



(12) 发明专利

(10) 授权公告号 CN 101373528 B

(45) 授权公告日 2014.04.02

(21) 申请号 200710120579.5

1 和 4.

(22) 申请日 2007.08.21

CN 1340764 A, 2002.03.20, 摘要、权利要求

1.

(73) 专利权人 联想(北京)有限公司

审查员 胡徐兵

地址 100085 北京市海淀区上地信息产业基地
创业路 6 号

(72) 发明人 于辰涛

(74) 专利代理机构 北京银龙知识产权代理有限公司 11243

代理人 许静 黄灿

(51) Int. Cl.

G06Q 20/38 (2012.01)

(56) 对比文件

CN 1497485 A, 2004.05.19, 摘要、说明书第 7 页第 9 行至 11 页第 4 行、附图 1.

CN 1381008 A, 2002.11.20, 摘要、权利要求 1-8、说明书第 6 页第 15 行至 12 页第 30 行、附图

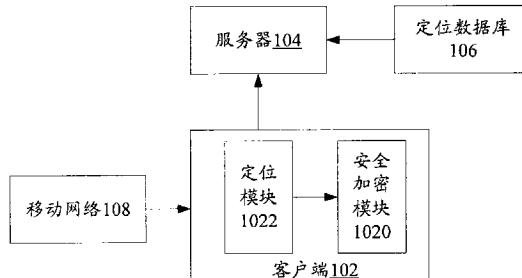
权利要求书3页 说明书7页 附图4页

(54) 发明名称

基于位置认证的电子支付系统、设备、及方法

(57) 摘要

本发明公开了一种基于位置认证的电子支付系统，包括：客户端，包括定位模块和安全加密模块，其中，定位模块用于获取用户的交易位置信息，安全加密模块用于生成加密的位置宣告信息，其中，位置宣告信息包括：交易位置信息和会话标识；定位数据库，用于存储与用户的交易记录相关的位置描述信息；服务器，用于通过将交易位置信息与定位数据库中的位置描述信息进行比较，来验证来自客户端的交易位置信息所表示的位置是否为可信位置。通过本发明，进一步降低了电子支付服务人工验证成本，同时又增加了黑客在异地发出支付定单的难度，提高了现有技术方案的安全性，提高了用户体验。



1. 一种基于位置认证的电子支付系统,其特征在于,包括:

客户端,包括定位模块和安全加密模块,其中,所述定位模块用于获取用户的交易位置信息,所述安全加密模块用于生成加密的位置宣告信息,其中,所述位置宣告信息包括:所述交易位置信息和会话标识;

定位数据库,用于存储与用户的交易记录相关的位置描述信息;以及

服务器,用于通过将所述交易位置信息与所述定位数据库中的所述位置描述信息进行比较,来验证来自所述客户端的所述交易位置信息所表示的位置是否为可信位置。

2. 根据权利要求 1 所述的电子支付系统,其特征在于,所述客户端生成对所述位置宣告信息加密的密钥,并将所述密钥上传至所述服务器。

3. 根据权利要求 1 所述的电子支付系统,其特征在于,所述服务器生成对所述位置宣告信息加密的密钥,并将所述密钥下发至所述客户端。

4. 根据权利要求 2 或 3 所述的电子支付系统,其特征在于,所述定位数据库连接至所述服务器,所述服务器通过查询所述定位数据库获取所述用户的所述位置描述信息。

5. 根据权利要求 4 所述的电子支付系统,其特征在于,所述服务器使用所述密钥将所述位置宣告信息解密,获取其中的所述交易位置信息,并将所述交易位置信息与所述位置描述信息进行比较,在二者一致的情况下,判定所述交易位置信息所表示的位置为可信位置。

6. 根据权利要求 2 或 3 所述的电子支付系统,其特征在于,所述定位数据库连接至所述客户端,所述客户端通过查询所述定位数据库获取所述用户的所述位置描述信息,并将所述位置描述信息上传至所述服务器。

7. 根据权利要求 6 所述的电子支付系统,其特征在于,所述服务器使用所述密钥将所述位置宣告信息解密,获取其中的所述交易位置信息,并将所述交易位置信息与所述位置描述信息进行比较,在二者一致的情况下,判定所述交易位置信息所表示的位置为可信位置。

8. 根据权利要求 1 至 3 中任一项所述的电子支付系统,其特征在于,所述位置宣告信息中进一步包括时间戳。

9. 根据权利要求 8 所述的电子支付系统,其特征在于,所述位置宣告信息中进一步包括:客户端设备标识、用户标识。

10. 根据权利要求 1 至 3 中任一项所述的电子支付系统,其特征在于,所述客户端包含两个异质网络,一个网络为用于访问互联网的普通网络,另一个网络为具有定位能力的无线网络。

11. 根据权利要求 1 至 3 中任一项所述的电子支付系统,其特征在于,所述客户端包含一个具有定位能力的无线网络,所述客户端通过所述无线网络进行网络数据传输及定位服务。

12. 一种基于位置认证的电子支付设备,其特征在于,包括:

定位单元,用于获取用户交易的交易位置信息;

安全加密单元,用于生成加密的位置宣告信息,其中,所述位置宣告信息包括:所述交易位置信息和会话标识;

存储单元,用于存储与用户的交易记录相关的位置描述信息;

解密单元,用于将来自所述安全加密单元的所述位置宣告信息解密;以及

比较单元,用于将所述解密单元解密的所述交易位置信息与所述存储单元中存储的所述位置描述信息进行比较,以验证所述交易位置信息所表示的位置是否为可信位置。

13. 根据权利要求 12 所述的电子支付设备,其特征在于,

所述安全加密单元和所述解密单元进行加密 / 解密的密钥由所述电子支付设备所在的客户端生成,并且所述客户端将所述密钥上传至服务器;或者

所述安全加密单元对和所述解密单元进行加密 / 解密的密钥由服务器生成,并且所述服务器将所述密钥下发至所述电子支付设备。

14. 根据权利要求 13 所述的电子支付设备,其特征在于,所述比较单元在判断所述交易位置信息和所述位置描述信息一致的情况下,判断所述交易位置信息所表示的位置为可信位置。

15. 根据权利要求 12 至 14 中任一项所述的电子支付设备,其特征在于,所述存储单元独立于所述定位单元、所述安全加密单元、所述解密单元、以及所述比较单元。

16. 一种基于位置认证的电子支付方法,其特征在于,包括:

生成用于进行加密和解密操作的密钥;

客户端的安全加密模块使用所述密钥生成加密的位置宣告信息,其中,所述位置宣告信息包括:用户的交易位置信息和会话标识;

所述客户端将加密的所述位置宣告信息上传至所述服务器,并且所述服务器从定位数据库中查询与所述用户的交易记录相关的位置描述信息;以及

所述服务器使用所述密钥将所述位置宣告信息解密,并将所述位置描述信息与解密获得的所述交易位置信息进行比较,在二者一致的情况下,判定所述交易位置信息所表示的位置为可信位置。

17. 根据权利要求 16 所述的电子支付方法,其特征在于,所述密钥由所述客户端生成,并被上传至所述服务器,或者,所述密钥由所述服务器生成,并被下发至所述客户端。

18. 根据权利要求 17 所述的电子支付方法,其特征在于,所述位置宣告信息中进一步包括时间戳。

19. 根据权利要求 18 所述的电子支付方法,其特征在于,所述位置宣告信息中进一步包括:客户端设备标识、用户标识。

20. 一种基于位置认证的电子支付方法,其特征在于,包括:

生成用于进行加密和解密操作的密钥;

所述安全加密模块使用所述密钥生成加密的位置宣告信息,其中,所述位置宣告信息包括:用户的交易位置信息和会话标识;

所述客户端从定位数据库中查询与所述用户的交易记录相关的位置描述信息,并将所述位置描述信息和加密的所述位置宣告信息上传至所述服务器;以及

所述服务器使用所述密钥将所述位置宣告信息解密,并将所述位置描述信息与解密获得的所述交易位置信息进行比较,在二者一致的情况下,判定所述交易位置信息所表示的位置为可信位置。

21. 根据权利要求 20 所述的电子支付方法,其特征在于,所述密钥由所述客户端生成,并被上传至所述服务器,或者,所述密钥由所述服务器生成,并被下发至所述客户端。

22. 根据权利要求 21 所述的电子支付方法, 其特征在于, 所述位置宣告信息中进一步包括时间戳。

23. 根据权利要求 22 所述的电子支付方法, 其特征在于, 所述位置宣告信息中进一步包括: 客户端设备标识、用户标识。

基于位置认证的电子支付系统、设备、及方法

技术领域

[0001] 本发明涉及计算机安全通讯领域，并且特别地，涉及基于位置认证的电子支付系统、设备、及方法。

背景技术

[0002] 目前，随着电子商务的快速发展，越来越多的用户正在逐渐习惯使用网络进行个人金融管理服务和网上交易。但是由于用户对安全性问题的顾虑，也限制了电子商务和电子支付的进一步普及。业界为了提升电子支付终端的安全性，提出了多种解决办法。例如，Visa 和 Mastercard 推动的 PCI DSS 技术标准，在用户支付时，使用密码进行用户身份认证。

[0003] 对于用户而言，大部分的电子支付行为发生在用户经常上网的场所，这样的场所主要是用户的居住地、学校、和单位。而几乎所有的欺诈，都由黑客远程控制，比如网钓攻击和恶意代码，黑客将用户的个人核心金融数据获得后，在异地伪造订单，进行虚拟交易或实体交易，从而造成用户的金融损失。因此，目前电子支付的防欺诈解决方案很多方案也主要解决异地订单的有效性验证问题。

[0004] 目前，从 Cybersource 的统计数字来看，AVS (Address Verification Service, 地址验证服务)、CVN (Card Verification Number, 卡片验证码) 已经成为最频繁使用的电子支付防欺诈解决方案。超过 80% 的电子商务网站部署了 AVS (Address Verification Service, 地址验证服务) 系统（日访问量超过 100 万的大型电子商务网站部署高达 100%）。AVS 通过用户的订单交付地址和用户通讯地址的比对，确认用户身份和订单的有效性，然而，AVS 无法对无收单地址的支付服务提供安全保证，另外还有针对电子商务网站的 IP 地址验证方案，其验证用户的 IP 地址所在的服务提供商和国家，如果存在明显差异，则决定为非法定单，但是该方法粒度很粗，在恶意用户使用代理时，此方法将失效。

[0005] 部署 AVS、CVN、IPGI、和 APV 基本上可以大幅减少欺诈，使得黑客只能对很少比率的用户进行成功的金融欺诈。统计显示，主要电子商务网站的欺诈损失基本在营业额 1% 以下，然而由于电子支付金额快速提升，欺诈损失金额呈逐年上升的趋势。

[0006] 另外，随着无线网络的普及，用户也越来越多的在不可信的网络区域访问互联网。这使得用户金融数据容易被网络嗅探器进行攻击。而仅为了针对这些场所增加全面的安全支付解决方案，比如增加更多的设备和密码，实践证明，此种方案也不可接受。一个典型例子是，USB Key 在欧美并不被广泛接收，安全传输协议 SET 也遭到失败。因此，电子支付需要智能化程度更高，又不降低用户安全体验的解决方案。为此，电子支付网站为了降低欺诈风险，也广泛使用人工定单核实的方式验证定单的有效性，而这又极大地增加了电子支付网站的服务成本。而黑客通常通过木马程序或钓鱼网站获得用户的核心金融数据，然后通过远程方式在短时间内同时提交多个有效定单的方式，依靠电子支付网站人工核对的漏洞，造成用户的金融损失。

[0007] 从电子商务安全技术发展的特点来看，具有较高用户易用性的安全性方案较容易得到广泛的推广。因此，如果能够在现有的 AVS 方案和 IP 地址验证方案的基础上，提供一

种能够进一步降低电子支付服务人工验证成本,同时又增加黑客在异地发出支付定单的难度的解决方案无疑是理想的。

发明内容

[0008] 考虑到现有技术中存在的上述问题而提出本发明,为此,本发明旨在提供一种基于位置认证的电子支付方案,具体地,提供基于位置认证的电子支付系统、设备、及方法,其能够进一步降低电子支付服务人工验证成本,同时又增加黑客在异地发出支付定单的难度。

[0009] 根据本发明,首先提供了一种基于位置认证的电子支付系统。

[0010] 该系统包括:客户端,包括定位模块和安全加密模块,其中,定位模块用于获取用户的交易位置信息,安全加密模块用于生成加密的位置宣告信息,其中,位置宣告信息包括:交易位置信息和会话标识;定位数据库,用于存储与用户的交易记录相关的位置描述信息;服务器,用于通过将交易位置信息与定位数据库中的位置描述信息进行比较,来验证来自客户端的交易位置信息所表示的位置是否为可信位置。

[0011] 其中,客户端生成对位置宣告信息加密的密钥,并将密钥上传至服务器。或者,服务器生成对位置宣告信息加密的密钥,并将密钥下发至客户端。

[0012] 定位数据库可以连接至服务器,这样,服务器通过查询定位数据库获取用户的位置描述信息。之后,服务器使用密钥将位置宣告信息解密,获取其中的交易位置信息,并将交易位置信息与位置描述信息进行比较,在二者一致的情况下,判定交易位置信息所表示的位置为可信位置。

[0013] 定位数据库也可以连接至客户端,客户端通过查询定位数据库获取用户的位置描述信息,并将位置描述信息上传至服务器。之后,服务器使用密钥将位置宣告信息解密,获取其中的交易位置信息,并将交易位置信息与位置描述信息进行比较,在二者一致的情况下,判定交易位置信息所表示的位置为可信位置。

[0014] 另外,上述位置宣告信息中进一步包括时间戳,并且可以进一步包括:客户端设备标识、用户标识。

[0015] 另外,客户端可以包含两个异质网络,一个网络为用于访问互联网的普通网络,另一个网络为具有定位能力的无线网络。或者,客户端可以包含一个具有定位能力的无线网络,客户端通过该无线网络进行网络数据传输及定位服务。

[0016] 根据本发明,还提供了一种基于位置认证的电子支付设备。

[0017] 该设备包括:定位单元,用于获取用户交易的交易位置信息;安全加密单元,用于生成加密的位置宣告信息,其中,位置宣告信息包括:交易位置信息和会话标识;存储单元,用于存储与用户的交易记录相关的位置描述信息;解密单元,用于将来自安全加密单元的位置宣告信息解密;比较单元,用于解密单元解密的交易位置信息与存储单元中存储的位置描述信息进行比较,以验证交易位置信息所表示的位置是否为可信位置。

[0018] 其中,安全加密单元对位置宣告信息进行加密的密钥由电子支付设备所在的客户端生成,并且客户端将密钥上传至服务器,或者,安全加密单元对位置宣告信息进行加密的密钥由服务器生成,并且服务器将密钥下发至电子支付设备。

[0019] 比较单元在判断交易位置信息和位置描述信息一致的情况下,判断交易位置信息

所表示的位置为可信位置。

[0020] 另外,在该设备中,存储单元可以独立于定位单元和安全加密单元以及解密单元和比较单元。

[0021] 根据本发明,还提供了一种基于位置认证的电子支付方法。

[0022] 该方法包括以下处理:生成用于进行加密和解密操作的密钥;客户端的安全加密模块使用密钥生成加密的位置宣告信息,其中,位置宣告信息包括:用户的交易位置信息和会话标识;客户端将加密的位置宣告信息上传至服务器,并且服务器从定位数据库中查询与用户的交易记录相关的位置描述信息;服务器使用密钥将位置宣告信息解密,并将位置描述信息与解密获得的交易位置信息进行比较,在二者一致的情况下,判定交易位置信息所表示的位置为可信位置。

[0023] 其中,在上述处理中,密钥由客户端生成,并被上传至服务器,或者,密钥由服务器生成,并被下发至客户端。

[0024] 另外,该方法中的位置宣告信息中进一步包括时间戳,并且可以进一步包括:客户端设备标识、用户标识。

[0025] 根据本发明,还提供了另一种基于位置认证的电子支付方法。

[0026] 在该方法中,包括以下处理:生成用于进行加密和解密操作的密钥;安全加密模块使用密钥生成加密的位置宣告信息,其中,位置宣告信息包括:用户的交易位置信息和会话标识;客户端从定位数据库中查询与用户的交易记录相关的位置描述信息,并将位置描述信息和加密的位置宣告信息上传至服务器;服务器使用密钥将位置宣告信息解密,并将位置描述信息与解密获得的交易位置信息进行比较,在二者一致的情况下,判定交易位置信息所表示的位置为可信位置。

[0027] 其中,在上述处理中,密钥由客户端生成,并被上传至服务器,或者,密钥由服务器生成,并被下发至客户端。

[0028] 另外,该方法中的位置宣告信息中进一步包括时间戳,并且可以进一步包括:客户端设备标识、用户标识。

[0029] 通过本发明,进一步降低了电子支付服务人工验证成本,同时又增加了黑客在异地发出支付定单的难度,提高了现有技术方案的安全性,提高了用户体验。

[0030] 本发明的其它特征和优点将在随后的说明书中阐述,并且,部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0031] 附图用来提供对本发明的进一步理解,并且构成说明书的一部分,与本发明的实施例一起用于解释本发明,并不构成对本发明的限制。在附图中:

[0032] 图1是根据本发明实施例的基于位置认证的电子支付系统的示意图;

[0033] 图2是根据本发明实施例的基于位置认证的电子支付设备的示意图;

[0034] 图3是根据本发明实施例的基于位置认证的电子支付方法的流程图;

[0035] 图4是根据本发明实施例的电子支付方法中密钥生成过程的流程图;

[0036] 图5是根据本发明实施例的另一种基于位置认证的电子支付方法的流程图;以及

[0037] 图 6 是根据本发明实施例的用户在电子商务网站进行交易的具体处理流程图。

具体实施方式

[0038] 本发明实施例提供的基于位置认证的电子支付方案可以作为电子商务网站的 AVS 解决方案和 IP 地址验证方案的扩展方案，在移动终端和带有移动通讯接口的计算设备上，借助于本发明，利用设备的定位能力，使得用户在非可信环境下的交易使用加强的认证方案，在可信环境下的交易不改变用户目前的交易方式。另外，本发明的目的不是完全解决电子支付的安全性问题，而是在现有方案的基础上，进一步提高电子支付的安全性和用户体验。

[0039] 以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

[0040] 系统实施例

[0041] 根据本发明的系统实施例，首先提供了一种基于位置认证的电子支付系统。

[0042] 如图 1 所示，该系统包括客户端 102（包括安全加密模块 1020 和定位模块 1022）、服务器 104、定位数据库 106，还可以包括与客户端 102 连接的移动网络 108。

[0043] 概括地说，客户端 102 将由安全加密模块 1020 加密的交易位置信息发送到服务器 104，服务器 104 使用其与安全加密模块的共享密钥将该加密信息解密，并通过与定位数据库 106 中的位置描述信息进行比较来验证交易位置信息所表示的位置是否为可信位置，并且后续可以根据验证结果采取不同的处理策略。

[0044] 具体地，客户端在首次使用时，必须进行客户端初始化，客户端初始化主要针对安全加密模块 1020 进行相应的设置，例如，密钥的生成（将在下文中进行详细描述），加密方式的设置等，以使服务器在其后的通讯过程中，能够认证和解码客户端传回的信息（例如，下文中的位置宣告信息），以及验证其有效性（可以通过加密和签名来验证）。

[0045] 具体地，安全加密模块 1020 可以采用对称密钥或非对称密钥的方式对位置宣告信息进行加密处理。服务器和客户端的安全加密模块配对使用相应的解密密钥。对称密钥的加密方式可以包括 DES、3DES、AES、RC4、RC5 等，非对称密钥的加密方式可以包括 RSA、ECC 等。为了保证上传消息不被修改，还可以对消息进行数字签名。数字签名算法可以是 SHA-1，MD5 和 HMAC 等。

[0046] 安全加密模块 1020（可以是安全芯片、SIM 卡 /UICC 芯片，或者是主机上的软件程序）用于生成加密的位置宣告信息（例如，可以是经纬度信息），此后，该位置宣告信息将被发送至服务器，为了保证位置宣告信息不被伪造和重放，因此在发送之前首先对其进行加密。位置宣告信息中包括用户的交易位置信息（根据定位模块的不同，可以是位置点坐标，也可以是终端所在区块的定位标识数据。）和会话标识（例如，可以是交易标识、订单标识等）。另外，位置宣告信息中还包括时间戳，并且还可以进一步包括客户端设备标识、用户标识。其中，时间戳主要用于防止黑客进行重放攻击，时间戳可以是当前交易时间，也可以是内部计数器产生的随机数。

[0047] 上述的用户交易位置信息由客户端的定位模块 1022 获取。定位模块通过无线网络位置编码信息获得用户的所在位置，其可以通过全球定位终端（GPS）、电信网络（GSM 网

络、CDMA 网络、或 3G 网络) 来获得终端位置信息, 也可以使用 LBS(移动定位业务) 服务反馈的位置信息。

[0048] 安全加密模块 1020 对位置宣告信息加密的密钥, 由客户端和服务器共享, 其可以以证书的形式存储在安全加密单元的内部。该密钥可以由客户端动态生成, 也可以由服务器进行初始化。其中, 当密钥由客户端生成时, 客户端会通过 SSL 加密通道将密钥上传至服务器。当密钥由服务器生成时, 服务器会将密钥下发至客户端。

[0049] 优选地, 客户端可以进一步包括网络传输模块、安全认证模块等(图中未示出)。网络传输模块用于通过网络传输数据包, 并和服务端建立数据通道。安全认证模块用于根据服务器的反馈生成用户提示。并且, 客户端可以包含多种产品形态, 例如, 可以包含两个异质网络, 一个为普通网络, 可以为有线网络或近距无线网络, 主要用于用户访问互联网, 另一个为具有定位能力的无线网络, 包括 GPS、3G、和 RFID 等; 也可以仅包含一个具有定位能力的无线网络, 客户端可以通过无线网络同时进行网络数据传输和定位服务。

[0050] 定位数据库 106 用于存储与用户的交易记录相关的位置描述信息(具体的位置信息, 例如, 单位、住处等); 这样, 服务器 104 通过将客户端的交易位置信息与定位数据库中的位置描述信息进行比较, 来验证来自客户端的交易位置信息所表示的位置是否为可信位置。

[0051] 对于定位数据库 106, 其可以连接至服务器, 也可以连接至客户端, 其中, 图 1(a) 示出了定位数据库连接至服务器的情形, 而图 1(b) 示出了定位数据库连接至客户端的情形。客户端与服务器之间的交互会因为定位数据库与二者的连接关系的不同而有所改变。

[0052] 具体地, 在定位数据库连接至服务器 104 的情况下, 服务器通过查询定位数据库获取用户的位置描述信息。之后, 服务器使用密钥将客户端上传的位置宣告信息解密, 获取其中的交易位置信息, 并将交易位置信息与位置描述信息进行比较, 在二者一致的情况下, 判定交易位置信息所表示的位置为可信位置。如果二者一致, 例如, 用户的当前交易位置是已经登记或记录的历史交易位置(可信位置), 则启动用户正常登录流程, 相反, 在二者不一致的情况下, 例如, 用户的当前交易位置是一个未登记或记录的位置(非可信位置), 则服务器可以提示用户, 并且后续可以启动非可信环境验证流程。

[0053] 定位数据库 106 也可以连接至客户端 102, 此时, 客户端而不是服务器通过查询定位数据库获取用户的位置描述信息, 并将位置描述信息上传至服务器。之后, 服务器使用密钥将位置宣告信息解密, 获取其中的交易位置信息, 并将交易位置信息与位置描述信息进行比较, 在二者一致的情况下, 判定交易位置信息所表示的位置为可信位置。

[0054] 这样, 通过上述处理, 使得用户的位置宣告信息使用独立的安全加密模块进行加密, 以加密方式提交, 保证了位置信息的可靠性。即使黑客了解用户可信位置, 由于对位置宣告信息的安全加密, 使得伪造此信息的难度非常大。另外, 通过将当前交易位置信息和客户交易订单已有数据进行比对, 根据用户位置决定用户认证方法, 以最小的改变用户的使用习惯。此外, 服务器可以使用现有架构, 无须进行较大修改, 因此以较小的成本显著提升了系统安全性。

[0055] 设备实施例

[0056] 根据本发明的设备实施例, 提供了一种基于位置认证的电子支付设备。

[0057] 如图 2 所示, 用于实施本发明的该设备包括定位单元 202、安全加密单元 204、存储

单元 206、解密单元 208、比较单元 210。

[0058] 具体地,定位单元 202,用于获取用户交易的交易位置信息;安全加密单元 204,用于生成加密的位置宣告信息,其中,位置宣告信息包括:交易位置信息和会话标识;存储单元 206,用于存储与用户的交易记录相关的位置描述信息;解密单元 208,用于将来自安全加密单元的位置宣告信息解密;比较单元 210,用于解密单元解密的交易位置信息与存储单元中存储的位置描述信息进行比较,以验证位置宣告信息的有效性。比较单元可以直接连接至存储单元,并从中获取位置描述信息,也可以由其他部件获取存储单元中的位置描述信息,然后提交给比较单元,本发明对此没有限制。

[0059] 其中,比较单元在判断交易位置信息和位置描述信息一致的情况下,判断交易位置信息所表示的位置为可信位置,否则,判定交易位置信息所表示的位置为非可信位置。之后,服务器可以根据比较单元的比较结果启动不同的认证流程。

[0060] 其中,安全加密单元 204 对位置宣告信息进行加密的密钥由电子支付设备所在的客户端生成,并且客户端将密钥上传至服务器,或者,安全加密单元对位置宣告信息进行加密的密钥由服务器生成,并且服务器将密钥下发至电子支付设备。

[0061] 另外,在该设备中,存储单元可以独立于定位单元和安全加密单元以及解密单元和比较单元,例如,定位单元和安全加密单元位于客户端侧,而解密单元和比较单元位于服务器侧,而存储单元可以连接至服务器或客户端。

[0062] 方法实施例一

[0063] 根据本发明的方法实施例,提供了一种基于位置认证的电子支付方法。

[0064] 如图 3 所示,该方法包括以下处理:

[0065] 步骤 S302,生成用于进行加密和解密操作的密钥;

[0066] 步骤 S304,客户端的安全加密模块使用密钥生成加密的位置宣告信息,其中,位置宣告信息包括:用户的交易位置信息(可以是位置点坐标或定位标识数据)和会话标识(之前,需要客户端的定位模块首先获取交易位置信息);

[0067] 步骤 S306,客户端将加密的位置宣告信息上传至服务器;

[0068] 步骤 S308,服务器从定位数据库中查询与用户的交易记录相关的位置描述信息;

[0069] 步骤 S310,服务器使用密钥将位置宣告信息解密,并将位置描述信息与解密获得的交易位置信息进行比较,在二者一致的情况下,判定交易位置信息所表示的位置为可信位置。之后,服务器可以根据交易位置信息表示的位置是否可信选择启动不同的认证流程,例如,在可信位置的情况下,启动可信环境下的普通认证流程,在非可信位置的情况下,启动不可信环境下的加强认证流程,并且优选地反馈客户端。

[0070] 另外,上述的位置宣告信息中进一步包括时间戳,并且可以进一步包括:客户端设备标识、用户标识。

[0071] 对于密钥的生成可以有不同的方式,例如,密钥可以由客户端生成,并被上传至服务器,或者,密钥可以由服务器生成,并被下发至客户端。具体地,图 4 示出了生成密钥的详细流程。如图 4 所示,首先进行客户端初始化,之后,可以由服务器生成密钥,并且客户端通过 SSL 加密通道取得密钥,之后可以将其保存在安全加密模块中;或者,由客户端的安全加密模块生成密钥,通过客户端将该密钥通过 SSL 加密通道上传服务器,并将密钥保存在安全加密模块中。

[0072] 在该实施例中,由服务器从定位数据库中查询与用户的交易记录相关的位置描述信息,并进行与交易位置信息的比较。然而,本发明不限于此,例如,可以由客户端从定位数据库中查询与用户的交易记录相关的位置描述信息,以下的方法实施例二描述了该情况下的处理。

[0073] 方法实施例二

[0074] 根据本发明的方法实施例,还提供了另一种基于位置认证的电子支付方法。

[0075] 如图 5 所示,该方法包括以下处理:

[0076] 步骤 S502,生成用于进行加密和解密操作的密钥;

[0077] 步骤 S504,安全加密模块使用密钥生成加密的位置宣告信息,其中,位置宣告信息包括:用户的交易位置信息和会话标识(与方法实施例一类似,之前需要客户端的定位模块首先获取交易位置信息);

[0078] 步骤 S506,客户端从定位数据库中查询与用户的交易记录相关的位置描述信息,并将位置描述信息和加密的位置宣告信息上传至服务器;

[0079] 步骤 S508,服务器使用密钥将位置宣告信息解密,并将位置描述信息与解密获得的交易位置信息进行比较,在二者一致的情况下,判定交易位置信息所表示的位置为可信位置。

[0080] 与方法实施例一类似,在上述处理中,密钥由客户端生成,并被上传至服务器,或者,密钥由服务器生成,并被下发至客户端。同样,上述的位置宣告信息中进一步包括时间戳,并且可以进一步包括:客户端设备标识、用户标识。

[0081] 需要说明的是,以上系统实施例中描述的多个细节同样适用于该设备实施例和方法实施例,为了不必要的重复本发明,省略了对相同或相似部分的重复描述。

[0082] 为了更好的理解本发明,以下通过本发明的具体应用实例来进一步描述本发明的实施例,同样,给出的以下实例仅仅是示例和说明性的,而不是对本发明进行任何限制。

[0083] 图 6 给出了用户在电子商务网站进行交易的实例的具体处理流程。

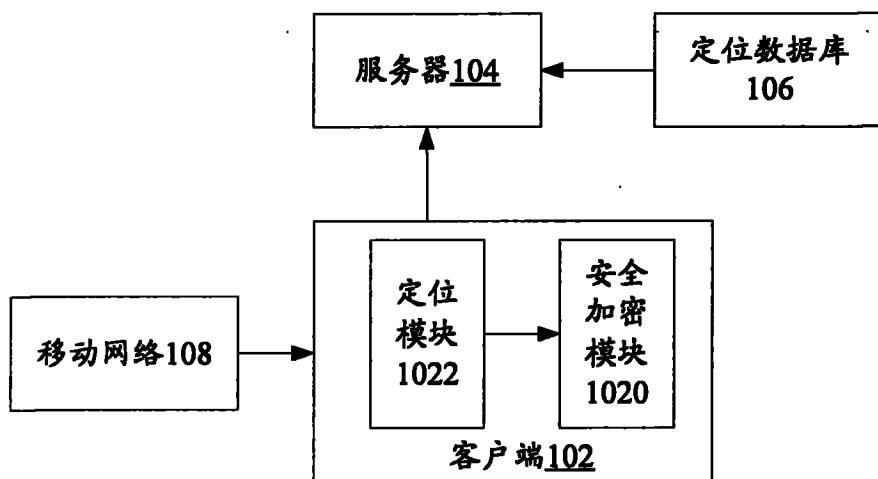
[0084] 如图 6 所示,当用户在电子商务网站上提交订单时,电子商务网站将要求客户端提交交易位置信息。

[0085] 响应于电子商务网站的上述要求,客户端将从定位模块获得位置信息,并通过安全加密模块对该位置信息进行加密。之后,客户端通过 SSL 加密通道将加密的位置信息传递到电子商务网站。

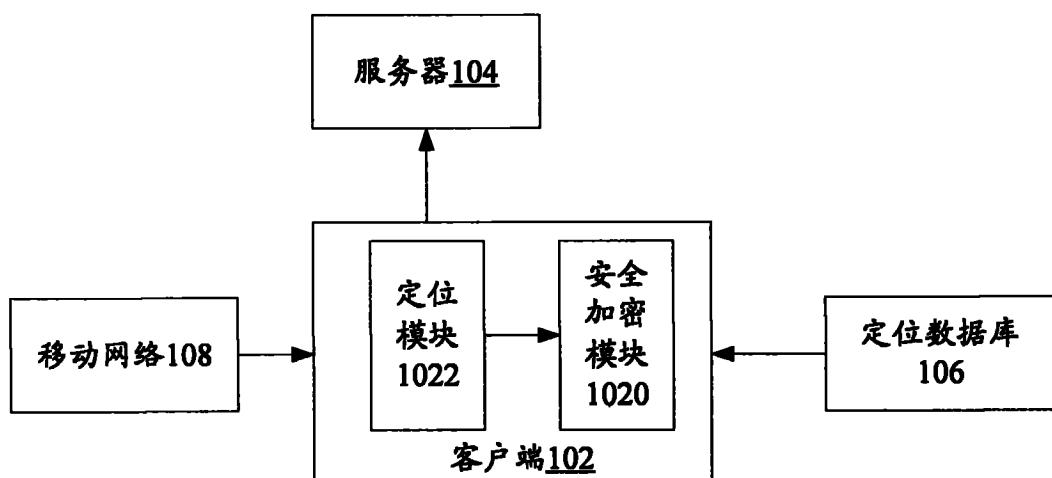
[0086] 电子商务网站根据该位置信息查询定位数据库,获得位置详细描述,并比较该位置详细描述与用户交易的位置信息的一致性,如果一致,则启动正常订单交付流程,如果不一致,则可以向用户给出密码提示问题,对用户身份进行认证,在用户认证通过的情况下,启动正常订单交付流程,否则,拒绝用户订单,并可以将欺诈交易提交给真实用户。

[0087] 通过本发明,进一步降低了电子支付服务人工验证成本,同时又增加了黑客在异地发出支付定单的难度,提高了现有技术方案的安全性,提高了用户体验。

[0088] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。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。



(a)



(b)

图 1

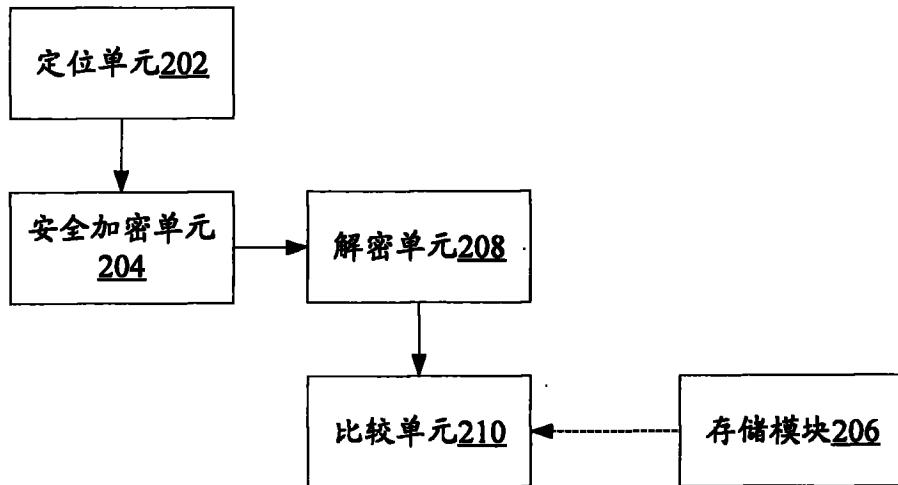


图 2

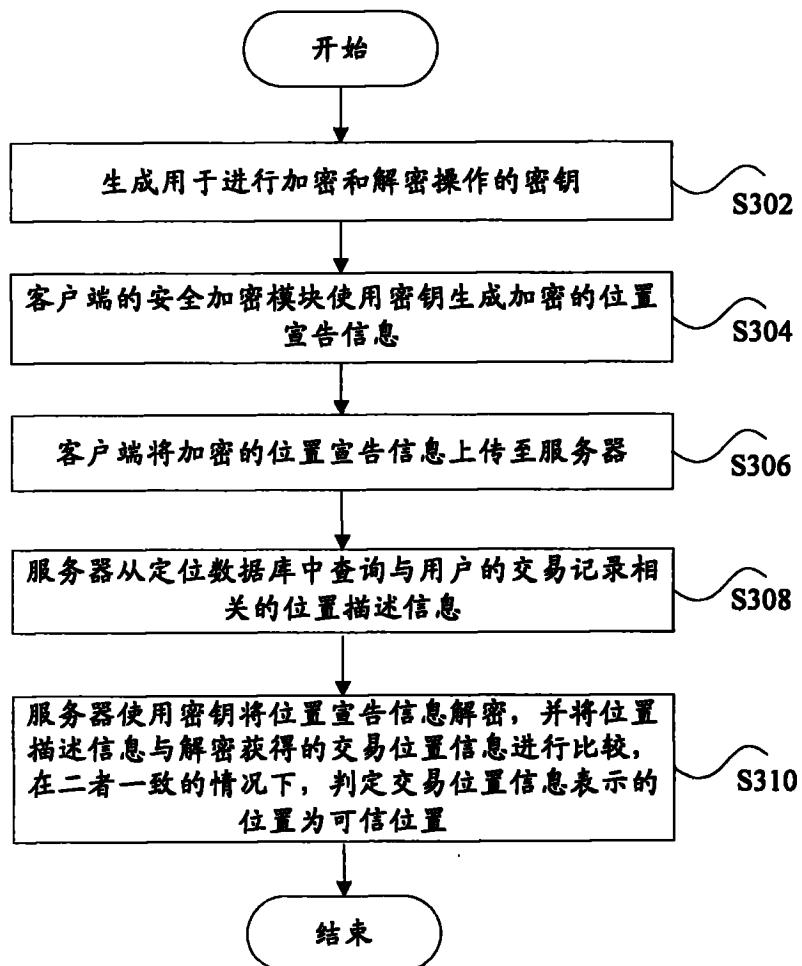


图 3

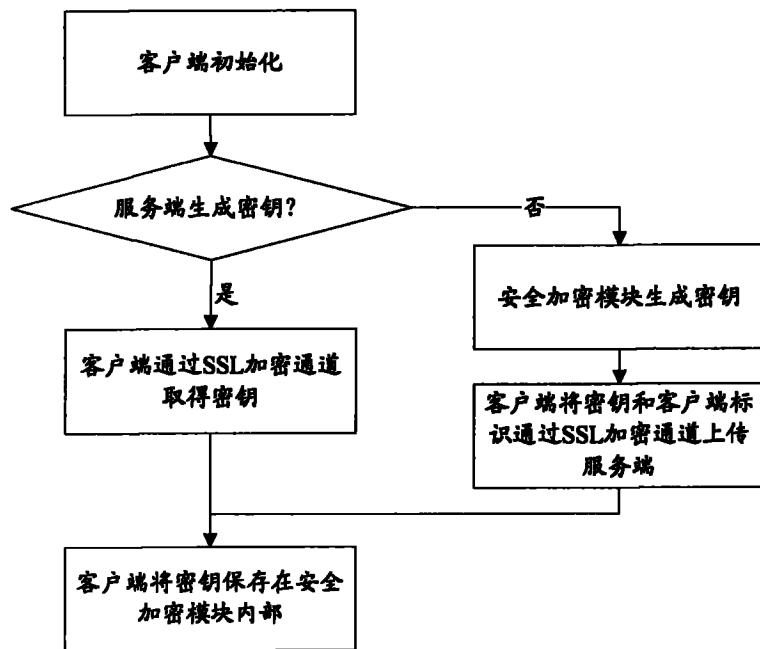


图 4

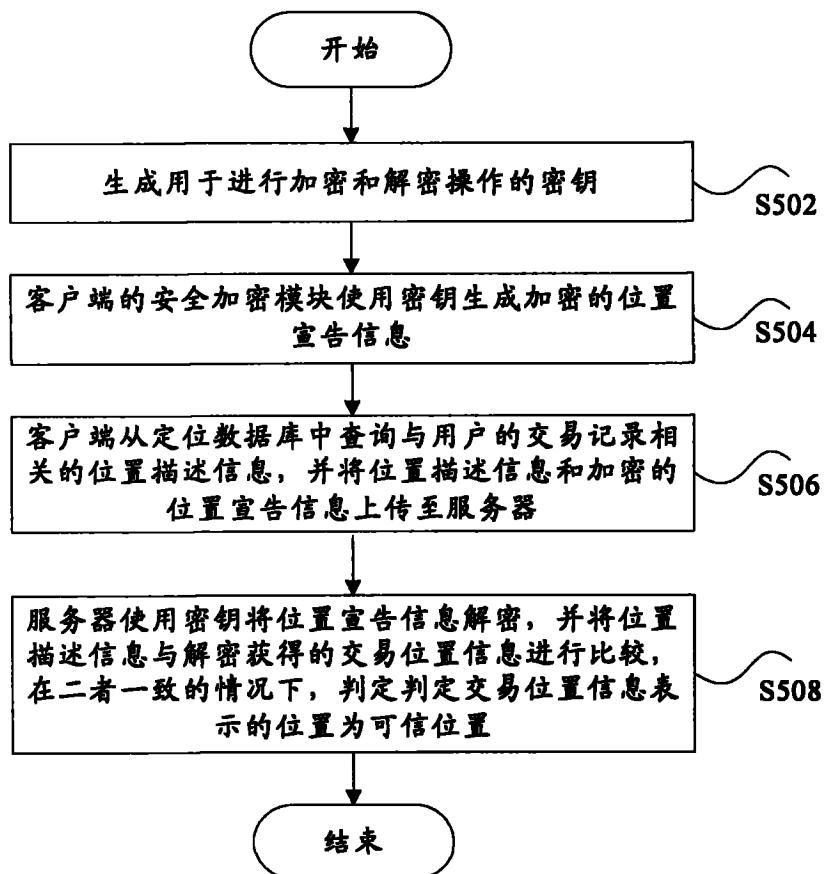


图 5

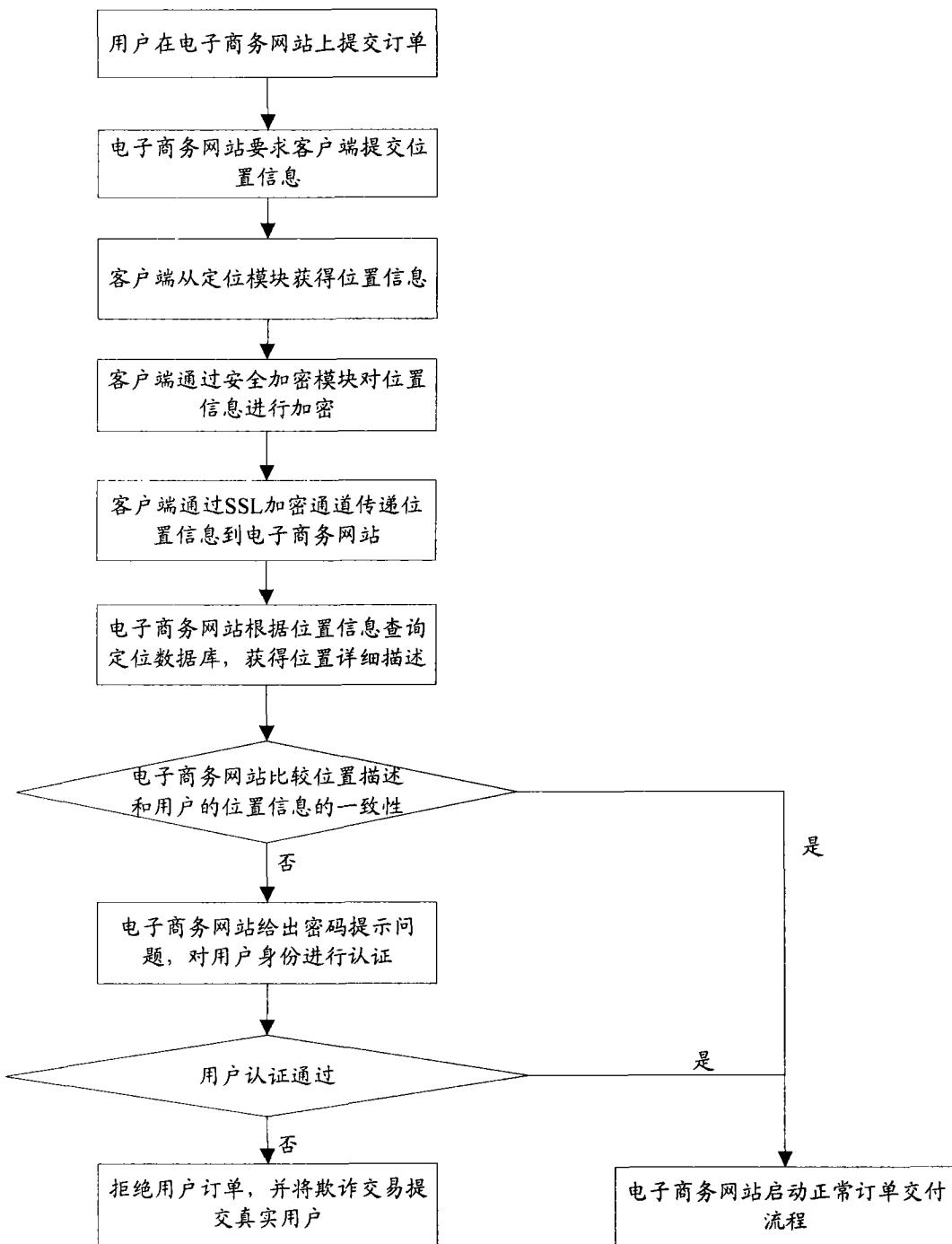


图 6