(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103035078 B
(45)授权公告日 2015.05.27

(21)申请号 201210501311.7
(22)申请日 2012.11.30
(73)专利权人 深圳天源迪科信息技术股份有限公司
地址 518000 广东省深圳市高新区南区市高新技术工业村 T3 栋 B3 楼
(72)发明人 汪东升 陈起 朱孟祥
(74)专利代理机构 深圳市德力知识产权代理事务所 44265
代理人 林才桂
(51)Int.Cl.
G07G 1/00(2006.01)

(56)对比文件
CN 101464981 A,2009.06.24, 全文 .

审查员 陈媛媛

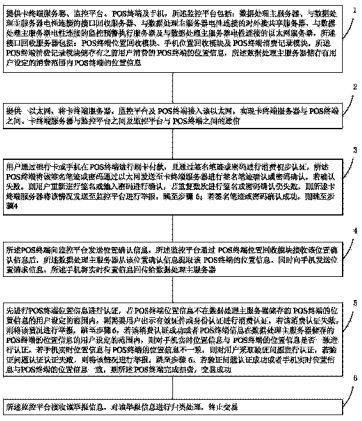
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于位置的支付安全监控方法

(57)摘要

本发明提供一种基于位置的支付安全监控方法，包括以下步骤：步骤1、提供卡终端服务器、监控平台、POS终端及手机，该监控平台包括数据处理主服务器，该数据处理主服务器储存有用户设定的消费范围内POS终端的位置信息；步骤2、提供一以太网，将卡终端服务器、监控平台及POS终端接入该以太网；步骤3、用户通过POS终端进行刷卡付款，并完成初步认证；步骤4、该数据处理主服务器提取POS终端的位置信息，同时获取手机实时位置信息；步骤5、先对POS终端进行位置信息认证，再对手机实时位置信息与POS终端的位置信息是否一致进行认证，若POS位置信息认证成功，且手机实时位置信息与POS终端的位置信息一致，则进行交易。



CN 103035078 B

1. 一种基于位置的支付安全监控方法，其特征在于，包括以下步骤：

步骤 1、提供卡终端服务器、监控平台、POS 终端及手机，所述监控平台包括：数据处理主服务器、与数据处理主服务器电性连接的接口回收服务器、与数据处理主服务器电性连接的对外接共享服务器、与数据处理主服务器电性连接的监控预警执行服务器及与数据处理主服务器电性连接的以太网服务器，所述接口回收服务器包括：POS 终端位置回收模块、手机位置回收模块及 POS 终端消费记录模块，所述 POS 终端消费记录模块储存有之前用户消费的 POS 终端的位置信息，所述数据处理主服务器储存有用户设定的消费范围内 POS 终端的位置信息；

步骤 2、提供一以太网，将卡终端服务器、监控平台及 POS 终端接入该以太网，实现卡终端服务器与 POS 终端之间、卡终端服务器与监控平台之间及监控平台与 POS 终端之间的通信；

步骤 3、用户通过银行卡或手机在 POS 终端进行刷卡付款，且通过签名笔迹或密码进行消费初步认证，所述 POS 终端将该签名笔迹或密码通过以太网发送至卡终端服务器进行签名笔迹确认或密码确认，若确认失败，则用户重新进行签名或输入密码进行确认，若重复数次进行签名或密码确认仍失败，则所述卡终端服务器将该情况发送至监控平台进行举报，跳至步骤 6；若签名笔迹或密码确认成功，则跳至步骤 4；

步骤 4、所述 POS 终端向监控平台发送位置确认信息，所述监控平台通过 POS 终端位置回收模块接收该位置确认信息后，所述数据处理主服务器从该位置确认信息提取该 POS 终端的位置信息，同时向手机发送位置请求信息，所述手机将实时位置信息回传给数据处理主服务器；

步骤 5、先进行 POS 终端位置信息的认证，若 POS 终端位置信息不在数据处理主服务器储存的 POS 终端的位置信息的用户设定的范围内，则需要用户出示有效证件或身份认证进行消费认证，若该消费认证失败，则将该情况进行举报，跳至步骤 6，若该消费认证成功或者 POS 终端位置信息在数据处理主服务器储存的 POS 终端的位置信息的用户设定的范围内，则对手机实时位置信息与 POS 终端的位置信息是否一致进行认证，若手机实时位置信息与 POS 终端的位置信息不一致，则对用户采取验证问题进行认证，若验证问题认证失败，则将该情况进行举报，跳至步骤 6，若验证问题认证成功或者手机实时位置信息与 POS 终端的位置信息一致，则所述 POS 终端完成扣费，交易成功；

步骤 6、所述监控平台接收该举报信息，对该举报信息进行归类处理，终止交易。

2. 如权利要求 1 所述的基于位置的支付安全监控方法，其特征在于，所述监控平台的手机位置回收模块重复获取用户的运动轨迹并保存。

3. 如权利要求 1 所述的基于位置的支付安全监控方法，其特征在于，所述监控平台中的数据处理主服务器储存有所有 POS 终端位置信息。

4. 如权利要求 3 所述的基于位置的支付安全监控方法，其特征在于，所述用户对监控平台中数据处理主服务器储存的所有 POS 终端位置信息进行区域范围划分，划分为红名单区域及黑名单区域。

5. 如权利要求 1 所述的基于位置的支付安全监控方法，其特征在于，所述手机实时位置信息与 POS 终端的位置信息是否一致指的是手机与 POS 终端两者的位置距离是否在合理范围内。

6. 如权利要求 1 所述的基于位置的支付安全监控方法，其特征在于，所述手机包括：第一处理模块、与第一处理模块电性连接的定位模块及与第一处理模块电性连接的无线通信模块。

7. 如权利要求 6 所述的基于位置的支付安全监控方法，其特征在于，所述步骤 4 中手机通过定位模块采用 GPS 或者信令进行实时定位，并将实时位置信息通过无线通信模块发送至手机位置回收模块。

8. 如权利要求 1 所述的基于位置的支付安全监控方法，其特征在于，所述步骤 6 包括以下步骤：

步骤 6.1、所述监控平台接收该举报信息，对该举报信息进行归类处理；

步骤 6.2、所述监控平台再次对用户身份进行确认；

步骤 6.3、若确认成功，则进行交易；若确认失败，则终止交易，并进行信息不完整反馈。

9. 如权利要求 8 所述的基于位置的支付安全监控方法，其特征在于，所述步骤 6.1 中的举报信息的类别包括：POS 终端位置信息不对、用户信息被盗、信用卡非法套现及手机网络登记信息不实。

10. 如权利要求 8 所述的基于位置的支付安全监控方法，其特征在于，所述步骤 6.2 中通过用户出示有效证件或身份认证、验证问题对用户身份进行确认。

基于位置的支付安全监控方法

技术领域

[0001] 本发明涉及人们日常生活密切相关的在线支付及现场支付领域，尤其涉及一种利用支付人的位置、支付位置及账号来判断支付业务的合法性的支付安全监控方法。

背景技术

[0002] 移动互联网，就是将移动通信和互联网二者结合起来，成为一体。移动通信和互联网成为当今世界发展最快、市场潜力最大、前景最诱人的两大业务，它们的增长速度都是任何预测家未曾预料到的，所以移动互联网可以预见将会创造经济神话。

[0003] 随着移动互联网的诞生及其蓬勃发展，让在线支付、现场支付业务成为人们日常生活最紧密的事情之一，人们购物不再需要携带大量的现金在身上，出行方便，安全，而且还可以网上购物，节省逛商场及店铺的时间。但是现行在线支付及现场支付业务存在以下形式：a、银行卡现场刷卡 b、手机卡现场支付 c、账号在线支付。

[0004] 目前的持卡现场支付的方式是人持卡在商场、服务机构等 POS 机上刷卡，并输入密码或者是手写笔迹认知来进行消费。该种账号安全管理与模式存在以下安全漏洞：

[0005] (1) 笔迹认证具有模糊性和人为因素在，难以精确控制，模仿笔迹或者工作疏忽导致的账号盗用情况时有发生；

[0006] (2) 密码认证存在被恶意商家记录或者破解的可能，并且目前案例不在少数。

[0007] 为了解决上述安全漏洞，现行的解决方法是通过每笔消费进行短信通知方式来确保账号消费的安全，但此种方式属于后知后觉的方式，并且短信的提醒受制于手机接收条件的影响存在不及时的问题，主要是当被盗用发生后才知道，无法在被盗用前做出预防措施。

发明内容

[0008] 本发明的目的在于提供一种基于位置的支付监控方法，解决现有在线支付、现场 POS 机支付存在的安全问题，保障在线支付、现场 POS 机支付的安全。

[0009] 为实现上述目的，本发明提供一种基于位置的支付安全监控方法，包括以下步骤：

[0010] 步骤 1、提供卡终端服务器、监控平台、POS 终端及手机，所述监控平台包括：数据处理主服务器、与数据处理主服务器电性连接的接口回收服务器、与数据处理主服务器电性连接的对外接共享服务器、与数据处理主服务器电性连接的监控预警执行服务器及与数据处理主服务器电性连接的以太网服务器，所述接口回收服务器包括：POS 终端位置回收模块、手机位置回收模块及 POS 终端消费记录模块，所述 POS 终端消费记录模块储存有之前用户消费的 POS 终端的位置信息，所述数据处理主服务器储存有用户设定的消费范围内 POS 终端的位置信息；

[0011] 步骤 2、提供一以太网，将卡终端服务器、监控平台及 POS 终端接入该以太网，实现卡终端服务器与 POS 终端之间、卡终端服务器与监控平台之间及监控平台与 POS 终端之间

的通信；

[0012] 步骤3、用户通过银行卡或手机在POS终端进行刷卡付款，且通过签名笔迹或密码进行消费初步认证，所述POS终端将该签名笔迹或密码通过以太网发送至卡终端服务器进行签名笔迹确认或密码确认，若确认失败，则用户重新进行签名或输入密码进行确认，若重复数次进行签名或密码确认仍失败，则所述卡终端服务器将该情况发送至监控平台进行举报，跳至步骤6；若签名笔迹或密码确认成功，则跳至步骤4；

[0013] 步骤4、所述POS终端向监控平台发送位置确认信息，所述监控平台通过POS终端位置回收模块接收该位置确认信息后，所述数据处理主服务器从该位置确认信息提取该POS终端的位置信息，同时向手机发送位置请求信息，所述手机将实时位置信息回传给数据处理主服务器；

[0014] 步骤5、先进行POS终端位置信息进行认证，若POS终端位置信息不在数据处理主服务器储存的POS终端的位置信息的用户设定的范围内，则需要用户出示有效证件或身份认证进行消费认证，若该消费认证失败，则将该情况进行举报，跳至步骤6，若该消费认证成功或者POS终端位置信息在数据处理主服务器储存的POS终端的位置信息的用户设定的范围内，则对手机实时位置信息与POS终端的位置信息是否一致进行认证，若手机实时位置信息与POS终端的位置信息不一致，则对用户采取验证问题进行认证，若验证问题认证认证失败，则将该情况进行举报，跳至步骤6，若验证问题认证成功或者手机实时位置信息与POS终端的位置信息一致，则所述POS终端完成扣费，交易成功；

[0015] 步骤6、所述监控平台接收该举报信息，对该举报信息进行归类处理，终止交易。

[0016] 所述监控平台的手机位置回收模块重复获取用户的运动轨迹并保存。

[0017] 所述监控平台中的数据处理主服务器储存有所有POS终端位置信息。

[0018] 所述用户对监控平台中数据处理主服务器储存的所有POS终端位置信息进行区域范围划分，划分为红名单区域及黑名单区域。

[0019] 所述手机实时位置信息与POS终端的位置信息是否一致指的是手机与POS终端两者的位置距离是否在合理范围内。

[0020] 所述手机包括：第一处理模块、与第一处理模块电性连接的定位模块及与第一处理模块电性连接的无线通信模块。

[0021] 所述步骤4中手机通过定位模块采用GPS或者信令进行实时定位，并将实时位置信息通过无线通信模块发送至手机位置回收模块。

[0022] 所述步骤6包括以下步骤：

[0023] 步骤6.1、所述监控平台接收该举报信息，对该举报信息进行归类处理；

[0024] 步骤6.2、所述监控平台再次对用户身份进行确认；

[0025] 步骤6.3、若确认成功，则进行交易；若确认失败，则终止交易，并进行信息不完整反馈。

[0026] 所述步骤6.1中的举报信息的类别包括：POS终端位置信息不对、用户信息被盗、信用卡非法套现及手机网络登记信息不实。

[0027] 所述步骤6.2中通过用户出示有效证件或身份认证、验证问题对用户身份进行确认。

[0028] 本发明的有益效果：本发明基于位置的支付监控方法通过监控平台对POS终端进

行收集管理，并划分红黑名单区域，并在后续消费过程中进行对 POS 终端的位置信息进行认证，再通过判断用户身上的手机与 POS 终端的距离是否在合理范围内，从而完成交易认证，在现有的密码认证及签名笔迹认证的基础上，加入了位置信息的确认，操作简单方便，性能可靠，充分利用了移动互联网、支付业务、位置服务、云计算等行业的发展成果，对未来银行卡支付、在线支付提供了安全保障，让用户消费更放心，彻底解决当前信用卡被盗用、手机账号被盗用的问题，同时也能帮助管理机构发现用户的恶意行为，如：信用卡违规套现等。

[0029] 为了能更进一步了解本发明的特征以及技术内容，请参阅以下有关本发明的详细说明与附图，然而附图仅提供参考与说明用，并非用来对本发明加以限制。

附图说明

[0030] 下面结合附图，通过对本发明的具体实施方式详细描述，将使本发明的技术方案及其它有益效果显而易见。

[0031] 附图中，

[0032] 图 1 为本发明基于位置的支付安全监控方法的框架流程图；

[0033] 图 2 为应用本发明基于位置的支付安全监控方法的系统组成示意图；

[0034] 图 3 为本发明基于位置的支付安全监控方法的工作流程图。

具体实施方式

[0035] 为更进一步阐述本发明所采取的技术手段及其效果，以下结合本发明的优选实施例及其附图进行详细描述。

[0036] 请参阅图 1 至 3，本发明提供一种基于位置的支付安全监控方法，将账号认证、笔迹认证、密码认证、位置验证集于一身，形成一基于位置支付安全监控系统，该系统采用 GPRS 技术、海量数据分析技术进行数据传输及数据处理。该方法包括以下步骤：

[0037] 步骤 1、提供卡终端服务器 20、监控平台 40、POS 终端 60 及手机 80，所述监控平台 40 包括：数据处理主服务器 42、与数据处理主服务器 42 电性连接的接口回收服务器 44、与数据处理主服务器 42 电性连接的对外接共享服务器 46、与数据处理主服务器 42 电性连接的监控预警执行服务器 47 及与数据处理主服务器 42 电性连接的以太网服务器 48，所述接口回收服务器 44 包括：POS 终端位置回收模块 442、手机位置回收模块 444 及 POS 终端消费记录模块 446，所述 POS 终端消费记录模块 446 储存有之前用户消费的 POS 终端的位置信息及用户设定的消费范围内 POS 终端的位置信息；

[0038] 该卡终端服务器 20 为银行储存用户信息的总服务器，通过该卡终端服务器 20 可以对用户身份信息、用户的银行卡账号及其对应的密码及签名笔迹进行认证，使得该方法支持线性的密码认证、签名认证，使交易认证方式可以平滑过渡，降低对该使用该方法进行交易确认的培训成本。

[0039] 所述数据处理主服务器 42 对各种位置信息及认证问题进行处理，协助完成整个交易过程；所述接口回收服务器 44 用于回收手机 80、POS 终端 60 的位置信息，对手机 80 的实时位置及用户常去的位置进行分类保存；所述对外接共享服务器 46 用于外接数据线，利用外部设备透过该对外共享服务器 46 查看位置信息及对认证问题进行设置，进而达到共

享数据库的目的；所述监控预警执行服务器47用于当POS终端60、手机（用户实时位置）80及用户设定的消费范围内POS终端的位置信息不一致时，进行举报处理；所述以太网服务器48用于与以太网90进行交互，实现信息的传递。所述监控平台40的POS终端位置回收模块442用于收集所有POS终端60的位置信息并发送给数据处理主服务器42，同时可以获取当前交易的POS终端的位置信息，所述手机位置回收模块444重复获取用户的运动轨迹及实时获取手机80的实时位置信息，所述POS终端消费记录模块446用于记录银行卡成功交易的POS终端60的位置信息及用户设定的消费范围内POS终端60的位置信息，从而得出用户经常消费的POS终端60的位置信息。所述监控平台40中的数据处理主服务器42储存有所有POS终端60位置信息，利用该POS终端位置回收模块442、手机位置回收模块444及POS终端消费记录模块446可以快速对监控平台40中储存的所有POS终端60位置信息进行区域范围划分，划分为红名单区域及黑名单区域，所述红名单区域则为安全消费区域，黑名单区域则为需认证才能交易区域。这就可以在用户消费交易时，增加位置信息的认证，利用多样化的认证方式，特别是历史位置的确认，可以回避账号被盗用的现象。

[0040] 所述手机80包括：第一处理模块82、与第一处理模块82电性连接的定位模块86及与第一处理模块82电性连接的无线通信模块84。该第一处理模块82用于下发控制指令及进行数据处理；该定位模块86用于进行实时定位，该手机80用户随身携带，进而可以获取用户往常的行动轨迹，每时每刻定位用户所在的位置，同时也可以获取用户交易时刻的实时位置信息，协助完成整个交易过程，该定位模块86的定位方式为GPS定位方式或者信令定位方式；所述无线通信模块84用于实现该手机80与监控平台40的无线通信，两者之间的通信还可以通过中转基站进行信息转发。所述监控平台40还包括一主题挖掘服务器49。

[0041] 步骤2、提供一以太网90，将卡终端服务器20、监控平台40及POS终端60接入该以太网90，实现卡终端服务器20与POS终端60之间、卡终端服务器20与监控平台40之间及监控平台40与POS终端60之间的通信；

[0042] 通过该以太网90为卡终端服务器20、监控平台40及POS终端60三者实现信息交互提供平台，快速完成通信。

[0043] 步骤3、用户通过银行卡或手机在POS终端进行刷卡付款（101），且通过签名笔迹或密码进行消费初步认证（103），所述POS终端60将该签名笔迹或密码通过以太网90发送至卡终端服务器20进行签名笔迹确认或密码确认（102），若确认失败，则用户重新进行签名或输入密码进行确认，若重复数次进行签名或密码确认仍失败，则所述卡终端服务器20将该情况发送至监控平台40进行举报，跳至步骤6；若签名笔迹或密码确认成功，则跳至步骤4；

[0044] 在该步骤中，重复进行签名或密码确认的次数优选为3次，利用现有的签名笔迹确认或密码确认来完成交易的初步身份确认，若用户输入的签名笔迹或密码不对，则进行监控举报。

[0045] 步骤4、所述POS终端60向监控平台40发送位置确认信息，所述监控平台40通过POS终端位置回收模块442接收该位置确认信息后，所述数据处理主服务器42从该位置确认信息提取该POS终端60的位置信息，同时向手机80发送位置请求信息，所述手机80将实时位置信息回传给数据处理主服务器42；

[0046] 在本步骤中手机 80 通过定位模块 86 采用 GPS 或者信令进行实时定位，并将实时位置信息通过无线通信模块 84 发送至手机位置回收模块 444。

[0047] 所述数据处理主服务器 42 对手机 80 实时位置信息、POS 终端 60 的位置信息及数据处理主服务器 42 储存的用户设定的消费范围内 POS 终端 60 的位置信息进行处理。

[0048] 步骤 5、先进行 POS 终端 60 位置信息进行认证 (104)，若 POS 终端 60 位置信息不在数据处理主服务器 42 储存的 POS 终端 60 的位置信息的用户设定的范围内，则需要用户出示有效证件或身份认证进行消费认证，若该消费认证认证失败，则将该情况进行举报，跳至步骤 6，若该消费认证认证成功或者 POS 终端 60 位置信息在数据处理主服务器 42 储存的 POS 终端 60 的位置信息的用户设定的范围内，则对手机 80 实时位置信息与 POS 终端 60 的位置信息是否一致 (112)，若手机 80 实时位置信息与 POS 终端 60 的位置信息不一致，则对用户采取验证问题进行认证 (111)，若验证问题认证失败，则将该情况进行举报，跳至步骤 6，若验证问题认证成功或者手机 80 实时位置信息与 POS 终端 69 的位置信息一致 (105)，则所述 POS 终端 60 完成扣费，交易成功 (106)；

[0049] 在经过用户签名笔迹或输入的密码确认后，再进行 POS 终端 60 位置信息是否在数据处理主服务器 42 储存的 POS 终端 60 的位置信息的用户设定的范围（即红名单范围）内进行确认 (104)，若 POS 终端 60 位置信息不在数据处理主服务器 42 储存的 POS 终端 60 的位置信息的用户设定的范围内，无论手机 80 的实时位置信息是否与 POS 终端 60 的位置信息一致，均需要用户出示有效证件或身份认证进行消费确认，若该消费认证确认失败，则将该情况进行举报，若该消费认证确认成功或 POS 终端 69 位置信息在数据处理主服务器 42 储存的 POS 终端 60 的位置信息的用户设定的范围内，则进行下一步确认，对手机 80 实时位置信息与 POS 终端 60 的位置信息是否一致进行认证，若手机 80 实时位置信息与 POS 终端 60 的位置信息不一致，则对用户采取验证问题进行认证 (111)，若验证问题认证失败，则将该情况进行举报，若验证问题认证成功或者手机 80 实时位置信息与 POS 终端 69 的位置信息一致 (105)，则所述 POS 终端 60 完成扣费，交易成功 (106)。这极大提高了交易的安全。

[0050] 在本较佳实施例中，所述手机 80 实时位置信息与 POS 终端 60 的位置信息是否一致指的是手机 80 与 POS 终端 60 两者的位置相距的距离是否在合理范围内，优选两者的距离在 20 米范围内。所述认证问题包括：用户常住地、最近消费的地方或该银行卡常用地等。

[0051] 步骤 6、所述监控平台 40 接收该举报信息 (107)，对该举报信息进行归类处理，终止交易 (110)。

[0052] 在本步骤中，是对举报信息的处理，其具体包括以下步骤：

[0053] 步骤 6.1、所述监控平台 40 接收该举报信息 (107)，对该举报信息进行归类处理；

[0054] 所述举报信息的类别包括：POS 终端 60 位置信息不对、用户信息被盗、信用卡非法套现及手机网络登记信息不实等，对该些举报信息进行归类整理，分别对银行卡的监控。

[0055] 步骤 6.2、所述监控平台 40 再次对用户身份进行确认 (109)；

[0056] 通过用户出示有效证件或身份认证、验证问题等对用户身份进行确认，其中，所述认证问题包括：用户常住地、该银行卡消费常用地及上次刷卡消费的地点等，该些认证问题与用户密切相关的，用户很容易就回答正确，因而很容易正确地辨认到用户的身份信息。

[0057] 步骤 6.3、若确认成功，则进行交易；若确认失败，则终止交易 (110)，并进行信息不完整反馈 (108)。

[0058] 用户每进行一次POS消费，都需要进行上述步骤1至步骤6，实现签名笔迹确认或密码确认、及位置信息的确认，安全可靠。

[0059] 该方法采用在密码认证或签名笔迹认证的基础上，对用户位置信息（手机80实时位置信息）及POS终端60的位置信息进行认证，具体地对POS终端60进行统一的管理与认证，并利用云技术（HADOOP）将用户每笔的消费进行记录、每天的行动轨迹进行记录，建立有效性模型，对POS终端60与人的位置进行核对，从而完成消费交易，很好地解决了用户密码验证之外的签字认证无规范可依的问题，解决了使用银行卡、手机账号消费过程中遇到的盗刷、非法套现问题。

[0060] 综上所述，本发明提供一种基于位置的支付监控方法，通过监控平台对POS终端进行收集管理，并划分红黑名单区域，并在后续消费过程中进行对POS终端的位置信息进行认证，再判断用户身上的手机与POS终端的距离是否在合理范围内，从而完成交易认证，在现有的密码认证及签名笔迹认证的基础上，加入了位置信息的确认，操作简单方便，性能可靠，充分利用了移动互联网、支付业务、位置服务、云计算等行业的发展成果，对未来银行卡支付、在线支付提供了安全保障，让用户消费更放心，彻底解决当前信用卡被盗用、手机账号被盗用的问题，同时也能帮助管理机构发现用户的恶意行为，如：信用卡违规套现等。

[0061] 以上所述，对于本领域的普通技术人员来说，可以根据本发明的技术方案和技术构思作出其他各种相应的改变和变形，而所有这些改变和变形都应属于本发明权利要求的保护范围。


提供卡终端服务器、监控平台、POS终端及手机，所述监控平台包括：数据处理主服务器、与数据处理主服务器电性连接的接口回收服务器、与数据处理主服务器电性连接的对外接共享服务器、与数据处理主服务器电性连接的监控预警执行服务器及与数据处理主服务器电性连接的以太网服务器，所述接口回收服务器包括：POS终端位置回收模块、手机位置回收模块及POS终端消费记录模块，所述POS终端消费记录模块储存有之前用户消费的POS终端的位置信息，所述数据处理主服务器储存有用户设定的消费范围内POS终端的位置信息
1
提供一以太网，将卡终端服务器、监控平台及POS终端接入该以太网，实现卡终端服务器与POS终端之间、卡终端服务器与监控平台之间及监控平台与POS终端之间的通信
2
用户通过银行卡或手机在POS终端进行刷卡付款，且通过签名笔迹或密码进行消费初步认证，所述POS终端将该签名笔迹或密码通过以太网发送至卡终端服务器进行签名笔迹确认或密码确认，若确认失败，则用户重新进行签名或输入密码进行确认，若重复数次进行签名或密码确认仍失败，则所述卡终端服务器将该情况发送至监控平台进行举报，跳至步骤6；若签名笔迹或密码确认成功，则跳至步骤4
3
所述POS终端向监控平台发送位置确认信息，所述监控平台通过POS终端位置回收模块接收该位置确认信息后，所述数据处理主服务器从该位置确认信息提取该POS终端的位置信息，同时向手机发送位置请求信息，所述手机将实时位置信息回传给数据处理主服务器
4
先进行POS终端位置信息进行认证，若POS终端位置信息不在数据处理主服务器储存的POS终端的位置信息的用户设定的范围内，则需要用户出示有效证件或身份认证进行消费认证，若该消费认证失败，则将该情况进行举报，跳至步骤6，若该消费认证成功或者POS终端信息在数据处理主服务器储存的POS终端的位置信息的用户设定的范围内，则对手机实时位置信息与POS终端的位置信息是否一致进行认证，若手机实时位置信息与POS终端的位置信息不一致，则对用户采取验证问题进行认证，若验证问题认证认证失败，则将该情况进行举报，跳至步骤6，若验证问题认证成功或者手机实时位置信息与POS终端的位置信息一致，则所述POS终端完成扣费，交易成功
5
所述监控平台接收该举报信息，对该举报信息进行归类处理，终止交易
6

图 1

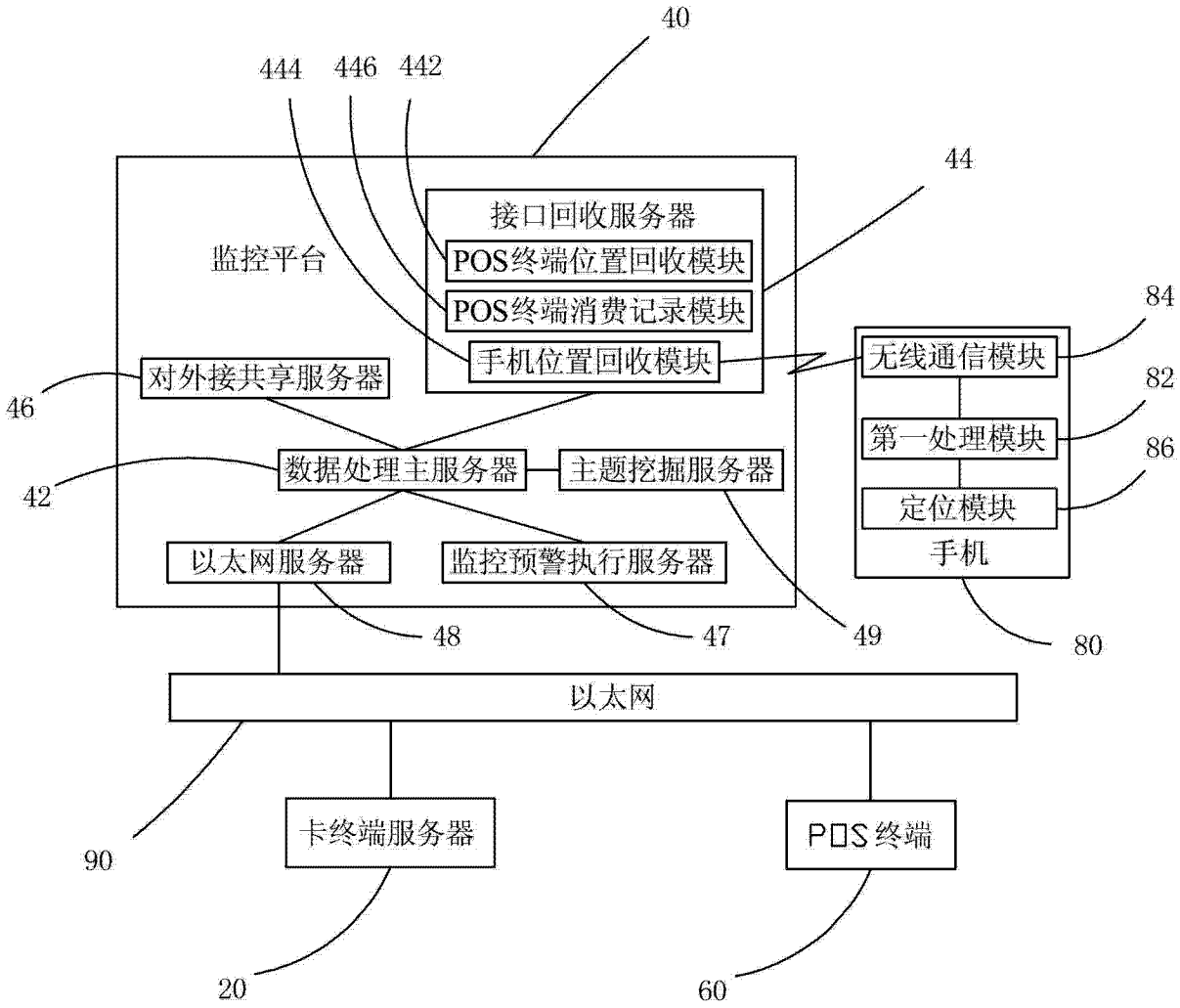

40
444
446
442
44
监控平台
接口回收服务器
POS终端位置回收模块
POS终端消费记录模块
手机位置回收模块
84
无线通信模块
82
第一处理模块
86
定位模块
手机
46
对外接共享服务器
42
数据处理主服务器
主题挖掘服务器
以太网服务器
监控预警执行服务器
48
47
49
80
以太网
90
卡终端服务器
POS终端
20
60

图 2

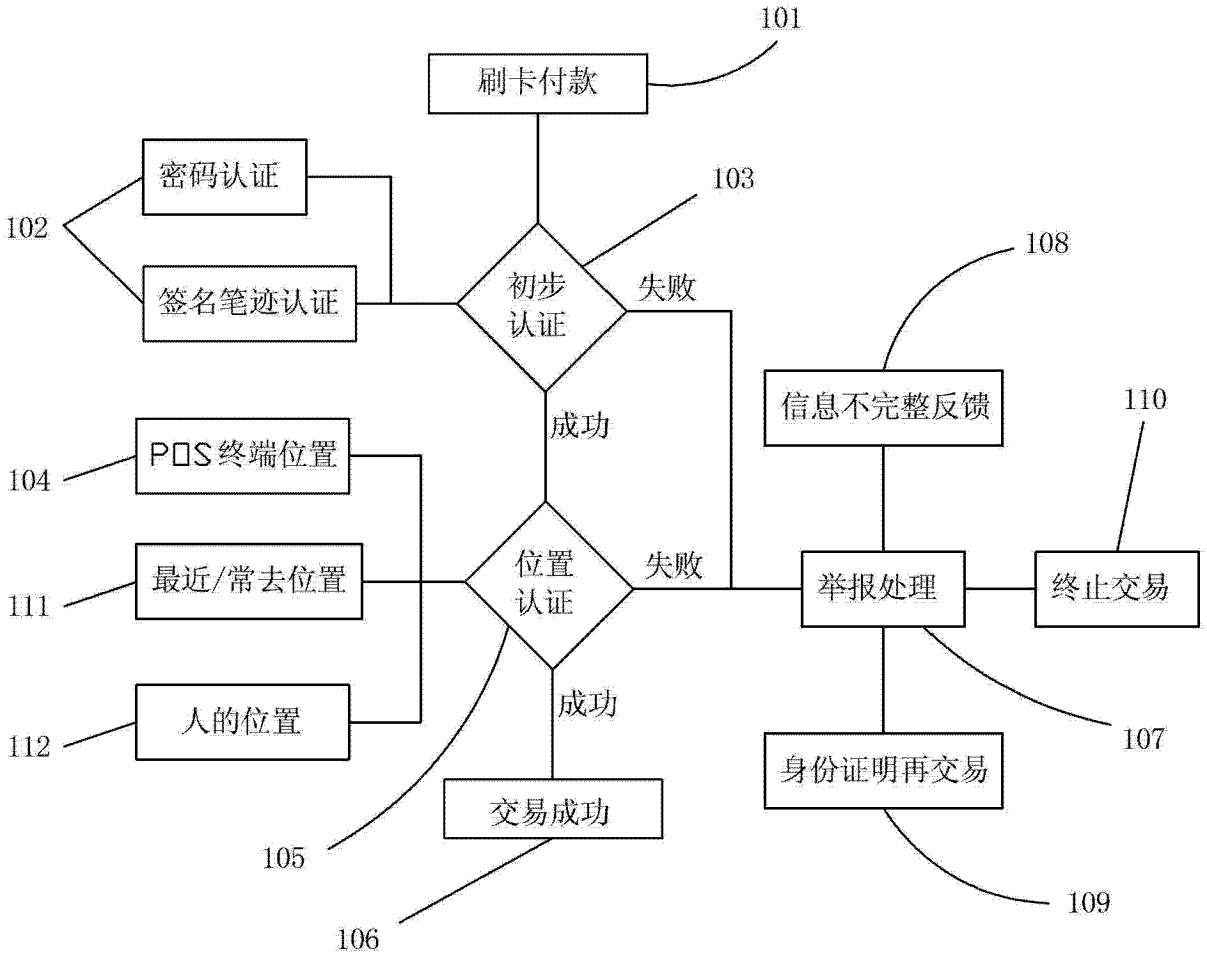

101
刷卡付款
密码认证
102
签名笔迹认证
初步
认证
103
失败
108
信息不完整反馈
110
成功
POS终端位置
104
最近/常去位置
111
人的位置
112
位置
认证
失败
举报处理
终止交易
成功
107
身份证明再交易
交易成功
105
109
106

图 3