



(12)发明专利申请

(10)申请公布号 CN 106952096 A

(43)申请公布日 2017.07.14

(21)申请号 201710122559.5

(22)申请日 2017.03.03

(71)申请人 中国工商银行股份有限公司

地址 100140 北京市西城区复兴门内大街
55号

(72)发明人 陈俊清 舒文字 高峰 葛睿彬

(74)专利代理机构 北京三友知识产权代理有限公司 11127

代理人 王涛

(51)Int.Cl.

G06Q 20/40(2012.01)

H04L 29/06(2006.01)

权利要求书5页 说明书13页 附图4页

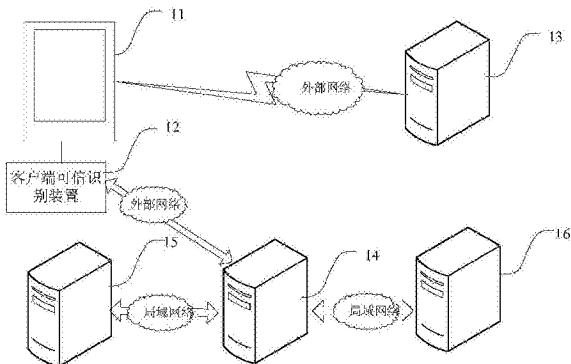
(54)发明名称

客户端设备的安全认证系统、方法及客户端
可信识别装置

(57)摘要

本发明提供了一种客户端设备的安全认证系
统、方法及客户端可信识别装置，涉及客户端
安全认证技术领域。方法包括：客户端可信识别
装置采集客户端设备的指纹要素信息，生成认证
信息；认证服务器设备解析认证信息，向指纹特
征库设备发送匹配请求；指纹特征库设备查询客
户身份标识对应的各客户历史设备指纹信息，确
定认证信息与各客户历史设备的匹配度；认证服
务器设备根据匹配度中的最大值确定客户端设
备的认证状态；在认证状态为认证成功时，向客
户端可信识别装置发送客户身份标识以及可信
标识；在认证状态为待认证状态时，根据客户认
证信息库设备进行新设备可信认证；以使得交易
应用服务器设备根据客户端设备认证结果，对交
易会话请求进行处理。

A CN 106952096



CN

1. 一种客户端设备的安全认证系统，其特征在于，包括：客户端设备、客户端可信识别装置、交易应用服务器设备、认证服务器设备、指纹特征库设备、客户认证信息库设备；所述客户端设备与所述客户端可信识别装置连接；所述客户端设备通过外部网络与所述交易应用服务器设备通信连接；所述客户端可信识别装置通过外部网络与所述认证服务器设备通信连接；所述认证服务器设备通过局域网络分别与所述指纹特征库设备和客户认证信息库设备通信连接；

所述客户端可信识别装置，用于监测客户端设备，并在监测到客户端设备向所述交易应用服务器设备发送交易会话请求时，采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息，将所述认证信息发送到所述认证服务器设备；

所述认证服务器设备，用于解析所述认证信息，并向所述指纹特征库设备发送匹配请求；

所述指纹特征库设备，用于查询所述客户身份标识对应的各客户历史设备指纹信息，并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配，确定所述认证信息与各客户历史设备的匹配度，并将各匹配度中的最大值发送给所述认证服务器设备；

所述认证服务器设备，还用于根据所述匹配度中的最大值确定客户端设备的认证状态；在所述认证状态为认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在所述认证状态为待认证状态时，根据客户认证信息库设备进行新设备可信认证；在新设备可信认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在新设备可信认证失败时，向所述客户端可信识别装置发送所述客户身份标识以及不可信标识；

所述客户端可信识别装置，还用于通过所述客户端设备向交易应用服务器设备发送客户端设备认证结果，以使得所述交易应用服务器设备根据客户端设备认证结果，对所述交易会话请求进行处理；所述客户端设备认证结果包括所述客户身份标识以及不可信标识，或者所述客户身份标识以及可信标识。

2. 根据权利要求1所述的客户端设备的安全认证系统，其特征在于，所述指纹要素信息包括软件要素、硬件要素和网络要素；所述软件要素包括操作系统信息、浏览器名称信息、屏幕分辨率信息；所述硬件要素包括CPU等级信息、硬盘编号信息；所述网络要素包括网络类型信息、MAC地址信息。

3. 根据权利要求2所述的客户端设备的安全认证系统，其特征在于，所述客户端可信识别装置，具体用于：

根据预先设置的串码格式将各指纹要素信息生成为指纹串码；

将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中，并进行加密，生成认证信息字符串。

4. 根据权利要求3所述的客户端设备的安全认证系统，其特征在于，在所述指纹特征库设备中记录有客户身份标识对应的各客户历史设备指纹信息，所述客户身份标识对应的各客户历史设备指纹信息包括指纹要素信息中各要素指纹特征项的实际取值以及各要素指纹特征项对应的可信概率值；

所述指纹特征库设备,具体用于:

查询所述客户身份标识对应的各客户历史设备指纹信息;

将指纹要素信息中的各指纹要素的取值与各客户历史设备相应各要素指纹特征项的实际取值进行匹配;若指纹要素信息中的一指纹要素的取值与其相应要素指纹特征项的实际取值不相同,则选取相应要素指纹特征项对应的可信概率值;

根据公式: $P=P_1 \cdot P_2 \cdot \dots \cdot P_k$ 确定所述认证信息与各客户历史设备的匹配度;其中,P为所述认证信息与各客户历史设备的匹配度; P_k 表示同一客户历史设备中选取的各相应要素指纹特征项对应的可信概率值。

5. 根据权利要求4所述的客户端设备的安全认证系统,其特征在于,所述认证服务器设备,具体用于:

判断所述匹配度中的最大值是否大于预先设置的匹配度阈值;在所述匹配度中的最大值大于所述匹配度阈值时,确定客户端设备的认证状态为认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在所述匹配度中的最大值小于等于所述匹配度阈值时,确定客户端设备的认证状态为待认证状态。

6. 根据权利要求5所述的客户端设备的安全认证系统,其特征在于,所述认证服务器设备,具体还用于:

在确定客户端设备的认证状态为待认证状态时,向客户端可信识别装置发送所述客户身份标识以及待认证标识;

所述客户端可信识别装置,具体还用于在接收到所述待认证标识后,接收用户输入的客户认证信息,并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备;

所述认证服务器设备,具体还用于向客户认证信息库设备发送新设备可信认证请求信息;所述新设备可信认证请求信息包括所述客户身份标识以及所述客户认证信息;

所述客户认证信息库设备,具体用于根据所述客户身份标识在客户认证信息库设备本地查询所述客户身份标识对应的认证信息内容,将所述客户认证信息与所述认证信息内容进行匹配,生成匹配结果,并将所述匹配结果发送给所述认证服务器设备;所述匹配结果包括匹配成功结果和匹配失败结果;

所述认证服务器设备,具体还用于在所述匹配结果为匹配成功结果时,确定新设备可信认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识,并通过指纹特征库设备存储所述客户身份标识对应的认证信息,以更新客户身份标识对应的各客户历史设备指纹信息;在所述匹配结果为匹配失败结果时,确定新设备可信认证失败,向所述客户端可信识别装置发送所述客户身份标识以及不可信标识。

7. 根据权利要求6所述的客户端设备的安全认证系统,其特征在于,所述客户认证信息包括介质号或生物特征信息;所述介质号包括客户认证密码;所述生物特征信息包括客户手指指纹信息、客户手掌掌纹信息、客户人脸识别信息、客户声音识别信息或者客户眼球识别信息。

8. 一种客户端设备的安全认证方法,其特征在于,应用于权利要求1所述的客户端设备的安全认证系统,所述方法包括:

客户端可信识别装置监测客户端设备,并在监测到客户端设备向交易应用服务器设备

发送交易会话请求时，采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息，将所述认证信息发送到认证服务器设备；

所述认证服务器设备解析所述认证信息，并向指纹特征库设备发送匹配请求；

所述指纹特征库设备查询所述客户身份标识对应的各客户历史设备指纹信息，并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配，确定所述认证信息与各客户历史设备的匹配度，并将各匹配度中的最大值发送给所述认证服务器设备；

所述认证服务器设备根据所述匹配度中的最大值确定客户端设备的认证状态；在所述认证状态为认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在所述认证状态为待认证状态时，根据客户认证信息库设备进行新设备可信认证；在新设备可信认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在新设备可信认证失败时，向所述客户端可信识别装置发送所述客户身份标识以及不可信标识；

所述客户端可信识别装置通过所述客户端设备向交易应用服务器设备发送客户端设备认证结果，以使得所述交易应用服务器设备根据客户端设备认证结果，对所述交易会话请求进行处理；所述客户端设备认证结果包括所述客户身份标识以及不可信标识，或者所述客户身份标识以及可信标识。

9. 根据权利要求8所述的客户端设备的安全认证方法，其特征在于，所述指纹要素信息包括软件要素、硬件要素和网络要素；所述软件要素包括操作方法信息、浏览器名称信息、屏幕分辨率信息；所述硬件要素包括CPU等级信息、硬盘编号信息；所述网络要素包括网络类型信息、MAC地址信息。

10. 根据权利要求9所述的客户端设备的安全认证方法，其特征在于，所述采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息，包括：

根据预先设置的串码格式将各指纹要素信息生成为指纹串码；

将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中，并进行加密，生成认证信息字符串。

11. 根据权利要求10所述的客户端设备的安全认证方法，其特征在于，在所述指纹特征库设备中记录有客户身份标识对应的各客户历史设备指纹信息，所述客户身份标识对应的各客户历史设备指纹信息包括指纹要素信息中各要素指纹特征项的实际取值以及各要素指纹特征项对应的可信概率值；

所述指纹特征库设备查询所述客户身份标识对应的各客户历史设备指纹信息，并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配，确定所述认证信息与各客户历史设备的匹配度，包括：

查询所述客户身份标识对应的各客户历史设备指纹信息；

将指纹要素信息中的各指纹要素的取值与各客户历史设备相应各要素指纹特征项的实际取值进行匹配；若指纹要素信息中的一指纹要素的取值与其相应要素指纹特征项的实际取值不相同，则选取相应要素指纹特征项对应的可信概率值；

根据公式： $P = P_1 \cdot P_2 \cdot \dots \cdot P_k$ 确定所述认证信息与各客户历史设备的匹配度；其中， P

为所述认证信息与各客户历史设备的匹配度; P_k 表示同一客户历史设备中选取的各相应要素指纹特征项对应的可信概率值。

12. 根据权利要求11所述的客户端设备的安全认证方法,其特征在于,所述认证服务器设备根据所述匹配度中的最大值确定客户端设备的认证状态;在所述认证状态为认证成功时,向所述客户端可信识别装置发送所述客户身份标识以及可信标识,包括:

判断所述匹配度中的最大值是否大于预先设置的匹配度阈值;在所述匹配度中的最大值大于所述匹配度阈值时,确定客户端设备的认证状态为认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在所述匹配度中的最大值小于等于所述匹配度阈值时,确定客户端设备的认证状态为待认证状态。

13. 根据权利要求12所述的客户端设备的安全认证方法,其特征在于,在所述认证状态为待认证状态时,根据客户认证信息库设备进行新设备可信认证,包括:

在确定客户端设备的认证状态为待认证状态时,向客户端可信识别装置发送所述客户身份标识以及待认证标识;

所述客户端可信识别装置在接收到所述待认证标识后,接收用户输入的客户认证信息,并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备;

所述认证服务器设备向客户认证信息库设备发送新设备可信认证请求信息;所述新设备可信认证请求信息包括所述客户身份标识以及所述客户认证信息;

所述客户认证信息库设备根据所述客户身份标识在客户认证信息库设备本地查询所述客户身份标识对应的认证信息内容,将所述客户认证信息与所述认证信息内容进行匹配,生成匹配结果,并将所述匹配结果发送给所述认证服务器设备;所述匹配结果包括匹配成功结果和匹配失败结果;

所述方法还包括:

所述认证服务器设备在所述匹配结果为匹配成功结果时,确定新设备可信认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识,并通过指纹特征库设备存储所述客户身份标识对应的认证信息,以更新客户身份标识对应的各客户历史设备指纹信息;在所述匹配结果为匹配失败结果时,确定新设备可信认证失败,向所述客户端可信识别装置发送所述客户身份标识以及不可信标识。

14. 根据权利要求13所述的客户端设备的安全认证方法,其特征在于,所述客户认证信息包括介质号或生物特征信息;所述介质号包括客户认证密码;所述生物特征信息包括客户手指指纹信息、客户手掌掌纹信息、客户人脸识别信息、客户声音识别信息或者客户眼球识别信息。

15. 一种客户端可信识别装置,其特征在于,包括:

客户端设备监测单元,用于监测客户端设备;

指纹要素信息采集单元,用于在监测到客户端设备向交易应用服务器设备发送交易会话请求时,采集所述客户端设备的指纹要素信息,并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息;

信息安全通讯单元,用于将所述认证信息发送到认证服务器设备;接收认证服务器设备发送的客户身份标识以及可信标识,或者接收认证服务器设备发送的客户身份标识以及不可信标识;通过客户端设备向交易应用服务器设备发送客户端设备认证结果,以使得所

述交易应用服务器设备根据客户端设备认证结果,对所述交易会话请求进行处理;所述客户端设备认证结果包括所述客户身份标识以及不可信标识,或者所述客户身份标识以及可信标识。

16. 根据权利要求15所述的客户端可信识别装置,其特征在于,还包括:

信息整合加密单元,用于根据预先设置的串码格式将各指纹要素信息生成为指纹串码;将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中,并进行加密,生成认证信息字符串。

17. 根据权利要求16所述的客户端可信识别装置,其特征在于,所述信息安全通讯单元,还用于接收认证服务器设备发送的客户身份标识以及待认证标识;接收用户输入的客户认证信息,并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备。

客户端设备的安全认证系统、方法及客户端可信识别装置

技术领域

[0001] 本发明涉及客户端安全认证技术领域，尤其涉及一种客户端设备的安全认证系统、方法及客户端可信识别装置。

背景技术

[0002] 当前，随着互联网金融的快速发展，金融交易的风险控制也将面临巨大挑战。犯罪分子可以通过黑客攻击、撞库、钓鱼等非法手段，获取客户身份证件、姓名、交易卡密码、手机号等敏感信息，在各种客户端设备上，仿冒真实客户进行登录、支付、转账交易等操作，给客户资金安全带来了巨大风险。为了有效控制这类风险，需要对客户端设备进行可信识别，若判定到客户端设备是可信的，说明是客户本人进行交易操作；若判定客户端设备是不可信的，说明交易操作存在风险，进而需要采取拒绝非法操作措施。

[0003] 目前，现有技术中最常用的可信识别方法主要以网络地址与硬件地址捆绑作为识别要素，但这种识别方式存在如下问题：一方面，网络地址与硬件地址是可以修改的，也很容易被伪造，犯罪分子可以利用伪地址进行登录，造成可信识别系统将非法客户端设备误判为可信设备。另一方面，由于识别要素比较单一，识别准确度不高，会出现误判断的情况，比如客户修改操作系统参数，或设备硬件变更引起网络或硬件地址变化，可信识别系统会将合法的客户端设备误判为不可信设备，从而影响客户正常交易。可见，当前亟需一种快速、准确识别安全客户端设备的方法，提高安全防控效果，保护客户的资金财产安全。

发明内容

[0004] 本发明的实施例提供一种客户端设备的安全认证系统、方法及客户端可信识别装置，以解决现有技术中的可信识别方法中识别要素单一，且可修改，造成识别结果不准确的问题。

[0005] 为达到上述目的，本发明采用如下技术方案：

[0006] 一种客户端设备的安全认证系统，包括：客户端设备、客户端可信识别装置、交易应用服务器设备、认证服务器设备、指纹特征库设备、客户认证信息库设备；所述客户端设备与所述客户端可信识别装置连接；所述客户端设备通过外部网络与所述交易应用服务器设备通信连接；所述客户端可信识别装置通过外部网络与所述认证服务器设备通信连接；所述认证服务器设备通过局域网络分别与所述指纹特征库设备和客户认证信息库设备通信连接；

[0007] 所述客户端可信识别装置，用于监测客户端设备，并在监测到客户端设备向所述交易应用服务器设备发送交易会话请求时，采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息，将所述认证信息发送到所述认证服务器设备；

[0008] 所述认证服务器设备，用于解析所述认证信息，并向所述指纹特征库设备发送匹配请求；

[0009] 所述指纹特征库设备,用于查询所述客户身份标识对应的各客户历史设备指纹信息,并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配,确定所述认证信息与各客户历史设备的匹配度,并将各匹配度中的最大值发送给所述认证服务器设备;

[0010] 所述认证服务器设备,还用于根据所述匹配度中的最大值确定客户端设备的认证状态;在所述认证状态为认证成功时,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在所述认证状态为待认证状态时,根据客户认证信息库设备进行新设备可信认证;在新设备可信认证成功时,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在新设备可信认证失败时,向所述客户端可信识别装置发送所述客户身份标识以及不可信标识;

[0011] 所述客户端可信识别装置,还用于通过所述客户端设备向交易应用服务器设备发送客户端设备认证结果,以使得所述交易应用服务器设备根据客户端设备认证结果,对所述交易会话请求进行处理;所述客户端设备认证结果包括所述客户身份标识以及不可信标识,或者所述客户身份标识以及可信标识。

[0012] 具体的,所述指纹要素信息包括软件要素、硬件要素和网络要素;所述软件要素包括操作系统信息、浏览器名称信息、屏幕分辨率信息;所述硬件要素包括CPU等级信息、硬盘编号信息;所述网络要素包括网络类型信息、MAC地址信息。

[0013] 此外,所述客户端可信识别装置,具体用于:

[0014] 根据预先设置的串码格式将各指纹要素信息生成为指纹串码;

[0015] 将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中,并进行加密,生成认证信息字符串。

[0016] 此外,在所述指纹特征库设备中记录有客户身份标识对应的各客户历史设备指纹信息,所述客户身份标识对应的各客户历史设备指纹信息包括指纹要素信息中各要素指纹特征项的实际取值以及各要素指纹特征项对应的可信概率值;

[0017] 所述指纹特征库设备,具体用于:

[0018] 查询所述客户身份标识对应的各客户历史设备指纹信息;

[0019] 将指纹要素信息中的各指纹要素的取值与各客户历史设备相应各要素指纹特征项的实际取值进行匹配;若指纹要素信息中的一指纹要素的取值与其相应要素指纹特征项的实际取值不相同,则选取相应要素指纹特征项对应的可信概率值;

[0020] 根据公式: $P=P_1 \cdot P_2 \cdot \dots \cdot P_k$ 确定所述认证信息与各客户历史设备的匹配度;其中,P为所述认证信息与各客户历史设备的匹配度;P_k表示同一客户历史设备中选取的各相应要素指纹特征项对应的可信概率值。

[0021] 另外,所述认证服务器设备,具体用于:

[0022] 判断所述匹配度中的最大值是否大于预先设置的匹配度阈值;在所述匹配度中的最大值大于所述匹配度阈值时,确定客户端设备的认证状态为认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在所述匹配度中的最大值小于等于所述匹配度阈值时,确定客户端设备的认证状态为待认证状态。

[0023] 进一步的,所述认证服务器设备,具体还用于:

[0024] 在确定客户端设备的认证状态为待认证状态时,向客户端可信识别装置发送所述

客户身份标识以及待认证标识；

[0025] 所述客户端可信识别装置，具体还用于在接收到所述待认证标识后，接收用户输入的客户认证信息，并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备；

[0026] 所述认证服务器设备，具体还用于向客户认证信息库设备发送新设备可信认证请求信息；所述新设备可信认证请求信息包括所述客户身份标识以及所述客户认证信息；

[0027] 所述客户认证信息库设备，具体用于根据所述客户身份标识在客户认证信息库设备本地查询所述客户身份标识对应的认证信息内容，将所述客户认证信息与所述认证信息内容进行匹配，生成匹配结果，并将所述匹配结果发送给所述认证服务器设备；所述匹配结果包括匹配成功结果和匹配失败结果；

[0028] 所述认证服务器设备，具体还用于在所述匹配结果为匹配成功结果时，确定新设备可信认证成功，向所述客户端可信识别装置发送所述客户身份标识以及可信标识，并通过指纹特征库设备存储所述客户身份标识对应的认证信息，以更新客户身份标识对应的各客户历史设备指纹信息；在所述匹配结果为匹配失败结果时，确定新设备可信认证失败，向所述客户端可信识别装置发送所述客户身份标识以及不可信标识。

[0029] 具体的，所述客户认证信息包括介质号或生物特征信息；所述介质号包括客户认证密码；所述生物特征信息包括客户手指指纹信息、客户手掌掌纹信息、客户人脸识别信息、客户声音识别信息或者客户眼球识别信息。

[0030] 一种客户端设备的安全认证方法，应用于上述的客户端设备的安全认证系统，所述方法包括：

[0031] 客户端可信识别装置监测客户端设备，并在监测到客户端设备向交易应用服务器设备发送交易会话请求时，采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息，将所述认证信息发送到认证服务器设备；

[0032] 所述认证服务器设备解析所述认证信息，并向指纹特征库设备发送匹配请求；

[0033] 所述指纹特征库设备查询所述客户身份标识对应的各客户历史设备指纹信息，并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配，确定所述认证信息与各客户历史设备的匹配度，并将各匹配度中的最大值发送给所述认证服务器设备；

[0034] 所述认证服务器设备根据所述匹配度中的最大值确定客户端设备的认证状态；在所述认证状态为认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在所述认证状态为待认证状态时，根据客户认证信息库设备进行新设备可信认证；在新设备可信认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在新设备可信认证失败时，向所述客户端可信识别装置发送所述客户身份标识以及不可信标识；

[0035] 所述客户端可信识别装置通过所述客户端设备向交易应用服务器设备发送客户端设备认证结果，以使得所述交易应用服务器设备根据客户端设备认证结果，对所述交易会话请求进行处理；所述客户端设备认证结果包括所述客户身份标识以及不可信标识，或者所述客户身份标识以及可信标识。

[0036] 具体的，所述指纹要素信息包括软件要素、硬件要素和网络要素；所述软件要素包

括操作方法信息、浏览器名称信息、屏幕分辨率信息；所述硬件要素包括CPU等级信息、硬盘编号信息；所述网络要素包括网络类型信息、MAC地址信息。

[0037] 具体的，所述采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息，包括：

[0038] 根据预先设置的串码格式将各指纹要素信息生成为指纹串码；

[0039] 将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中，并进行加密，生成认证信息字符串。

[0040] 具体的，在所述指纹特征库设备中记录有客户身份标识对应的各客户历史设备指纹信息，所述客户身份标识对应的各客户历史设备指纹信息包括指纹要素信息中各要素指纹特征项的实际取值以及各要素指纹特征项对应的可信概率值；

[0041] 所述指纹特征库设备查询所述客户身份标识对应的各客户历史设备指纹信息，并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配，确定所述认证信息与各客户历史设备的匹配度，包括：

[0042] 查询所述客户身份标识对应的各客户历史设备指纹信息；

[0043] 将指纹要素信息中的各指纹要素的取值与各客户历史设备相应各要素指纹特征项的实际取值进行匹配；若指纹要素信息中的一指纹要素的取值与其相应要素指纹特征项的实际取值不相同，则选取相应要素指纹特征项对应的可信概率值；

[0044] 根据公式： $P = P_1 \cdot P_2 \cdot \dots \cdot P_k$ 确定所述认证信息与各客户历史设备的匹配度；其中，P为所述认证信息与各客户历史设备的匹配度； P_k 表示同一客户历史设备中选取的各相应要素指纹特征项对应的可信概率值。

[0045] 具体的，所述认证服务器设备根据所述匹配度中的最大值确定客户端设备的认证状态；在所述认证状态为认证成功时，向所述客户端可信识别装置发送所述客户身份标识以及可信标识，包括：

[0046] 判断所述匹配度中的最大值是否大于预先设置的匹配度阈值；在所述匹配度中的最大值大于所述匹配度阈值时，确定客户端设备的认证状态为认证成功，向所述客户端可信识别装置发送所述客户身份标识以及可信标识；在所述匹配度中的最大值小于等于所述匹配度阈值时，确定客户端设备的认证状态为待认证状态。

[0047] 具体的，在所述认证状态为待认证状态时，根据客户认证信息库设备进行新设备可信认证，包括：

[0048] 在确定客户端设备的认证状态为待认证状态时，向客户端可信识别装置发送所述客户身份标识以及待认证标识；

[0049] 所述客户端可信识别装置在接收到所述待认证标识后，接收用户输入的客户认证信息，并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备；

[0050] 所述认证服务器设备向客户认证信息库设备发送新设备可信认证请求信息；所述新设备可信认证请求信息包括所述客户身份标识以及所述客户认证信息；

[0051] 所述客户认证信息库设备根据所述客户身份标识在客户认证信息库设备本地查询所述客户身份标识对应的认证信息内容，将所述客户认证信息与所述认证信息内容进行匹配，生成匹配结果，并将所述匹配结果发送给所述认证服务器设备；所述匹配结果包括匹配成功结果和匹配失败结果；

[0052] 所述方法还包括：

[0053] 所述认证服务器设备在所述匹配结果为匹配成功结果时,确定新设备可信认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识,并通过指纹特征库设备存储所述客户身份标识对应的认证信息,以更新客户身份标识对应的各客户历史设备指纹信息;在所述匹配结果为匹配失败结果时,确定新设备可信认证失败,向所述客户端可信识别装置发送所述客户身份标识以及不可信标识。

[0054] 具体的,所述客户认证信息包括介质号或生物特征信息;所述介质号包括客户认证密码;所述生物特征信息包括客户手指指纹信息、客户手掌掌纹信息、客户人脸识别信息、客户声音识别信息或者客户眼球识别信息。

[0055] 一种客户端可信识别装置,包括:

[0056] 客户端设备监测单元,用于监测客户端设备;

[0057] 指纹要素信息采集单元,用于在监测到客户端设备向交易应用服务器设备发送交易会话请求时,采集所述客户端设备的指纹要素信息,并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息;

[0058] 信息安全通讯单元,用于将所述认证信息发送到认证服务器设备;接收认证服务器设备发送的客户身份标识以及可信标识,或者接收认证服务器设备发送的客户身份标识以及不可信标识;通过客户端设备向交易应用服务器设备发送客户端设备认证结果,以使得所述交易应用服务器设备根据客户端设备认证结果,对所述交易会话请求进行处理;所述客户端设备认证结果包括所述客户身份标识以及不可信标识,或者所述客户身份标识以及可信标识。

[0059] 进一步的,所述的客户端可信识别装置,还包括:

[0060] 信息整合加密单元,用于根据预先设置的串码格式将各指纹要素信息生成为指纹串码;将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中,并进行加密,生成认证信息字符串。

[0061] 进一步的,所述信息安全通讯单元,还用于接收认证服务器设备发送的客户身份标识以及待认证标识;接收用户输入的客户认证信息,并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备。

[0062] 本发明实施例提供的一种客户端设备的安全认证系统、方法及客户端可信识别装置,通过采集多元化的客户端设备的指纹要素信息,与指纹特征库中的客户历史设备指纹信息匹配,对客户端设备的可信性进行认证;在客户端设备首次认证未通过时,还可以进一步进行新设备可信认证,保证了客户端设备的可靠性,在降低了交易风险的同时,也提升客户的操作体验,可以提高安全防控效果,保护客户的资金财产安全,避免了现有技术中的可信识别方法中识别要素单一,且可修改,造成识别结果不准确的问题。

附图说明

[0063] 为了更清楚地说明本发明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发明的一些实施例,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。

- [0064] 图1为本发明实施例提供的一种客户端设备的安全认证系统的结构示意图；
- [0065] 图2为本发明实施例提供的一种客户端设备的安全认证方法的流程图一；
- [0066] 图3为本发明实施例提供的一种客户端设备的安全认证方法的流程图二；
- [0067] 图4为本发明实施例提供的一种客户端可信识别装置的结构示意图。

具体实施方式

[0068] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0069] 如图1所示，本发明实施例提供一种客户端设备的安全认证系统，包括：客户端设备11、客户端可信识别装置12、交易应用服务器设备13、认证服务器设备14、指纹特征库设备15、客户认证信息库设备16。所述客户端设备11与所述客户端可信识别装置12连接；所述客户端设备11通过外部网络与所述交易应用服务器设备13通信连接；所述客户端可信识别装置12通过外部网络与所述认证服务器设备14通信连接；所述认证服务器设备14通过局域网络分别与所述指纹特征库设备15和客户认证信息库设备16通信连接。值得说明的是，在本发明实施例中，客户端可信识别装置12可以作为硬件设备部署于客户端设备11内部或以接口方式(例如串行端口、USB端口等硬件端口，但不仅局限于此)连接到客户端设备11上。此处的客户端设备可以为智能手机、平板电脑、笔记本电脑等。

[0070] 所述客户端可信识别装置12，用于监测客户端设备11，并在监测到客户端设备11向所述交易应用服务器设备13发送交易会话请求时，采集所述客户端设备11的指纹要素信息，并根据客户端可信识别装置12绑定的客户身份标识与所述指纹要素信息生成认证信息，将所述认证信息发送到所述认证服务器设备14。此处，所述客户端可信识别装置12绑定的客户身份标识可以是在客户领取客户端可信识别装置12时进行的协议绑定，也可以是客户通过柜面(如银行柜台业务)修改绑定。另外，客户端可信识别装置采集客户端设备11的指纹要素信息可以通过多种技术实现，例如插件/控件、javascript、分析HTTP/HTTPS协议等，但不仅局限于此。

[0071] 所述认证服务器设备14，用于解析所述认证信息，并向所述指纹特征库设备15发送匹配请求。

[0072] 所述指纹特征库设备15，用于查询所述客户身份标识对应的各客户历史设备指纹信息，并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配，确定所述认证信息与各客户历史设备的匹配度，并将各匹配度中的最大值发送给所述认证服务器设备14。

[0073] 所述认证服务器设备14，还用于根据所述匹配度中的最大值确定客户端设备11的认证状态；在所述认证状态为认证成功时，向所述客户端可信识别装置12发送所述客户身份标识以及可信标识；在所述认证状态为待认证状态时，根据客户认证信息库设备16进行新设备可信认证；在新设备可信认证成功时，向所述客户端可信识别装置12发送所述客户身份标识以及可信标识；在新设备可信认证失败时，向所述客户端可信识别装置12发送所述客户身份标识以及不可信标识。

[0074] 所述客户端可信识别装置12,还用于通过所述客户端设备11向交易应用服务器设备13发送客户端设备11认证结果,以使得所述交易应用服务器设备13根据客户端设备11认证结果,对所述交易会话请求进行处理;所述客户端设备11认证结果包括所述客户身份标识以及不可信标识,或者所述客户身份标识以及可信标识。

[0075] 具体的,所述指纹要素信息可以包括软件要素、硬件要素和网络要素;所述软件要素包括操作系统信息(例如Linux、Window7等)、浏览器名称信息(例如IE、Chrome等)、屏幕分辨率信息(例如 1024×768 、 1440×900 等);所述硬件要素包括中央处理器(Central Processing Unit,简称CPU)等级信息、硬盘编号信息(例如N34568888);所述网络要素包括网络类型信息(例如光纤)、MAC地址(Media Access Control地址)信息、IP地址信息(例如210.213.45.6)等。

[0076] 此外,所述客户端可信识别装置12,具体用于:

[0077] 根据预先设置的串码格式将各指纹要素信息生成为指纹串码。

[0078] 将客户端可信识别装置12绑定的客户身份标识封装入所述指纹串码中,并进行加密,生成认证信息字符串。

[0079] 此外,在所述指纹特征库设备15中记录有客户身份标识对应的各客户历史设备指纹信息,所述客户身份标识对应的各客户历史设备指纹信息包括指纹要素信息中各要素指纹特征项的实际取值以及各要素指纹特征项对应的可信概率值。

[0080] 所述指纹特征库设备15,具体用于:

[0081] 查询所述客户身份标识对应的各客户历史设备指纹信息。

[0082] 将指纹要素信息中的各指纹要素的取值与各客户历史设备相应各要素指纹特征项的实际取值进行匹配;若指纹要素信息中的一指纹要素的取值与其相应要素指纹特征项的实际取值不相同,则选取相应要素指纹特征项对应的可信概率值。

[0083] 根据公式: $P=P_1 \cdot P_2 \cdot \dots \cdot P_k$ 确定所述认证信息与各客户历史设备的匹配度;其中,P为所述认证信息与各客户历史设备的匹配度;Pk表示同一客户历史设备中选取的各相应要素指纹特征项对应的可信概率值。

[0084] 另外,所述认证服务器设备14,具体用于:

[0085] 判断所述匹配度中的最大值是否大于预先设置的匹配度阈值;在所述匹配度中的最大值大于所述匹配度阈值时,确定客户端设备11的认证状态为认证成功,向所述客户端可信识别装置12发送所述客户身份标识以及可信标识;在所述匹配度中的最大值小于等于所述匹配度阈值时,确定客户端设备11的认证状态为待认证状态。

[0086] 进一步的,所述认证服务器设备14,具体还用于:

[0087] 在确定客户端设备11的认证状态为待认证状态时,向客户端可信识别装置12发送所述客户身份标识以及待认证标识。

[0088] 所述客户端可信识别装置12,具体还用于在接收到所述待认证标识后,接收用户输入的客户认证信息,并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备14。

[0089] 此处,在客户端可信识别装置12中可以设置相应用于采集客户认证信息的硬件,例如触摸式显示屏、微型键盘,或者能够采集生物特征信息的集成电路模块,如指纹识别器等。

[0090] 所述认证服务器设备14,具体还用于向客户认证信息库设备16发送新设备可信认证请求信息;所述新设备可信认证请求信息包括所述客户身份标识以及所述客户认证信息。

[0091] 所述客户认证信息库设备16,具体用于根据所述客户身份标识在客户认证信息库设备16本地查询所述客户身份标识对应的认证信息内容,将所述客户认证信息与所述认证信息内容进行匹配,生成匹配结果,并将所述匹配结果发送给所述认证服务器设备14;所述匹配结果包括匹配成功结果和匹配失败结果。

[0092] 所述认证服务器设备14,具体还用于在所述匹配结果为匹配成功结果时,确定新设备可信认证成功,向所述客户端可信识别装置12发送所述客户身份标识以及可信标识,并通过指纹特征库设备15存储所述客户身份标识对应的认证信息,以更新客户身份标识对应的各客户历史设备指纹信息;在所述匹配结果为匹配失败结果时,确定新设备可信认证失败,向所述客户端可信识别装置12发送所述客户身份标识以及不可信标识。

[0093] 具体的,所述客户认证信息包括介质号或生物特征信息;所述介质号包括客户认证密码;所述生物特征信息包括客户手指指纹信息、客户手掌掌纹信息、客户人脸识别信息、客户声音识别信息或者客户眼球识别信息。

[0094] 本发明实施例提供的一种客户端设备的安全认证系统,通过采集多元化的客户端设备的指纹要素信息,与指纹特征库中的客户历史设备指纹信息匹配,对客户端设备的可信性进行认证;在客户端设备首次认证未通过时,还可以进一步进行新设备可信认证,保证了客户端设备的可靠性,在降低了交易风险的同时,也提升客户的操作体验,可以提高安全防控效果,保护客户的资金财产安全,避免了现有技术中的可信识别方法中识别要素单一,且可修改,造成识别结果不准确的问题。

[0095] 对应于上述图1所示的客户端设备的安全认证系统,如图2所示,本发明实施例提供一种客户端设备的安全认证方法,应用于上述的客户端设备的安全认证系统,所述方法包括:

[0096] 步骤201、客户端可信识别装置监测客户端设备,并在监测到客户端设备向交易应用服务器设备发送交易会话请求时,采集所述客户端设备的指纹要素信息,并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息,将所述认证信息发送到认证服务器设备。

[0097] 步骤202、所述认证服务器设备解析所述认证信息,并向指纹特征库设备发送匹配请求。

[0098] 步骤203、所述指纹特征库设备查询所述客户身份标识对应的各客户历史设备指纹信息,并根据所述客户历史设备指纹信息与指纹要素信息中的各指纹要素进行匹配,确定所述认证信息与各客户历史设备的匹配度,并将各匹配度中的最大值发送给所述认证服务器设备。

[0099] 步骤204、所述认证服务器设备根据所述匹配度中的最大值确定客户端设备的认证状态;在所述认证状态为认证成功时,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在所述认证状态为待认证状态时,根据客户认证信息库设备进行新设备可信认证;在新设备可信认证成功时,向所述客户端可信识别装置发送所述客户身份标识以及可信标识;在新设备可信认证失败时,向所述客户端可信识别装置发送所述客户身份

标识以及不可信标识。

[0100] 步骤205、所述客户端可信识别装置通过所述客户端设备向交易应用服务器设备发送客户端设备认证结果,以使得所述交易应用服务器设备根据客户端设备认证结果,对所述交易会话请求进行处理;所述客户端设备认证结果包括所述客户身份标识以及不可信标识,或者所述客户身份标识以及可信标识。

[0101] 本发明实施例提供的一种客户端设备的安全认证方法,通过采集多元化的客户端设备的指纹要素信息,与指纹特征库中的客户历史设备指纹信息匹配,对客户端设备的可信性进行认证;在客户端设备首次认证未通过时,还可以进一步进行新设备可信认证,保证了客户端设备的可靠性,在降低了交易风险的同时,也提升客户的操作体验,可以提高安全防控效果,保护客户的资金财产安全,避免了现有技术中的可信识别方法中识别要素单一,且可修改,造成识别结果不准确的问题。

[0102] 为了使本领域的技术人员更好的了解本发明,下面列举一个更为详细和具体的实施例,如图3所示,本发明实施例提供一种客户端设备的安全认证方法,包括:

[0103] 步骤301、客户端可信识别装置监测客户端设备。

[0104] 步骤302、在监测到客户端设备向交易应用服务器设备发送交易会话请求时,采集所述客户端设备的指纹要素信息,根据预先设置的串码格式将各指纹要素信息生成为指纹串码,将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中,并进行加密,生成认证信息字符串,将认证信息字符串形成的认证信息发送到认证服务器设备。

[0105] 此处,所述指纹要素信息可以包括软件要素、硬件要素和网络要素;所述软件要素包括操作方法信息、浏览器名称信息、屏幕分辨率信息;所述硬件要素包括CPU等级信息、硬盘编号信息;所述网络要素包括网络类型信息、MAC地址信息。

[0106] 此处,例如未能获取的指纹要素可以留空,形成客户端设备对应的指纹串码,如{Linux,光纤,...};再将客户身份标识,如(0234567)封装入指纹串码;最后进行进行加密,构成认证信息字符串,例如{0234567}{Linux,光纤,...}。

[0107] 另外,此处的交易会话可以根据不同的交易业务特性而不同,比如网银、手机银行以登录登出作为一次交易会话,而网上银行支付交易可以以每笔支付作为一次交易会话。

[0108] 步骤303、所述认证服务器设备解析所述认证信息,并向指纹特征库设备发送匹配请求。

[0109] 步骤304、所述指纹特征库设备查询所述客户身份标识对应的各客户历史设备指纹信息。

[0110] 具体的,在所述指纹特征库设备中记录有客户身份标识对应的各客户历史设备指纹信息,所述客户身份标识对应的各客户历史设备指纹信息包括指纹要素信息中各要素指纹特征项的实际取值以及各要素指纹特征项对应的可信概率值。

[0111] 如下表1所示:

[0112] 表1:

[0113]

要素	要素指纹特征项	实际取值	可信概率值
软件	浏览器	Chrome	0.99
	操作系统	Linux	0.95
硬件	硬盘编号	N34568888	0.23
网络	IP	210.213.45.6	0.98
	网络类型	光纤	0.99

[0114] 例如,一个客户历史设备的要素指纹特征项为浏览器,其实际取值是IE,其他要素指纹特征项与上述设备认证信息中的设备指纹是一样的,则得到匹配度为0.99。若在前述基础上,其操作系统为Windows7,则匹配度应该为 $0.99 \times 0.95 = 0.9405$ 。

[0115] 步骤305、将指纹要素信息中的各指纹要素的取值与各客户历史设备相应各要素指纹特征项的实际取值进行匹配;若指纹要素信息中的一指纹要素的取值与其相应要素指纹特征项的实际取值不相同,则选取相应要素指纹特征项对应的可信概率值。

[0116] 此处,例如一个客户历史设备有I个要素指纹特征项 N_i ($i=1, \dots, I$),每个特征项对应一个可信概率值 P_i ($i=1, \dots, I$),所述可信概率值就是这个要素指纹特征项对设备唯一性的影响程度,对设备唯一性的影响程度与可信概率值呈反向趋势。例如,若要素指纹特征项为IP地址,当IP地址改变了,对设备唯一性的影响程度小,那么它的可信概率值就比较大;确定该要素指纹特征项的数值,通常是根据业务领域的经验来设定数值,通常要素指纹特征项为IP地址的可信概率值为0.98,但不仅局限于此。

[0117] 步骤306、根据公式: $P = P_1 \cdot P_2 \cdot \dots \cdot P_k$ 确定所述认证信息与各客户历史设备的匹配度。

[0118] 其中,P为所述认证信息与各客户历史设备的匹配度; P_k 表示同一客户历史设备中选取的各相应要素指纹特征项对应的可信概率值。此处, $P \leq I$ 。

[0119] 步骤307、将各匹配度中的最大值发送给所述认证服务器设备。

[0120] 步骤308、所述认证服务器设备判断所述匹配度中的最大值是否大于预先设置的匹配度阈值。

[0121] 预先设置的匹配度阈值可以根据业务的实际需求进行设置,通常设置为75%。

[0122] 在所述匹配度中的最大值大于所述匹配度阈值时,执行步骤309。否则,在所述匹配度中的最大值小于等于所述匹配度阈值时,执行步骤310。

[0123] 步骤309、确定客户端设备的认证状态为认证成功,向所述客户端可信识别装置发送所述客户身份标识以及可信标识。在步骤309之后继续执行步骤316。

[0124] 步骤310、确定客户端设备的认证状态为待认证状态,向客户端可信识别装置发送所述客户身份标识以及待认证标识。

[0125] 步骤311、客户端可信识别装置在接收到所述待认证标识后,接收用户输入的客户认证信息,并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备。

- [0126] 步骤312、认证服务器设备向客户认证信息库设备发送新设备可信认证请求信息。
- [0127] 其中，所述新设备可信认证请求信息包括所述客户身份标识以及所述客户认证信息。
- [0128] 此处，所述客户认证信息包括介质号或生物特征信息；所述介质号包括客户认证密码；所述生物特征信息包括客户手指指纹信息、客户手掌掌纹信息、客户人脸识别信息、客户声音识别信息或者客户眼球识别信息。
- [0129] 步骤313、客户认证信息库设备根据所述客户身份标识在客户认证信息库设备本地查询所述客户身份标识对应的认证信息内容，将所述客户认证信息与所述认证信息内容进行匹配，生成匹配结果，并将所述匹配结果发送给所述认证服务器设备。
- [0130] 其中，所述匹配结果包括匹配成功结果和匹配失败结果。在步骤313之后执行步骤314或者步骤315。
- [0131] 步骤314、认证服务器设备在所述匹配结果为匹配成功结果时，确定新设备可信认证成功，向所述客户端可信识别装置发送所述客户身份标识以及可信标识，并通过指纹特征库设备存储所述客户身份标识对应的认证信息，以更新客户身份标识对应的各客户历史设备指纹信息。
- [0132] 步骤315、认证服务器设备在所述匹配结果为匹配失败结果时，确定新设备可信认证失败，向所述客户端可信识别装置发送所述客户身份标识以及不可信标识。
- [0133] 在步骤314和步骤315之后，继续执行步骤316。
- [0134] 步骤316、所述客户端可信识别装置通过所述客户端设备向交易应用服务器设备发送客户端设备认证结果，以使得所述交易应用服务器设备根据客户端设备认证结果，对所述交易会话请求进行处理。
- [0135] 其中，所述客户端设备认证结果包括所述客户身份标识以及不可信标识，或者所述客户身份标识以及可信标识。
- [0136] 此处，当交易应用服务器设备得到的认证结果中存在可信标识，则允许客户端设备与其进行交易会话。否则，当交易应用服务器设备得到的认证结果中存在不可信标识，则拒绝交易会话。
- [0137] 本发明实施例提供的一种客户端设备的安全认证方法，通过采集多元化的客户端设备的指纹要素信息，与指纹特征库中的客户历史设备指纹信息匹配，对客户端设备的可信性进行认证；在客户端设备首次认证未通过时，还可以进一步进行新设备可信认证，保证了客户端设备的可靠性，在降低了交易风险的同时，也提升客户的操作体验，可以提高安全防控效果，保护客户的资金财产安全，避免了现有技术中的可信识别方法中识别要素单一，且可修改，造成识别结果不准确的问题。
- [0138] 如图4所示，本发明实施例提供一种客户端可信识别装置，包括：
- [0139] 客户端设备监测单元41，用于监测客户端设备。
- [0140] 指纹要素信息采集单元42，用于在监测到客户端设备向交易应用服务器设备发送交易会话请求时，采集所述客户端设备的指纹要素信息，并根据客户端可信识别装置绑定的客户身份标识与所述指纹要素信息生成认证信息。
- [0141] 信息安全通讯单元43，用于将所述认证信息发送到认证服务器设备；接收认证服务器设备发送的客户身份标识以及可信标识，或者接收认证服务器设备发送的客户身份标

识以及不可信标识；通过客户端设备向交易应用服务器设备发送客户端设备认证结果，以使得所述交易应用服务器设备根据客户端设备认证结果，对所述交易会话请求进行处理；所述客户端设备认证结果包括所述客户身份标识以及不可信标识，或者所述客户身份标识以及可信标识。

[0142] 进一步的，如图4所示，所述的客户端可信识别装置，还包括：

[0143] 信息整合加密单元44，用于根据预先设置的串码格式将各指纹要素信息生成为指纹串码；将客户端可信识别装置绑定的客户身份标识封装入所述指纹串码中，并进行加密，生成认证信息字符串。

[0144] 进一步的，所述信息安全通讯单元43，还用于接收认证服务器设备发送的客户身份标识以及待认证标识；接收用户输入的客户认证信息，并将所述客户身份标识以及所述客户认证信息发送给所述认证服务器设备。

[0145] 本发明实施例提供的一种客户端可信识别装置，通过采集多元化的客户端设备的指纹要素信息，与指纹特征库中的客户历史设备指纹信息匹配，对客户端设备的可信性进行认证；在客户端设备首次认证未通过时，还可以进一步进行新设备可信认证，保证了客户端设备的可靠性，在降低了交易风险的同时，也提升客户的操作体验，可以提高安全防控效果，保护客户的资金财产安全，避免了现有技术中的可信识别方法中识别要素单一，且可修改，造成识别结果不准确的问题。

[0146] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0147] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理器或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0148] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0149] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0150] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内

容不应理解为对本发明的限制。

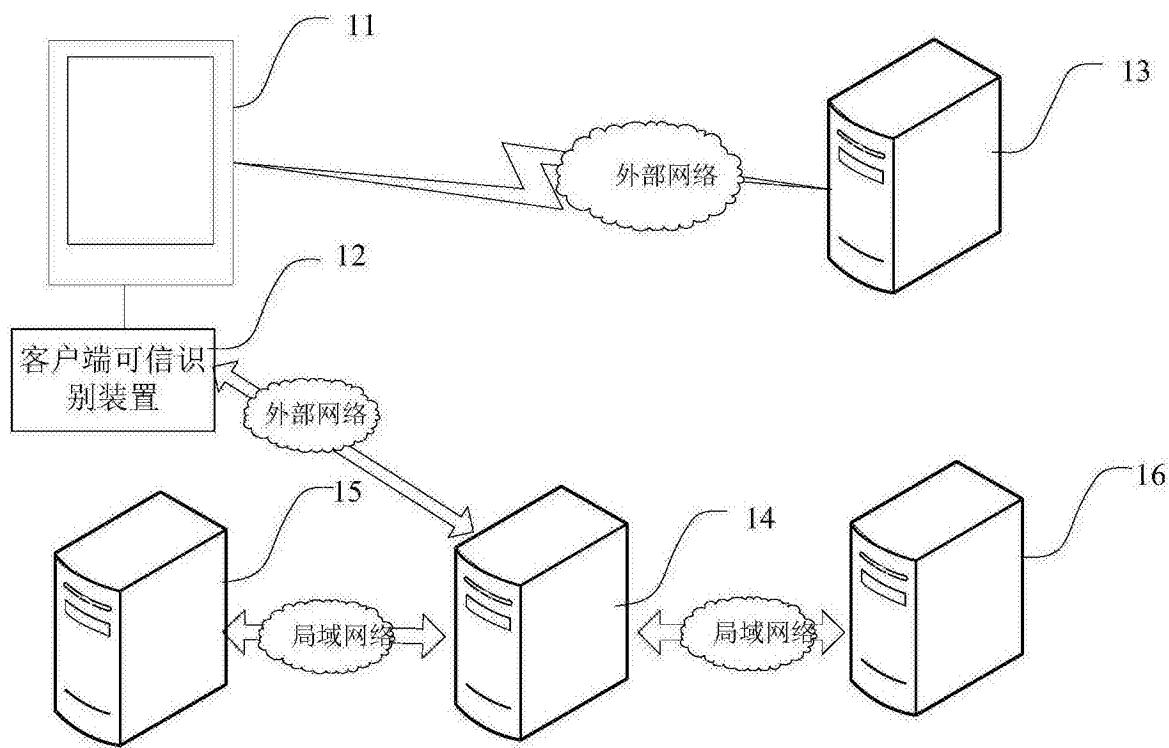


图1

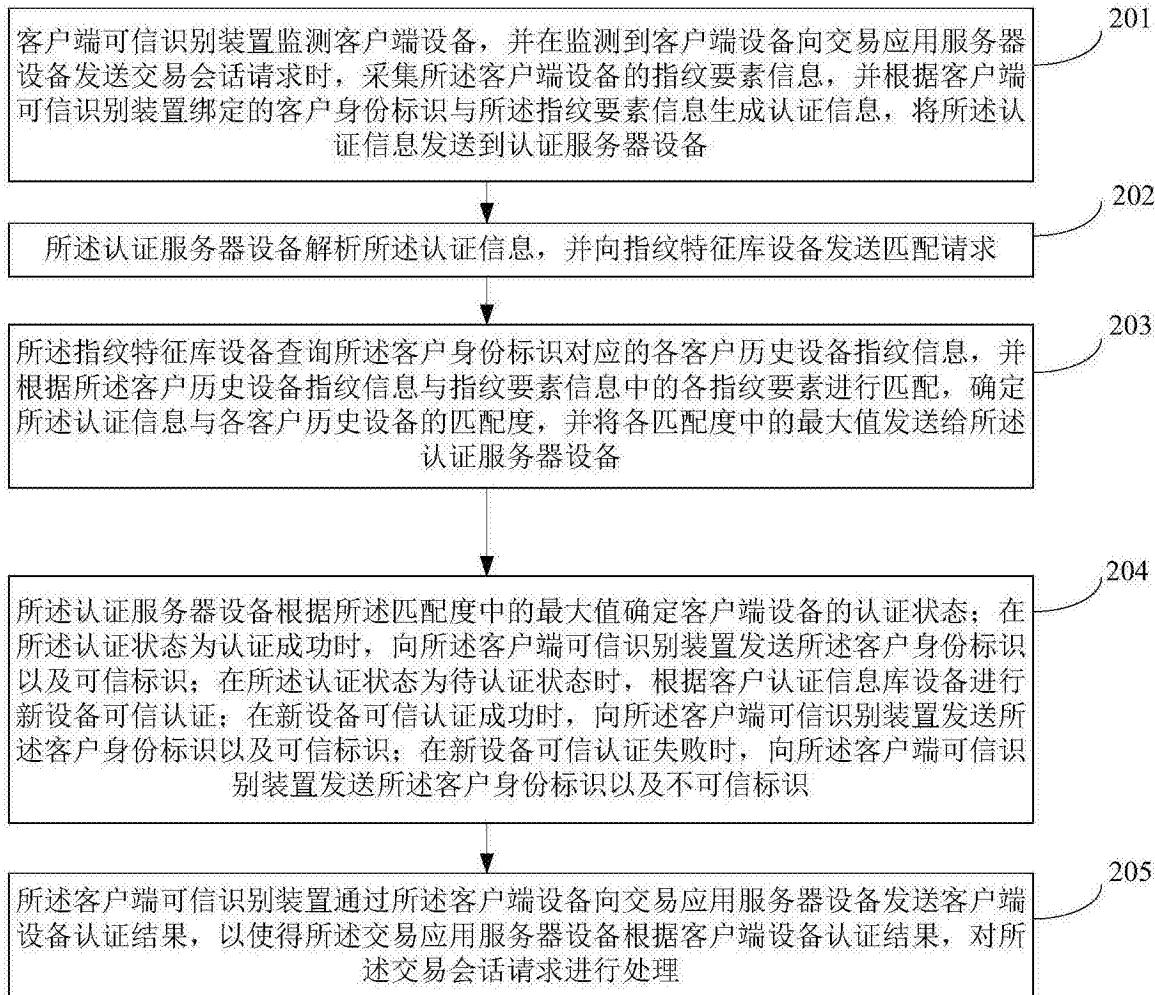


图2

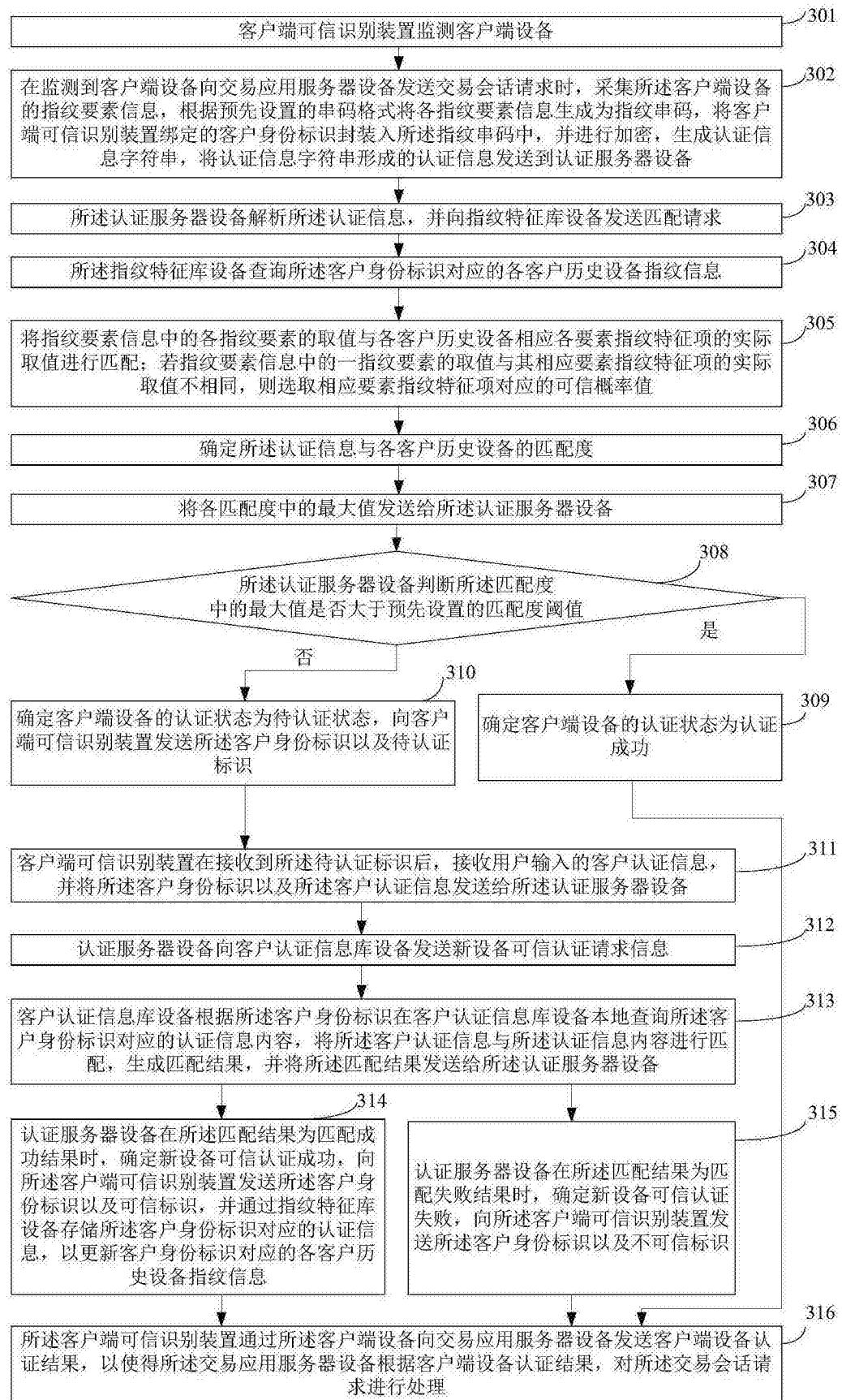


图3

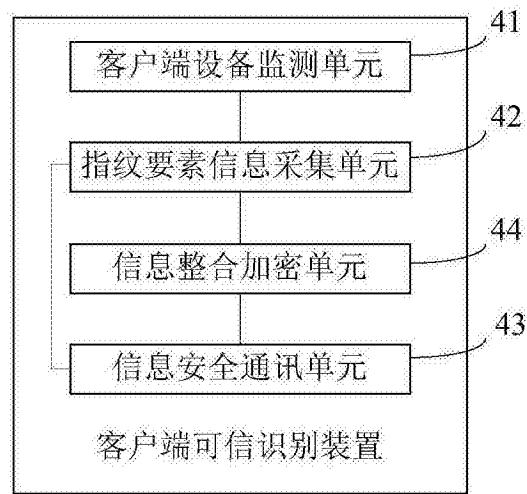


图4