(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 104657856 A
(43)申请公布日 2015.05.27

(21)申请号 201510107347.0

(22)申请日 2015.03.11

(71)申请人 上海美迪索科电子科技有限公司
地址 200241 上海市闵行区东川路555号4号楼302C室

(72)发明人 雍雯 武发明

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 郭国中 樊昕

(51)Int.Cl.
G06Q 20/32(2012.01)
G06Q 20/40(2012.01)
H04L 29/06(2006.01)

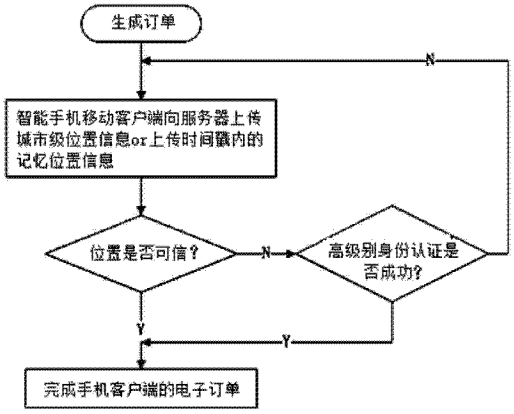
权利要求书2页 说明书4页 附图2页

(54)发明名称

基于位置认证的智能移动客户端支付方法及服务器系统

(57)摘要

本发明提供一种基于位置认证的智能移动客户端支付方法及服务器系统，由移动客户端生产包含城市级别的位置信息，生成订单时在身份认证的基础上，智能移动客户端需要同时向服务器系统上传位置信息，服务器系统通过算法进行位置认证，对于可信的位置即可直接完成移动客户端的电子订单，对于不可信的位置，则要求用户进行更高级别的身份认证；如果支付时遇到问题导致暂时难以获得其位置信息，则移动客户端查询之前使用过的位置信息，如果时间戳在可接受范围内，则上传该记忆位置信息至服务器，否则，认为位置认证失败，要求客户端进行更高级的身份认证。本发明能够提高智能移动客户端支付的安全性。



CN 104657856 A

1.一种基于位置认证的智能移动客户端支付方法，其特征在于，由移动客户端生产包含城市级别的位置信息，生成订单时在身份认证的基础上，智能移动客户端需要同时向服务器系统上传位置信息，服务器系统通过算法进行位置认证，对于可信的位置即可直接完成移动客户端的电子订单，对于不可信的位置，则要求用户进行更高级别的身份认证；如果支付时遇到问题导致暂时难以获得其位置信息，则移动客户端查询之前使用过的位置信息，如果时间戳在可接受范围内，则上传该记忆位置信息至服务器，否则，认为位置认证失败，要求客户端进行更高级的身份认证。

2.根据权利要求 1 所述的基于位置认证的智能移动客户端支付方法，其特征在于，所述服务器端通过算法进行位置认证的具体方法是：采取时钟 T 这个动态因素，在位置认证的初始阶段，当用户在客户端登陆并向资源服务器发出资源访问请求时，系统提示用户输入用户名 ID 和密码 PW，同时产生系统时钟 T，然后调用 RSA 算法，用自己的私匙 Ke 计算出 M ＝ H(ID，PW，T)，再将数据 (ID，M) 发送到服务器端，服务器端收到数据 M 后，查询用户数据库，得到用户密码 PW’以及用户公匙 Kd，同时计算得出时间因素 T’，然后调用 RSA 算法，用用户的公匙 Kd 对 M 进行解密得到 ID、PW 和 T，再将 PW 与 PW’，T 与 T’分别进行比较，只有当它们都匹配的时候才能通过客户端的身份认证。

3.根据权利要求 1 所述的基于位置认证的智能移动客户端支付方法，其特征在于，所述时间戳不超过 5min。

4.一种基于位置认证的智能移动客户端支付的服务器系统，其特征在于，用于完成如权利要求 1 或 2 所述的支付方法的位置认证，包括以下模块组成：

- 位置认证模块：对于客户端上传到服务器的位置信息进行认证，并为通过位置认证的用户生成一个全局会话 Session；

- 系统管理模块：系统管理模块主要实现一个服务器主线程，处理相应的事务，并实现对系统管理的接口；

- 用户模块：进行用户帐号管理；

-RSA 模块：系统的核心模块之一，主要完成大数运算，RSA 算法，文本的加密解密；

-CA 模块：给用户发放证书；

- 数据库管理模块：维护和后台 MySQL 数据库通信的基本模块；

- 日志审计模块：被所有其他模块所调用。

5.根据权利要求 4 所述的基于位置认证的智能移动客户端支付的服务器系统，其特征在于，所述位置认证模块还用于实现服务器端监听线程，对于每个请求认证的客户专门使用一个线程，处理与相应客户端的所有事务。

6.根据权利要求 5 所述的基于位置认证的智能移动客户端支付的服务器系统，其特征在于，所述系统管理模块针对每一个连接的用户创建一个单独的线程，服务器处理该用户的服务请求时参考所述 Session 里的信息。

7.根据权利要求 6 所述的基于位置认证的智能移动客户端支付的服务器系统，其特征在于，所述 Session 包括用户 ID，用户 IP，用户名，创建时间，生存时间，访问权限。

8.根据权利要求 5 所述的基于位置认证的智能移动客户端支付的服务器系统，其特征在于，所述用户模块进行用户账号管理主要包括两个方面的内容，分别为：新用户注册和用户信息更新，这些信息被保存在数据库中，以备系统调用。

9. 根据权利要求 8 所述的基于位置认证的智能移动客户端支付的服务器系统，其特征在于，所述用户模块还充当 CA 的角色，用来给用户发放证书。

基于位置认证的智能移动客户端支付方法及服务器系统

技术领域

[0001] 本发明涉及网络安全通讯领域，具体涉及一种基于位置认证的智能移动客户端支付方法及服务器系统。

背景技术

[0002] 信息安全的主要任务提供以下 5 种安全服务：身份认证服务、访问控制服务、数据保密服务，数据完整性服务和抗抵赖服务。其中身份认证服务实现网络安全的重要服务之一，它是网络应用系统中的第一道防线，是安全的网络系统的门户。涉及网络通信的各方必须通过某种形式的身份认证机制来证明它们的身份。目前主流的身份认证方式有 3 种，一种是传统的“用户名 + 口令”的基本认证方式，一种是基于生物特征的认证方式如人的指纹和虹膜，最后一种是基于“口令 + 硬件加密设备（如动态口令卡、USBKEY）”的双因素认证方式。传统的“用户名 + 口令”的认证方式其口令很容易被截取，安全性很低。基于生物特征的认证方式虽然安全性很高，但由于成本和技术的原因其应用有限。因此基于“口令 + 硬件加密设备”的双因素认证方式是目前电子商务和电子政务中广泛采用的身份认证机制

[0003] 近年随着智能手机的移动支付越来越普及，安全问题成为一个重要挑战。一方面由于手机病毒、钓鱼链接、支付环境复杂、快捷支付验证环节简化等影响，使用基于账户密码的身份认证并不能提供足够的安全保障，在支付过程中在账号密码的基础上添加基于位置认证，可以提高支付的安全性。另一方面智能手机是开放系统，手机上的 app 可能篡改伪造位置信息，对需要真实位置的服务造成影响，尤其可能欺骗基于位置的认证应用。

发明内容

[0004] 本发明针对上述现有技术中存在的技术问题，提供一种基于位置认证的智能移动客户端支付方法及服务器系统，大幅度增加了系统的可扩展性和重用性，在支付过程中在账号密码的基础上添加基于位置认证，可以有效提高支付的安全性。

[0005] 为达到上述目的，本发明所采用的技术方案如下：

[0006] 一种基于位置认证的智能移动客户端支付方法，由移动客户端生产包含城市级别的位置信息，生成订单时在身份认证的基础上，智能移动客户端需要同时向服务器系统上传位置信息，服务器系统通过算法进行位置认证，对于可信的位置即可直接完成移动客户端的电子订单，对于不可信的位置，则要求用户进行更高级别的身份认证；如果支付时遇到问题导致暂时难以获得其位置信息，则移动客户端查询之前使用过的位置信息，如果时间戳在可接受范围内，则上传该记忆位置信息至服务器，否则，认为位置认证失败，要求客户端进行更高级的身份认证。

[0007] 所述服务器系统通过算法进行位置认证的具体方法是：采取时钟 T 这个动态因素，在位置认证的初始阶段，当用户在客户端登陆并向资源服务器发出资源访问请求时，系统提示用户输入用户名 ID 和密码 PW，同时产生系统时钟 T，然后调用 RSA 算法（RSA 公钥密码算法是一种公认十分安全的公钥密码算法），用自己的私匙 Ke 计算出 M = H(ID, PW, T)，

再将数据(ID,M)发送到服务器端,服务器端收到数据M后,查询用户数据库,得到用户密码PW'以及用户公匙Kd,同时系统采用上述相同方法计算得出时间因素T',然后调用RSA算法,用用户的公匙Kd对M进行解密得到ID、PW和T,再将PW与PW',T与T'分别进行比较,只有当它们都匹配的时候才能通过客户端的身份认证。

[0008] 所述时间戳不超过5min。

[0009] 一种基于位置认证的智能移动客户端支付的服务器系统,用于完成上述的支付方法的位置认证,包括以下模块组成:

[0010] -位置认证模块

[0011] 对于客户端上传到服务器的位置信息进行认证,并为通过位置认证的用户生成一个全局会话Session。

[0012] 位置认证模块还要实现服务器端监听线程,对于每个请求认证的客户专门使用一个线程,处理与相应客户端的所有事务。

[0013] -系统管理模块

[0014] 系统管理模块主要实现一个服务器主线程,处理相应的事务;

[0015] 系统针对每一个连接的用户创建一个单独的线程,当用户通过服务器的身份认证后,会产生一个全局会话Session,驻留在服务器内存中,服务器处理该用户的一些服务请求时会参考Session里的信息;

[0016] Session包括用户ID,用户IP,用户名,创建时间,生存时间,访问权限等;

[0017] 系统管理模块还实现了对系统管理的接口。其主要功能有:数据库接口,设定数据库连接,以便于和后台数据库通讯。创建数据表格并且生成相应数据;

[0018] -用户模块

[0019] 用户帐号管理,包括增加、删除、修改用户帐号,修改密码,修改密匙,修改密匙有效期,修改权限等功能;

[0020] 其中的用户管理主要包括两个方面的内容,分别为:新用户注册和用户信息更新。

[0021] 这些信息被保存在数据库中,以备系统调用;

[0022] 此外用户模块还充当CA的角色,用来给用户发放证书;

[0023] -RSA模块:RSA模块是系统的核心模块之一,主要完成大数运算,RSA算法,文本的加密解密;

[0024] -CA模块

[0025] 给用户发放证书;

[0026] 当用户注册,证书的有效期限已经到期或者证书的私匙已经泄漏的时候,用户必须重新申请证书,CA经过核实后再对用户发放新的证书。如果是由于用户的私匙泄漏而产生的证书申请,那么更新后证书的内容与旧证书一样,只是CA用自己的新私钥对它进行数字签名;

[0027] -数据库管理模块

[0028] 维护和后台MySQL数据库通信的基本模块;

[0029] 其主要接口包括:数据连接,建立和维护和后台MySQL数据库的连接。其主要功能有连接数据库服务器,重新连接数据库服务器,选择数据库;

[0030] -日志审计模块

[0031] 服务器系统的一个常用基本模块，几乎被所有其他模块所调用；

[0032] 其主要的接口有生成相应事件日志记录，参数主要包括：时间，状态，事件类型，用户，时间处理对象等。

[0033] 本发明采用上述技术方案，所带来的有益效果如下：

[0034] 当代智能手机的移动支付越来越普及，安全问题是一个重要挑战。由于手机病毒、钓鱼链接、支付环境复杂、快捷支付验证环节简化等影响，使用基于账户密码的身份认证并不能提供足够的安全保障，本发明中提出的一种基于位置认证的智能移动客户端支付方法及服务器系统，在支付过程中在账号密码的基础上添加基于位置认证，可以有效提高支付的安全性。移动客户端生产包含城市级别的位置信息，生成订单时在身份认证的基础上，智能移动客户端需要同时向服务器系统上传位置信息，服务器系统通过算法进行位置认证，主要构造出一种基于位置认证的智能移动客户端支付的服务器系统，采用面向对象的软件构建技术，采用模块化设计的思想，从而大幅度增加了系统的可扩展性和重用性。

附图说明

[0035] 通过阅读参照以下附图对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0036] 图 1 是本发明位置认证过程流程图；

[0037] 图 2 是本发明系统结构模块组成框图；

[0038] 图 3 是 RSA 认证系统简化图；

[0039] 图 4 是 RSA 认证基本协议框图。

具体实施方式

[0040] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。

[0041] 本发明所提供的基于位置认证的移动客户端支付方法，具体内容如下：

[0042] 智能移动设备周期性较长（例如小时），长时间间隔地的向服务器发送位置信息帧，为避免隐私泄露，移动客户端可生产包含城市级别的位置信息。生成订单时在身份认证的基础上，智能手机移动客户端需要同时向服务器系统上传位置信息，服务器系统通过算法分析该位置信息是否可信，对于可信的位置即可直接完成手机客户端的电子订单，对于不可信的位置，则要求用户进行更高级别的身份认证（例手机动态验证码等验证方式）。如果支付时遇到网络传输困难等问题导致暂时难以获得其位置信息，则移动客户端可查询之前使用过的位置信息，如果时间戳在可接受范围内一般不会超过 5min，则上传该记忆位置信息至服务器，否则，认为位置认证失败，要求客户端进行更高级的身份认证。位置认证过程如图 1 所示。

[0043] 本发明所提供的基于位置认证的移动客户端支付方法中的服务器系统，其实现思想是采用面向对象的软件构建技术，采用模块化设计的思想，大幅度增加了系统的可扩展性和重用性。服务器系统包括位置认证模块、系统管理模块、用户模块、RSA 加密模块、数据

库管理模块和日志审计模块六个主要模块。

[0044] 为了进行可靠的客户端位置认证，并进行安全传输，系统服务器中加入了特有的位置认证模块与 RSA 模块。服务器系统的整个模块结构如图 2 所示，其中 RSA 模块是系统的基础模块，主要用来实现大数运算、RSA 加密解密等功能，经常会被其他模块所调用。数据库管理模块用来处理于用户数相关的一些操作，也会被其他模块基本所调用。系统的核心模块是系统管理模块，它主要用来加载服务，协调其他模块之间的功能调用。

[0045] 客户端与服务器间进行位置认证时需要通过 RSA 模块进行身份认证，在此基础上保障了数据传输的安全性。目前在 Internet 上使用基于公共密钥的安全策略进行身份认证必须有一个第三方的证明授权 (CA) 中心为客户签发身份证明。客户和服务器各自从 CA 获取证明，并且信任该证明授权中心。在会话和通讯时首先交换身份证明，其中包含了将各自的公钥交给对方，然后才使用对方的公钥验证对方的数字签名、交换通讯的加密密钥等。在确定是否接受对方的身份证明时，还需检查有关服务器，以确认该证明是否有效。简化的 RSA 位置认证系统结构图如图 3 所示。

[0046] 该系统设计中简化了 PKI 机制，CA 机构包含在系统服务器中，成为服务器的一个功能模块，其作用是用来为用户发放证书。客户端和服务器端总共只进行了两次信息传递，实现了一次性身份认证，简单快捷，但可能存在安全性不足的可能。为了提高安全性，系统设计中采取了时钟 T 这个动态因素。

[0047] 在位置认证的初始阶段，客户端根据当前的系统时间计算出时间因素 T，然后调用 RSA 算法，用自己的私匙 Ke 计算出 M ＝ H(ID,PW,T)，再将数据 (ID,M) 发送到服务器端。服务器端收到数据 M 后，查询用户数据库，得到用户密码 PW’ 以及用户公匙 Kd，同时计算得出时间因素 T’，然后调用 RSA 算法，用用户的公匙 Kd 对 M 进行解密得到 ID，PW 和 T，再将 PW 与 PW’，T 与 T’分别进行比较，只有当它们都匹配的时候才能通过客户端的身份认证。基本协议如图 4 所示。

[0048] 以上对本发明的具体实施例进行了描述。需要理解的是，本发明并不局限于上述特定实施方式，本领域技术人员可以在权利要求的范围内做出各种变形或修改，这并不影响本发明的实质内容。

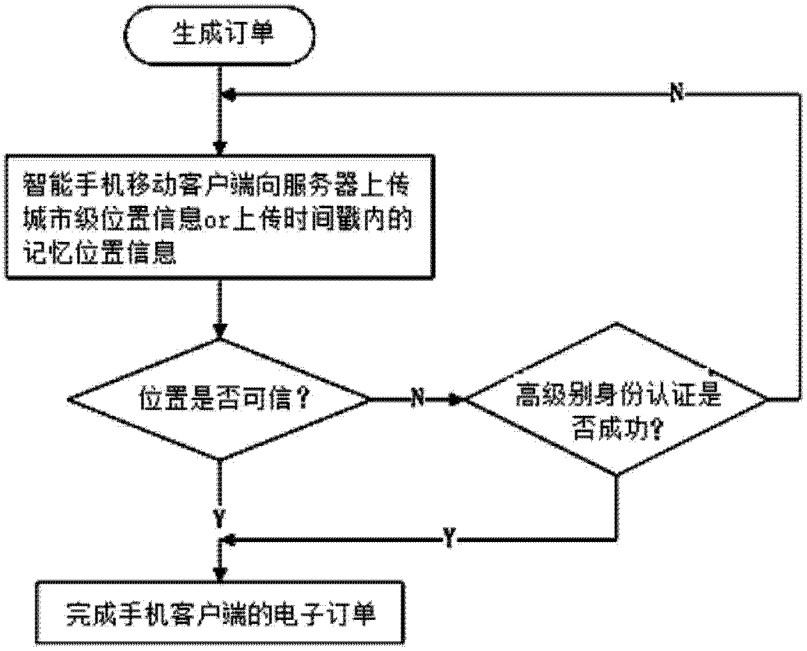

生成订单
N
智能手机移动客户端向服务器上传城市级位置信息or上传时间戳内的记忆位置信息
位置是否可信？
N
高级别身份认证是否成功？
Y
Y
完成手机客户端的电子订单

图 1

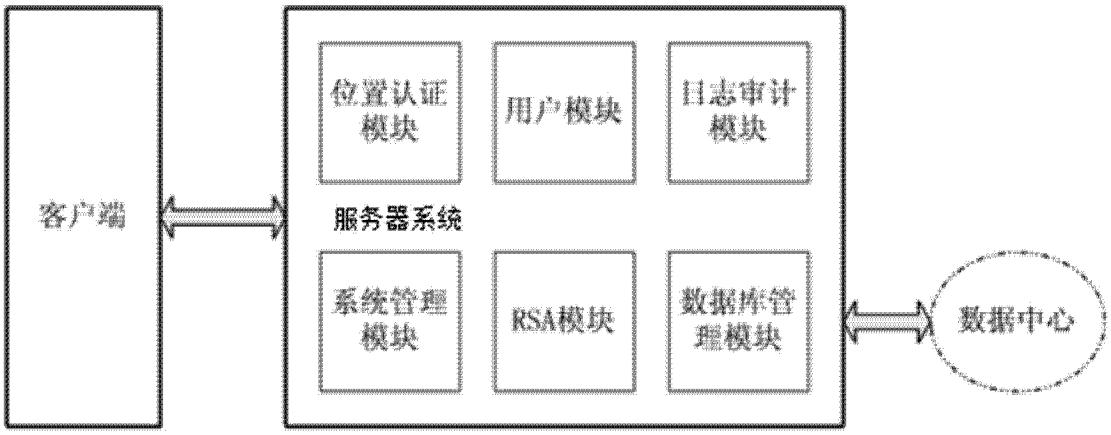

客户端
位置认证模块
用户模块
日志审计模块
服务器系统
系统管理模块
RSA模块
数据库管理模块
数据中心

图 2

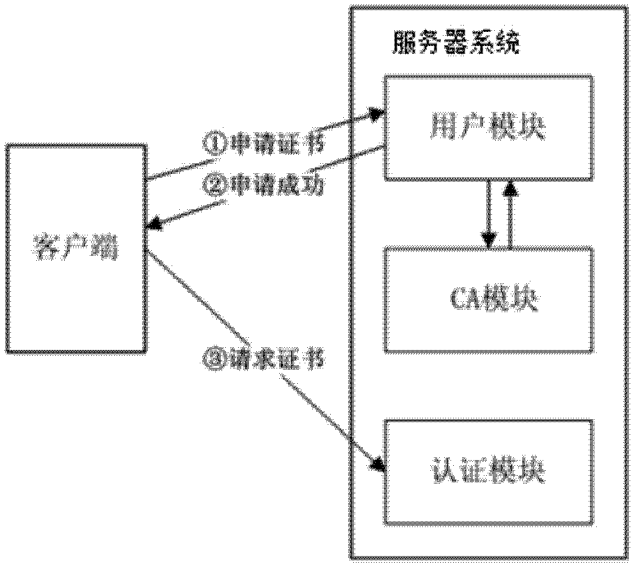

服务器系统
用户模块
①申请证书
②申请成功
客户端
CA模块
③请求证书
认证模块

图 3

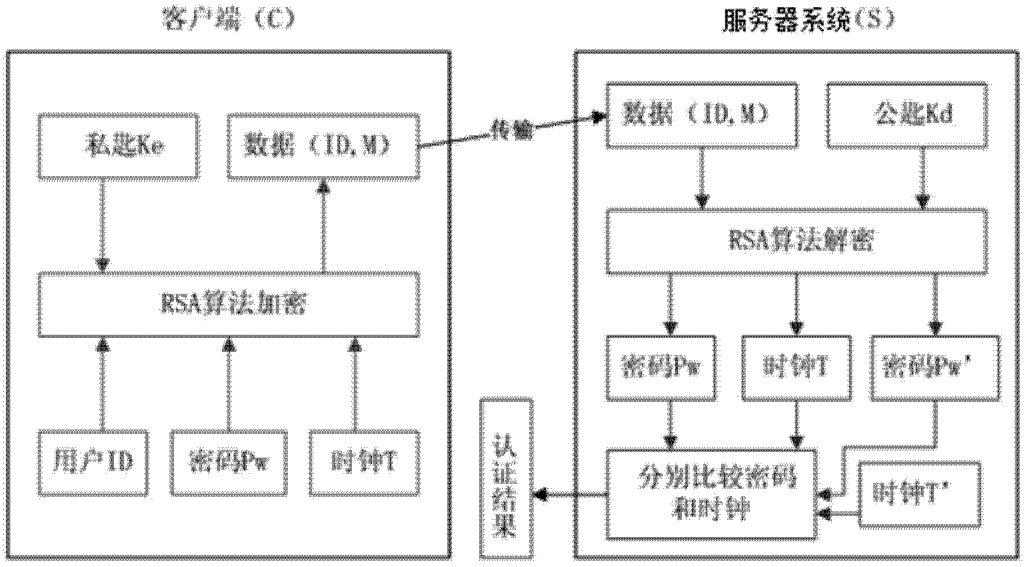

客户端（C）
服务器系统(S)
私匙Ke
数据（ID,M）
传输
数据（ID,M）
公匙Kd
RSA算法解密
RSA算法加密
密码Pw
时钟T
密码Pw'
用户ID
密码Pw
时钟T
认证结果
分别比较密码和时钟
时钟T'

图 4