端另一种实施例的模块结构示意图，如图 8 所示，所述客户端还可以包括：

第二接收模块 2051，可以用于接收服务器发的身份验证消息，和在身份验证通过后服务器发送的重新分配的唯一识别码和变动识别码；

验证处理模块 2052，可以用于基于接收到的身份验证消息进行身份验证；并在所述身份验证通过后，根据接收到的服务器重新分配的唯一识别码和变动识别码初始化本地安全存储。

本申请提供的防止拷贝攻击的客户端，可以基于服务器分配的唯一识别码和变动识别码与服务器进行信息交互的过程中验证失败客户端的本地安全存储是否受到拷贝攻击，通过变更随机数等方式使黑客拷贝攻击窃取的数据很容易过时，并且在服务器端实现拷贝攻击验证，达到有效保护客户端本地安全存储的数据，提高数据存储的安全性。

上述实施例所述的方法或服务器、客户端，可以通过在 TEE（可信执行环境）中实现安全存储，效果较好。当然，在采用其他执行环境，比如 android 系统环境，可以使用 c/c++等语言，通过混淆插花等技术，配合虚拟机技术实现安全存储，来达到提高软安全存储的安全性的目的。

尽管本申请内容中提到数据的本地安全存储、变动识别码的数据格式、加密解密处理、信息数据的发送接收的等之类的数据存储、设置、信息交互方式的描述，但是，本申请并不局限于必须是符合行业处理标准、规范或实施例所描述的情况。某些行业标准或者实施例描述的实施基础上略加修改后的实施方案也可以实现上述实施例相同、等同或相近、或变形后可预料的实施效果。应用这些修改或变形后的数据存储、设置、信息交互方式等，仍然可以属于本申请的所述保护可选实施方案范围之内。

虽然本申请提供了如实施例或流程图所述的方法操作步骤，但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式，不代表唯一的执行顺序。在实际中的装置或客户端产品执行时，可以按照实施例或者附图所示的方法顺序执行或者并行执行（例如并行处理器或者多线程处理的环境）。

上述实施例阐明的单元、装置或模块，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本申请时可以把各模块的功能在同一个或多个软件和/或硬件中实现，也可以将实现同一功能的模块由多个子模块或子单元的组合实现。

本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内部包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描

述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构、类等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，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，移动终端，服务器，或者网络设备等）执行本申请各个实施例或者实施例的某些部分所述的方法。

本说明书中的各个实施例采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。本申请可用于众多通用或专用的计算机系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的视频播放系统、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

虽然通过实施例描绘了本申请，本领域普通技术人员知道，本申请有许多变形和变化而不脱离本申请的精神，希望所附的权利要求包括这些变形和变化而不脱离本申请的精神。

权 利 要 求 书

1、一种防止拷贝攻击的处理方法，其特征在于，所述方法包括:

客户端向服务器发送业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

所述服务器解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码是否全部相同;

若所述比较结果为否，则所述服务器判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，所述服务器向所述客户端发送新的变动识别码;

所述客户端将接收到的新的变动识别码更新至所述本地安全存储中。

2、如权利要求 1 所述的一种防止拷贝攻击的处理方法，其特征在于，所述预设响应动作包括:

所述服务器下发要求所述业务数据对应的用户进行身份验证的消息，并在身份验证通过后向用户的客户端发送重新分配的唯一识别码和变动识别码。

3、一种防止拷贝攻击的处理方法，其特征在于，所述方法包括:

接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同;

若所述比较结果为否，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，向所述客户端发送新的变动识别码。

4、如权利要求 3 所述的一种防止拷贝攻击的处理方法，其特征在于，所述预设响应动作包括:

下发要求所述业务数据对应的用户进行身份验证的消息，并在身份验证通过后向用户的客户端发送重新分配的唯一识别码和变动识别码。

5、如权利要求 3 或 4 所述的一种防止拷贝攻击的处理方法，其特征在于，所述变动识别码被设置成采用整数逐次累加的方式生成。

6、如权利要求 3 或 4 所述的一种防止拷贝攻击的处理方法，其特征在于，客户端与服务器之间所述唯一识别和变动识别码的信息交互采用使用非对称加密、对称加密中的任意一种加密方式实现。

7、一种防止拷贝攻击的处理方法，其特征在于，所述方法包括:

在本地安全存储初始化时存储由服务器发送来的唯一识别码和变动识别码;

向服务器发送业务数据，所述业务数据包括本地安全存储的唯一识别码和变动识别码;

接收服务器发送的新的变动识别码，所述新的变动识别码为服务器比较客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码为全部相同时发送的变动识别码;

将接收到的所述新的变动识别码更新至所述本地安全存储中。

8、如权利要求 7 所述的一种防止拷贝攻击的处理方法，其特征在于，所述方法还包括:

基于接收到的身份验证消息进行身份验证；并在所述身份验证通过

后，根据接收到的服务器重新分配的唯一识别码和变动识别码初始化本地安全存储。

9、一种防止拷贝攻击的服务器，其特征在于，所述服务器包括:

数据接收模块，用于接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码;

比较模块，用于解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同;

处理模块，用于若所述比较模块的比较结果为否时，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，向所述客户端发送新的变动识别码。

10、如权利要求 9 所述一种防止拷贝攻击的服务器，其特征在于，所述处理模块包括:

第一处理模块，用于在判断客户端的本地安全存储为受到拷贝攻击时下发要求所述业务数据对应的用户进行身份验证的消息，并在身份验证通过后向用户的客户端发送重新分配的唯一识别码和变动识别码;

第二处理模块，用于在判断客户端的本地安全存储为未受到拷贝攻击时所述服务器向所述客户端发送新的变动识别码。

11、如权利要求 9 或 10 所述一种防止拷贝攻击的服务器，其特征在于，所述变动识别码被设置成采用整数逐次累加的方式生成。

12、如权利要求 9 或 10 所述一种防止拷贝攻击的服务器，其特征在

于，客户端与服务器之间所述唯一识别和变动识别码的信息交互采用使用非对称加密、对称加密中的任意一种加密方式实现。

13、一种防止拷贝攻击的客户端，其特征在于，所述客户端包括:

安全存储模块，用于在本地安全存储初始化时存储由服务器发送来的唯一识别码和变动识别码;

数据发送模块，用于向服务器发送业务数据，所述业务数据包括所述安全存储模块存储的唯一识别码和变动识别码;

第一接收模块，用于接收服务器发送的新的变动识别码，所述新的变动识别码为服务器比较客户端上传的唯一识别码和变动识别码与服务器记录的该客户端的唯一识别码和变动识别码为全部相同时发送的变动识别码;

更新模块，用于将接收到的所述新的变动识别码更新至所述本地安全存储中。

14、如权利要求 13 所述一种防止拷贝攻击的客户端，其特征在于，所述客户端还包括:

第二接收模块，用于接收服务器发的身份验证消息，和在身份验证通过后服务器发送的重新分配的唯一识别码和变动识别码;

验证处理模块，用于基于接收到的身份验证消息进行身份验证；并在所述身份验证通过后，根据接收到的服务器重新分配的唯一识别码和变动识别码初始化本地安全存储。

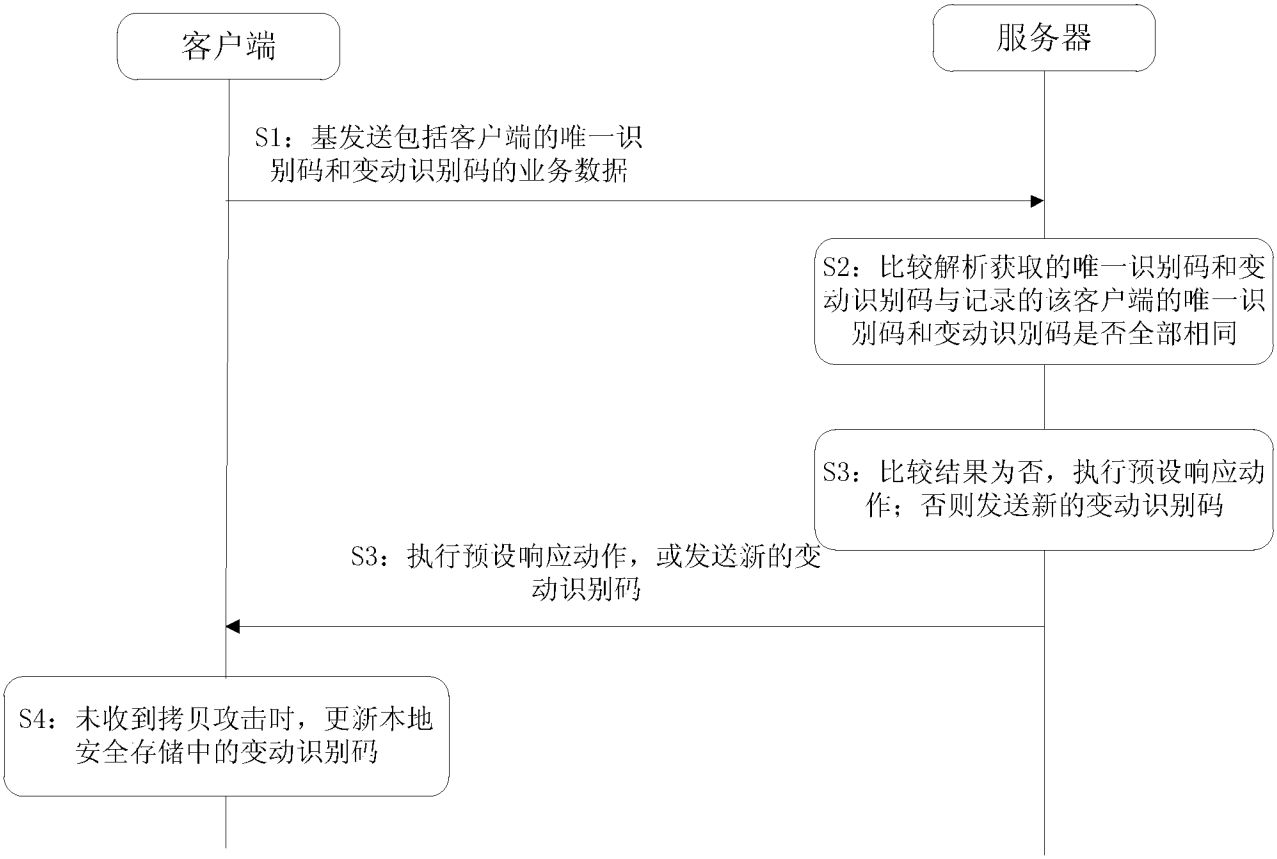
客户端
服务器
S1：基发送包括客户端的唯一识别码和变动识别码的业务数据
S2：比较解析获取的唯一识别码和变动识别码与记录的该客户端的唯一识别码和变动识别码是否全部相同
S3：比较结果为否，执行预设响应动作；否则发送新的变动识别码
S3：执行预设响应动作，或发送新的变动识别码
S4：未收到拷贝攻击时，更新本地安全存储中的变动识别码

图 1

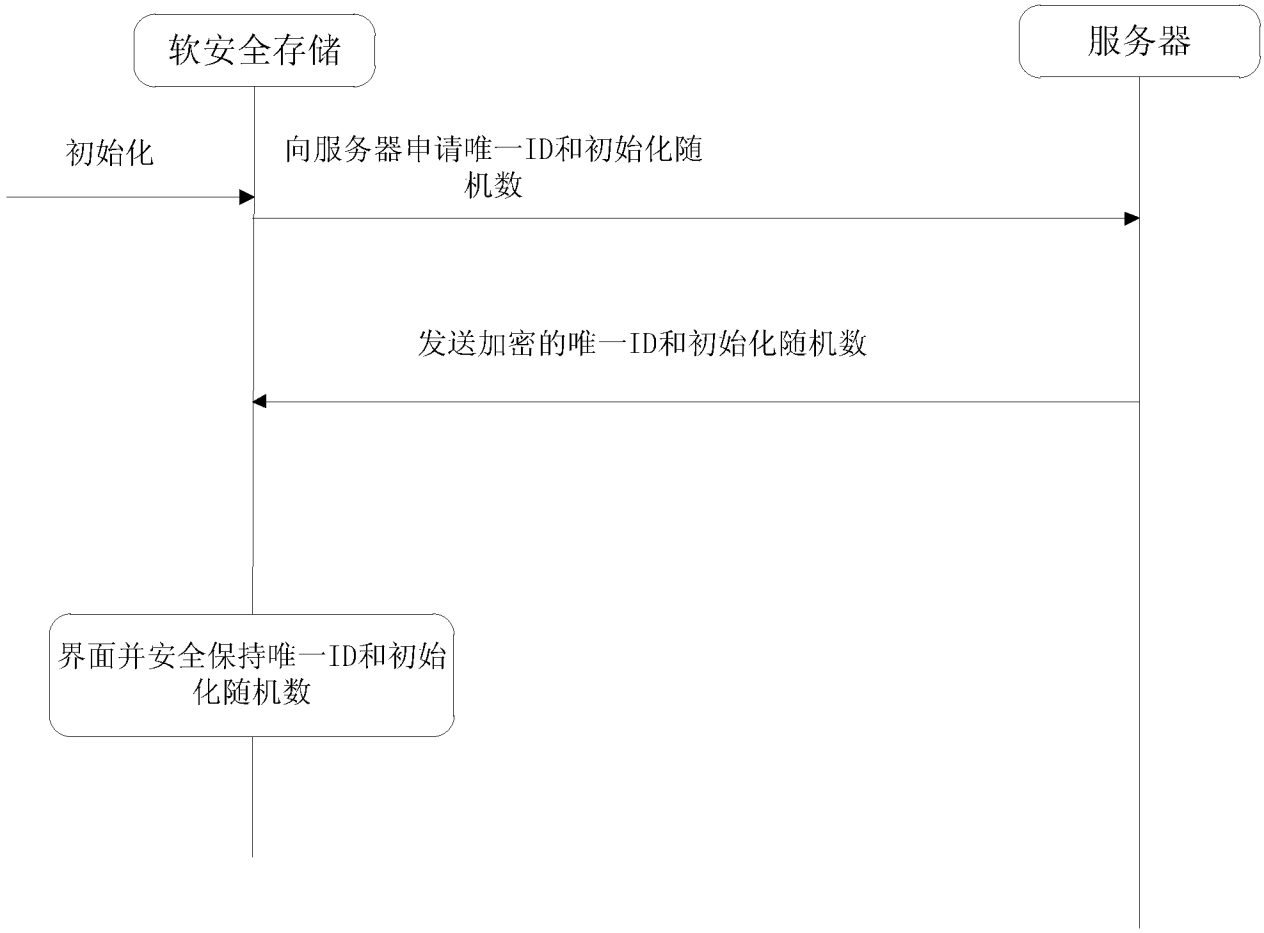
软安全存储
服务器
初始化
向服务器申请唯一ID和初始化随机数
发送加密的唯一ID和初始化随机数
界面并安全保持唯一ID和初始化随机数

图 2

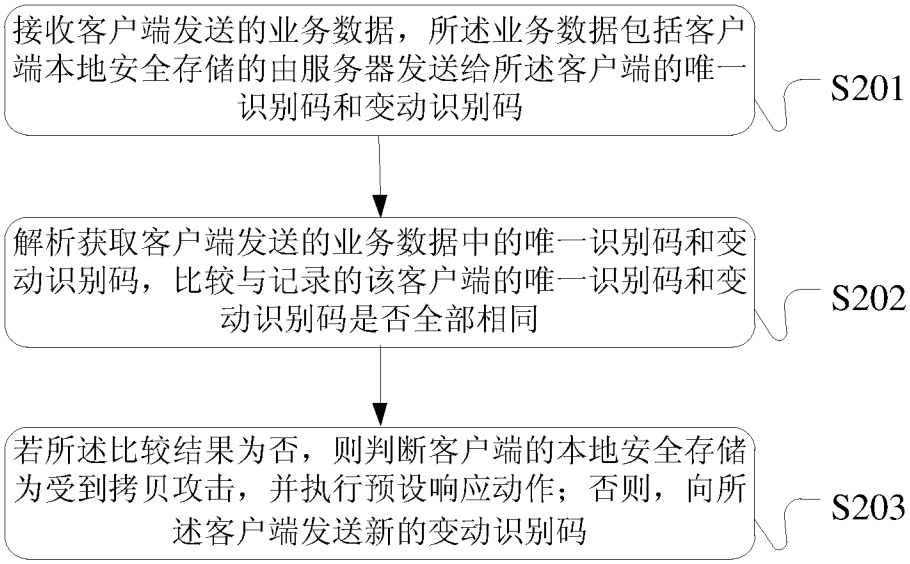
接收客户端发送的业务数据，所述业务数据包括客户端本地安全存储的由服务器发送给所述客户端的唯一识别码和变动识别码
S201
解析获取客户端发送的业务数据中的唯一识别码和变动识别码，比较与记录的该客户端的唯一识别码和变动识别码是否全部相同
S202
若所述比较结果为否，则判断客户端的本地安全存储为受到拷贝攻击，并执行预设响应动作；否则，向所述客户端发送新的变动识别码
S203

图 3

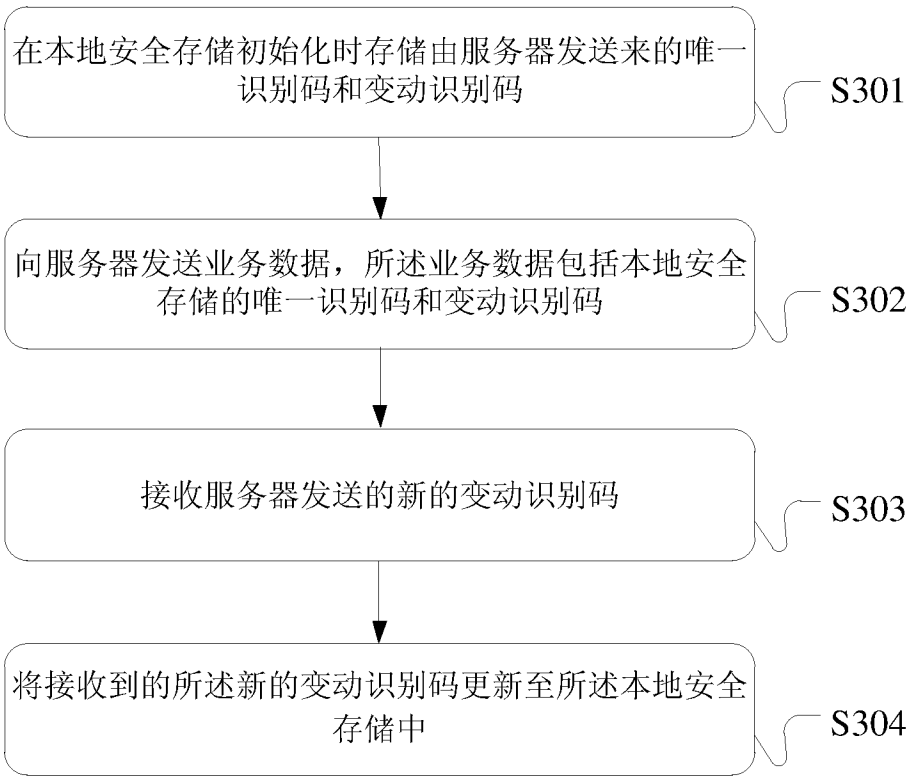
在本地安全存储初始化时存储由服务器发送来的唯一识别码和变动识别码
S301
向服务器发送业务数据，所述业务数据包括本地安全存储的唯一识别码和变动识别码
S302
接收服务器发送的新的变动识别码
S303
将接收到的所述新的变动识别码更新至所述本地安全存储中
S304

图 4

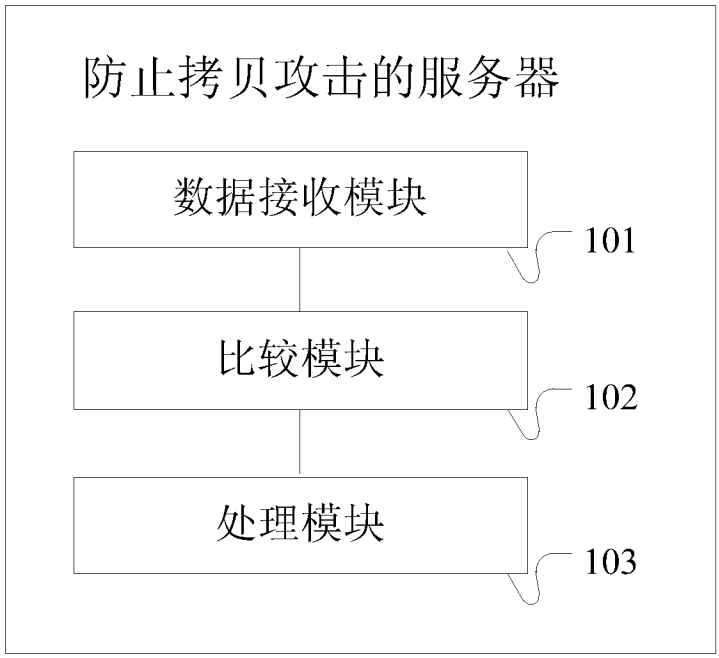
防止拷贝攻击的服务器
数据接收模块
101
比较模块
102
处理模块
103

图 5

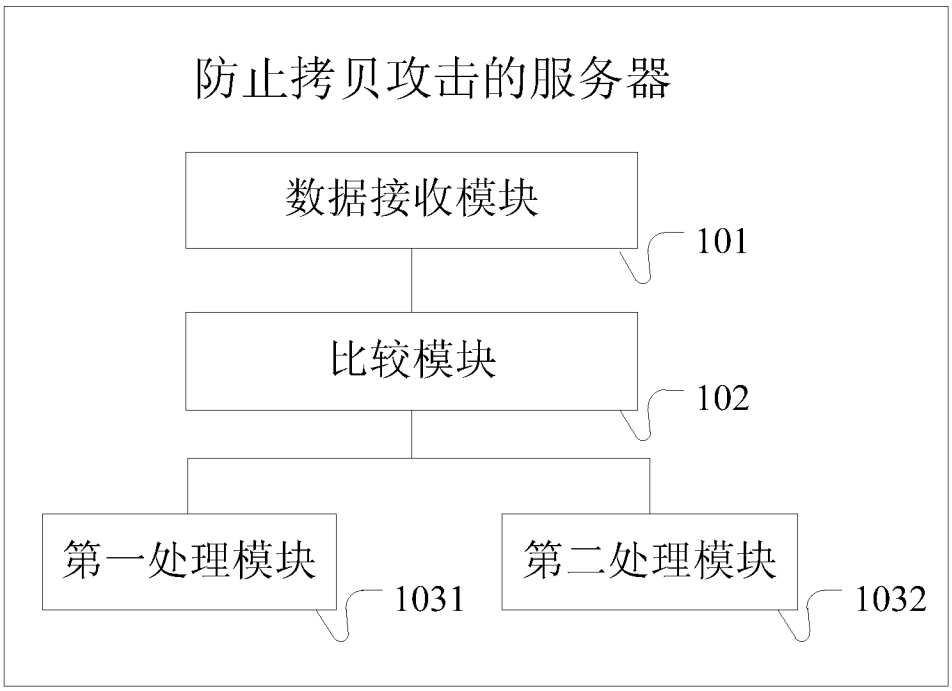
防止拷贝攻击的服务器
数据接收模块
101
比较模块
102
第一处理模块
1031
第二处理模块
1032

图 6

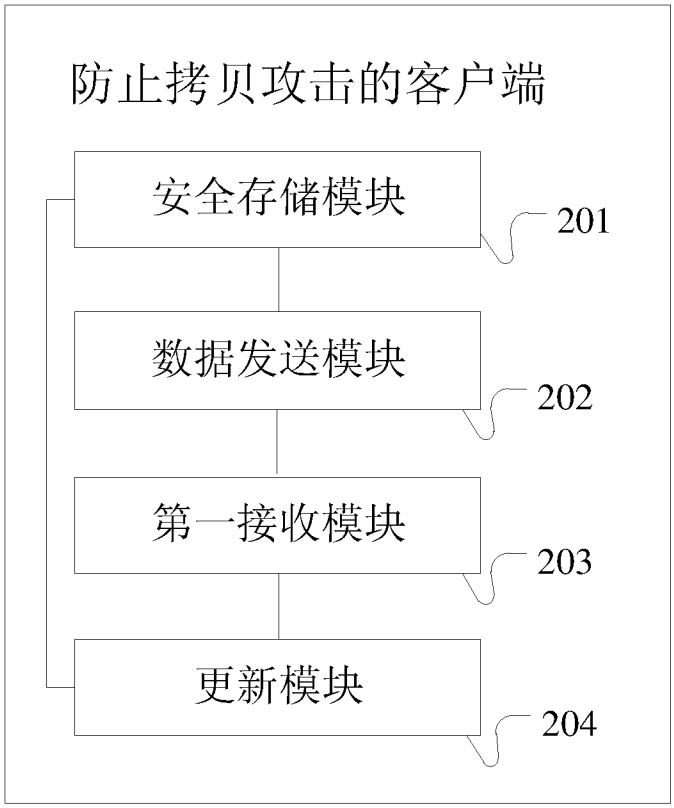

图 7

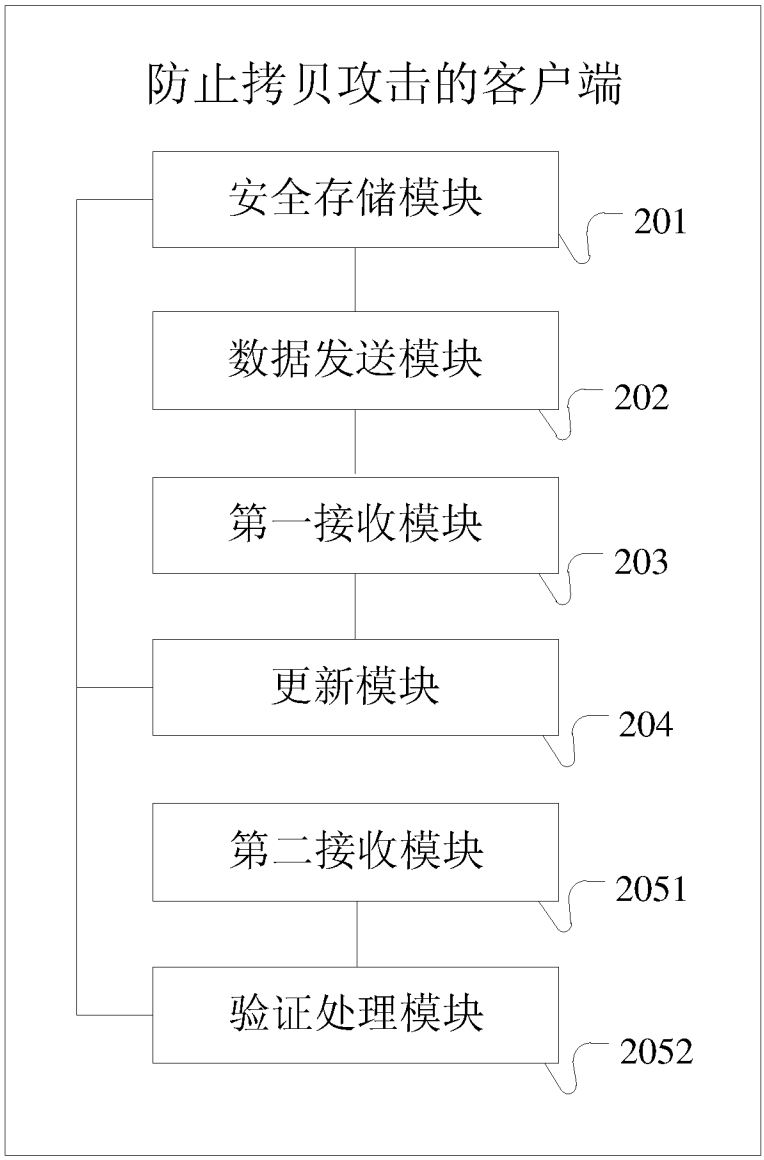
防止拷贝攻击的客户端
安全存储模块
201
数据发送模块
202
第一接收模块
203
更新模块
204
第二接收模块
2051
验证处理模块
2052

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/080006

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55(2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, GOOGLE: compare, copy attack, random, modify, change, hacker, sole, client, cloning attack, update, identification code, command, attack+, copy, code, dynamic, identif+, server?, client, secur+, safety

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104579694 A (ZHEJIANG UNIVERSITY), 29 April 2015 (29.04.2015), description, paragraphs [0066]-[0077], [0092] and[0125]	1-14
A	CN 101166091 A (ALIBABA CORPORATION), 23 April 2008 (23.04.2008), the whole document	1-14
A	CN 105491077 A (ZHEJIANG WELLCOM TECHNOLOGY CO., LTD.), 13 April 2016 (13.04.2016), the whole document	1-14
A	CN 104301288 A (ZHONGCHAO CREDIT CARD INDUSTRY DEVELOPMENT CO., LTD.), 21 January 2015 (21.01.2015), the whole document	1-14
A	CN 104331801 A (CHONGQING ZHITAO INFORMATION TECHNOLOGY CENTRE), 04 February 2015 (04.02.2015), the whole document	1-14
A	US 2013204935 A1 (SOARIC AB), 08 August 2013 (08.08.2013), the whole document	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29June 2017 (29.06.2017)	**10July 2017 (10.07.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **CHENG, Xiaomei** Telephone No.:(86-10) **62413598**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/080006

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104579694 A	29 April 2015	None	
CN 101166091 A	23 April 2008	HK 1120172 A1	15 April 2011
CN 105491077 A	13 April 2016	None	
CN 104301288 A	21 January 2015	None	
CN 104331801 A	04 February 2015	None	
US 2013204935 A1	08 August 2013	WO 2013117506 A1	15 August 2013
		EP 2813051 A1	17 December 2014

国际检索报告

国际申请号
PCT/CN2017/080006

A. 主题的分类

G06F 21/55(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC,GOOGLE: 进攻，攻击，码，比对，对比，比较，拷贝攻击，拷贝，复制攻击，复制，随机，改动，变动，动态，黑客，唯一，服务器，客户，克隆攻击，更新，变更，识别码，口令，安全，attack+, copy, code, dynamic, identif+, server?, client, secur+, safety

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104579694 A (浙江大学) 2015年 4月 29日 (2015-04-29) 说明书第[0066]-[0077]、[0092]、[0125]段	1-14
A	CN 101166091 A (阿里巴巴公司) 2008年 4月 23日 (2008-04-23) 全文	1-14
A	CN 105491077 A (浙江维尔科技股份有限公司) 2016年 4月 13日 (2016-04-13) 全文	1-14
A	CN 104301288 A (中钞信用卡产业发展有限公司) 2015年 1月 21日 (2015-01-21) 全文	1-14
A	CN 104331801 A (重庆智韬信息技术中心) 2015年 2月 4日 (2015-02-04) 全文	1-14
A	US 2013204935 A1 (SOARIC AB) 2013年 8月 8日 (2013-08-08) 全文	1-14

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 6月 29日	2017年 7月 10日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 程小梅 电话号码 (86-10)62413598

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/080006

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104579694	A	2015年 4月 29日		无		
CN	101166091	A	2008年 4月 23日	HK	1120172	A1	2011年 4月 15日
CN	105491077	A	2016年 4月 13日		无		
CN	104301288	A	2015年 1月 21日		无		
CN	104331801	A	2015年 2月 4日		无		
US	2013204935	A1	2013年 8月 8日	WO	2013117506	A1	2013年 8月 15日
				EP	2813051	A1	2014年 12月 17日