(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 104270359 B
(45)授权公告日 2018.04.17

(21)申请号 201410499859.1

(22)申请日 2014.09.25

(65)同一申请的已公布的文献号
申请公布号 CN 104270359 A

(43)申请公布日 2015.01.07

(73)专利权人 同济大学
地址 200092 上海市杨浦区四平路1239号

(72)发明人 蒋昌俊 陈闵中 闫春钢 丁志军 于汪洋 葛雍龙

(74)专利代理机构 上海天协和诚知识产权代理事务所 31216
代理人 叶凤

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 103699823 A,2014.04.02,
CN 102999572 A,2013.03.27,
US 2006020783 A1,2006.01.26,
CN 103714456 A,2014.04.09,

审查员 尤一名

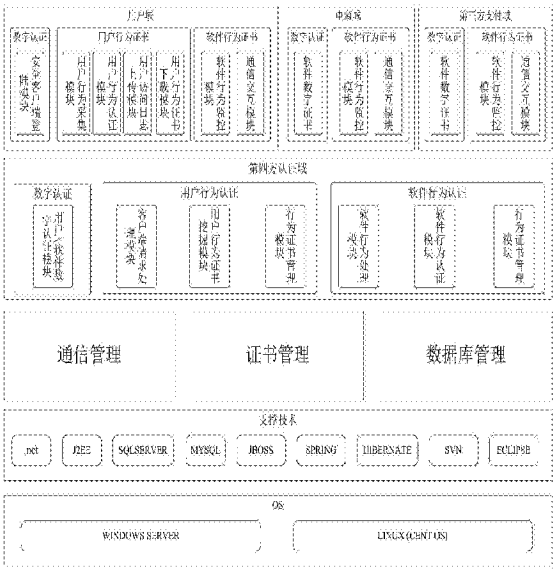
权利要求书1页 说明书4页 附图3页

(54)发明名称

网络交易的可信认证系统与方法

(57)摘要

网络交易的可信认证系统与方法，属于网络交易可信认证技术领域。系统的底层支持Windows和Linux两种主流操作系统；在底层支撑之上是基础管理模块，分别是通信管理模块、证书管理模块和数据库管理模块；在基础管理模块之上，是第四方认证域；还包括用户域、电商域和第三方支付域，等等。可信认证方法包括步骤：1)当网络交易发生时，用户通过登录安全客户端，上传数字证书进行数字认证，电商和第三方支付也同时上传其数字证书进行相应的数字认证；2)当数字认证通过后，用户通过用户行为证书下载模块下载行为证书，三方正式进入交易流程；等等。本发明具有很好的可扩展性、可移植性和通用性，配置、部署灵活方便，无需第三方软件支持。



CN 104270359 B

1.一种网络交易的可信认证系统,其特征在于,

网络交易可信认证系统的底层支持Windows和Linux两种主流操作系统,具有良好的跨平台能力,为上层的应用开发提供了良好的支持;

在底层支撑之上是三个比较底层的基础管理模块,分别是通信管理模块、证书管理模块和数据库管理模块;通信管理模块主要负责根据本系统特定需求对网络通信功能进行封装,为上层提供数据交换通信服务,提供给网络交易中的四方调用,进行数据交换;证书管理模块负责对软件行为证书、用户行为证书以及数字证书进行统一的管理,包括证书的搜索、更新、发布操作;数据库管理模块主要负责更新和维护数据库,提高数据访问效率;

在基础管理模块之上,就是网络交易可信认证系统的第四方认证域,其功能是监控和认证网络交易过程,对交易三方进行数字认证、通过用户行为证书验证用户身份的可信性,通过软件行为证书验证交易三方的网络交易行为的可信性;第四方认证域细分成数字证书、用户行为证书、软件行为证书三个子部分,对网络交易过程进行三重认证;

网络交易可信认证系统还包括另外三个域:用户域、电商域和第三方支付域;用户域主要负责对上传用户数字证书,通过用户行为证书验证用户身份可信性以及采集和上传客户端交易过程中的软件行为;电商域和第三方支付域的功能是上传其数字证书,采集和上传软件行为;

1)当网络交易发生时,用户通过登录安全客户端,上传数字证书进行数字认证,电商和第三方支付也同时上传其数字证书进行相应的数字认证;

2)当数字认证通过后,用户通过用户行为证书下载模块下载行为证书,三方正式进入交易流程;

3)在交易过程中,安全客户端通过用户行为采集模块实时采集用户行为,并交给用户行为认证模块,根据从第四方认证中心下载的该用户行为证书认证用户当前访问行为的可信性;如果认证通过,那么继续采集用户的访问行为,进行认证;若认证不通过,则将详细认证结果上传至认证中心,由认证中心进行审查、判定;同时,通过软件行为采集模块实时采集客户端软件行为,并由通信交互模块上传至认证中心;而电商和第三方支付也同样通过软件行为监控模块实时采集其软件行为,并由通信交互模块上传至认证中心;如果软件行为认证通过,则认证中心发回反馈信息,继续进行交易流程,同时三方软件行为监控继续进行实时采集;若认证不通过,则由认证中心广播通知交易三方交易流程出现异常,并终止交易;

4)当交易完成后,安全客户端由用户访问日志上传新的访问日志至认证中心,当认证中心收到新的访问日志后,发回反馈信息,用户退出安全客户端;

5)接着,认证中心通过证书管理模块调用用户行为证书挖掘模块对新的用户访问日志进行挖掘,更新该用户的行为证书;

当一个新的电商或第三方支付平台加入,则首先对其进行审核,通过后颁发数字证书;接着通过分析其网站源码,挖掘出其相应的软件行为证书,上传至认证中心,由行为证书管理模块统一进行管理。

网络交易的可信认证系统与方法

技术领域

[0001] 本发明涉及网络交易可信认证技术领域。

背景技术

[0002] 随着互联网的飞速发展以及计算机科学技术的不断进步，基于Internet的网络交易也如火如荼地迅猛发展起来，这不仅给我国经济的发展提供了持续的动力，同时也给广大人民的生活带来了极大的便利。越来越多的人通过网络交易和支付方式开展业务活动，网络交易的发展前景十分广阔。

[0003] 然而，由于网络交易和支付平台兴起不久，网络支付的安全体系还不健全，网络交易流程和行为的可信问题也变得越来越突出，已逐渐成为网络交易发展面临的瓶颈问题。在网络交易中可信问题主要包括两个方面，一是用户身份可信问题，即参与网络交易的用户身份是否合法；二是软件可信问题，即网络交易中交易各方的软件本身的行为以及软件之间的交互行为是否是可预期的。针对这两类问题，目前电子商务企业普遍采取的解决方案是数字证书和对软件进行补丁更新或是版本升级。经过调研，以国内某大型网络支付平台公司为例，目前的解决策略在业界的应用存在明显的不足：一是当用户的账户密码被盗后，无法识别黑客盗用用户的账户进行交易，侵害用户利益的用户身份可信问题；二是对系统运行时遇到的不可预期行为时总是无法及时发现并处理。存在这些不足主要原因在于，目前还缺乏一套针对控网络交易的可信认证系统去监控和管理交易各方自身和交易行为。

发明内容

[0004] 本发明面向的情况是当前网络交易用户身份可信问题以及交易各方软件行为可信问题得不到保障，同时缺乏有效监控和管理网络交易可信性的现状，提出采用用户行为证书和软件行为证书来决解认证用户身份可信以及软件行为可信的问题。

[0005] 针对网络交易的可信认证是通过搭建网络交易的第四方认证中心和安全客户端以及在电商网站和支付平台部署软件行为监控器，形成网络交易可信认证系统平台，并制定网络交易可信认证的认证协议。在网络交易可信认证系统中，第四方认证中心主要负责管理用户行为和软件行为证书，认证软件行为的可信性；安全客户端主要负责实时采集用户上网日志、认证用户行为的可行性同时采集网络交易中的客户端软件行为上传至第四方认证中心；软件行为监控器负责实时采集网络交易中电商及支付平台的软件行为并上传至第四方认证中心。

[0006] 本发明给出的技术方案为：

[0007] 一种网络交易的可信认证系统，其特征在于，网络交易可信认证系统底层支持Windows和Linux两种主流操作系统，具有良好的跨平台能力，为上层的应用开发提供了良好的支持。在支撑技术之上是三个比较底层的基础管理模块，分别是通信管理模块、证书管理模块和数据库管理模块。通信管理模块主要负责根据本系统特定需求对网络通信功能进行封装，为上层提供数据交换等通信服务，提供给网络交易中的四方调用，进行数据交换；

证书管理模块负责对软件行为证书、用户行为证书以及数字证书进行统一的管理，包括证书的搜索、更新、发布等操作；数据库管理模块主要负责更新和维护数据库，提高数据访问效率。在基础管理模块之上，就是网络交易可信认证系统的第四方认证域，其主要功能是监控和认证网络交易过程，对交易三方进行数字认证、通过用户行为证书验证用户身份的可信性，通过软件行为证书验证交易三方的网络交易行为的可信性。第四方认证域细分成数字证书、用户行为证书、软件行为证书三个子部分，对网络交易过程进行三重认证。在此之上，则是可信认证系统的另外三个域：用户域、电商域和第三方支付域。用户域主要负责对上传用户数字证书，通过用户行为证书验证用户身份可信性以及采集和上传客户端交易过程中的软件行为。电商域和第三方支付域的主要功能是上传其数字证书，采集和上传软件行为。

[0008] 一种网络交易的可信认证方法，其特征在于，包括步骤：

[0009] 1)当网络交易发生时，用户通过登录安全客户端，上传数字证书进行数字认证，电商和第三方支付也同时上传其数字证书进行相应的数字认证。

[0010] 2)当数字认证通过后，用户通过用户行为证书下载模块下载行为证书，三方正式进入交易流程。

[0011] 3)在交易过程中，安全客户端通过用户行为采集模块实时采集用户行为，并交给用户行为认证模块，根据从第四方认证中心下载的该用户行为证书认证用户当前访问行为的可信性。如果认证通过，那么继续采集用户的访问行为，进行认证；若认证不通过，则将详细认证结果上传至认证中心，由认证中心进行审查、判定。同时，通过软件行为采集模块实时采集客户端软件行为，并由通信交互模块上传至认证中心。而电商和第三方支付也同样通过软件行为监控模块实时采集其软件行为，并由通信交互模块上传至认证中心。如果软件行为认证通过，则认证中心发回反馈信息，继续进行交易流程，同时三方软件行为监控继续进行实时采集；若认证不通过，则由认证中心广播通知交易三方交易流程出现异常，并终止交易。

[0012] 4)当交易完成后，安全客户端由用户访问日志上传新的访问日志至认证中心，当认证中心收到新的访问日志后，发回反馈信息，用户退出安全客户端。

[0013] 5)接着，认证中心通过证书管理模块调用用户行为证书挖掘模块对新的用户访问日志进行挖掘，更新该用户的行为证书。

[0014] 当一个新的电商或第三方支付平台加入，则首先对其进行审核，通过后颁发数字证书；接着通过分析其网站源码，挖掘出其相应的软件行为证书，上传至认证中心，由行为证书管理模块统一进行管理。

[0015] 本发明采用第四方认证中心监控和认证网络交易过程中用户身份和软件行为的可信性。为此，本发明建立了四方网络交易可信认证系统的系统架构，结合数字认证、用户行为认证、软件行为认证对网络交易过程进行三重认证以保证网络交易的可信性和安全性。本发明具有很好的可扩展性、可移植性和通用性，配置、部署灵活方便，无需第三方软件支持。

附图说明

[0016] 图1网络交易可信认证系统架构图。

[0017] 图2网络交易可信认证系统模块部署图。

[0018] 图3网络交易可信认证系统认证流程。

具体实施方式

[0019] (案例)

[0020] 网络交易可信认证系统架构图,如图1所示。

[0021] 如图1所示,网络交易可信认证系统底层支持Windows和Linux两种主流操作系统,因此既可以部署在Window是系统上也可以部署在Linux系统上,具有良好的跨平台能力。支撑技术包括.net、J2EE、SqlServer、MySql、JBoss、SPRING和HIBERNATE等,为上层的应用开发提供了良好的支持。在支撑技术之上是三个比较底层的基础管理模块,分别是通信管理模块、证书管理模块和数据库管理模块。通信管理模块主要负责根据本系统特定需求对网络通信功能进行封装,为上层提供数据交换等通信服务,提供给网络交易中的四方调用,进行数据交换;证书管理模块负责对软件行为证书、用户行为证书以及数字证书进行统一的管理,包括证书的搜索、更新、发布等操作;数据库管理模块主要负责更新和维护数据库,提高数据访问效率。在基础管理模块之上,就是网络交易可信认证系统的第四方认证域,其主要功能是监控和认证网络交易过程,对交易三方进行数字认证、通过用户行为证书验证用户身份的可信性,通过软件行为证书验证交易三方的网络交易行为的可信性。第四方认证域细分成数字证书、用户行为证书、软件行为证书三个子部分,对网络交易过程进行三重认证。在此之上,则是可信认证系统的另外三个域:用户域、电商域和第三方支付域。用户域主要负责对上传用户数字证书,通过用户行为证书验证用户身份可信性以及采集和上传客户端交易过程中的软件行为。电商域和第三方支付域的主要功能是上传其数字证书,采集和上传软件行为。下面给出网络交易可信认证系统的各个功能模块的部署情况以及整个系统运行的认证协议流程,如图2、图3所示。

[0022] 如图2、图3所示,整个网络交易可信认证系统的认证协议流程如下:当网络交易发生时,用户通过登录安全客户端,上传数字证书进行数字认证,电商和第三方支付也同时上传其数字证书进行相应的数字认证。当数字认证通过后,用户通过用户行为证书下载模块下载行为证书,三方正式进入交易流程。在交易过程中,安全客户端通过用户行为采集模块实时采集用户行为,并交给用户行为认证模块,根据从第四方认证中心下载的该用户行为证书认证用户当前访问行为的可信性。如果认证通过,那么继续采集用户的访问行为,进行认证;若认证不通过,则将详细认证结果上传至认证中心,由认证中心进行审查、判定。同时,通过软件行为采集模块实时采集客户端软件行为,并由通信交互模块上传至认证中心。而电商和第三方支付也同样通过软件行为监控模块实时采集其软件行为,并由通信交互模块上传至认证中心。如果软件行为认证通过,则认证中心发回反馈信息,继续进行交易流程,同时三方软件行为监控继续进行实时采集;若认证不通过,则由认证中心广播通知交易三方交易流程出现异常,并终止交易。当交易完成后,安全客户端由用户访问日志上传新的访问日志至认证中心,当认证中心收到新的访问日志后,发回反馈信息,用户退出安全客户端。接着,认证中心通过证书管理模块调用用户行为证书挖掘模块对新的用户访问日志进行挖掘,更新该用户的行为证书。当一个新的电商或第三方支付平台加入,则首先对其进行审核,通过后颁发数字证书;接着通过分析其网站源码,挖掘出其相应的软件行为证书,上

传至认证中心，由行为证书管理模块统一进行管理。

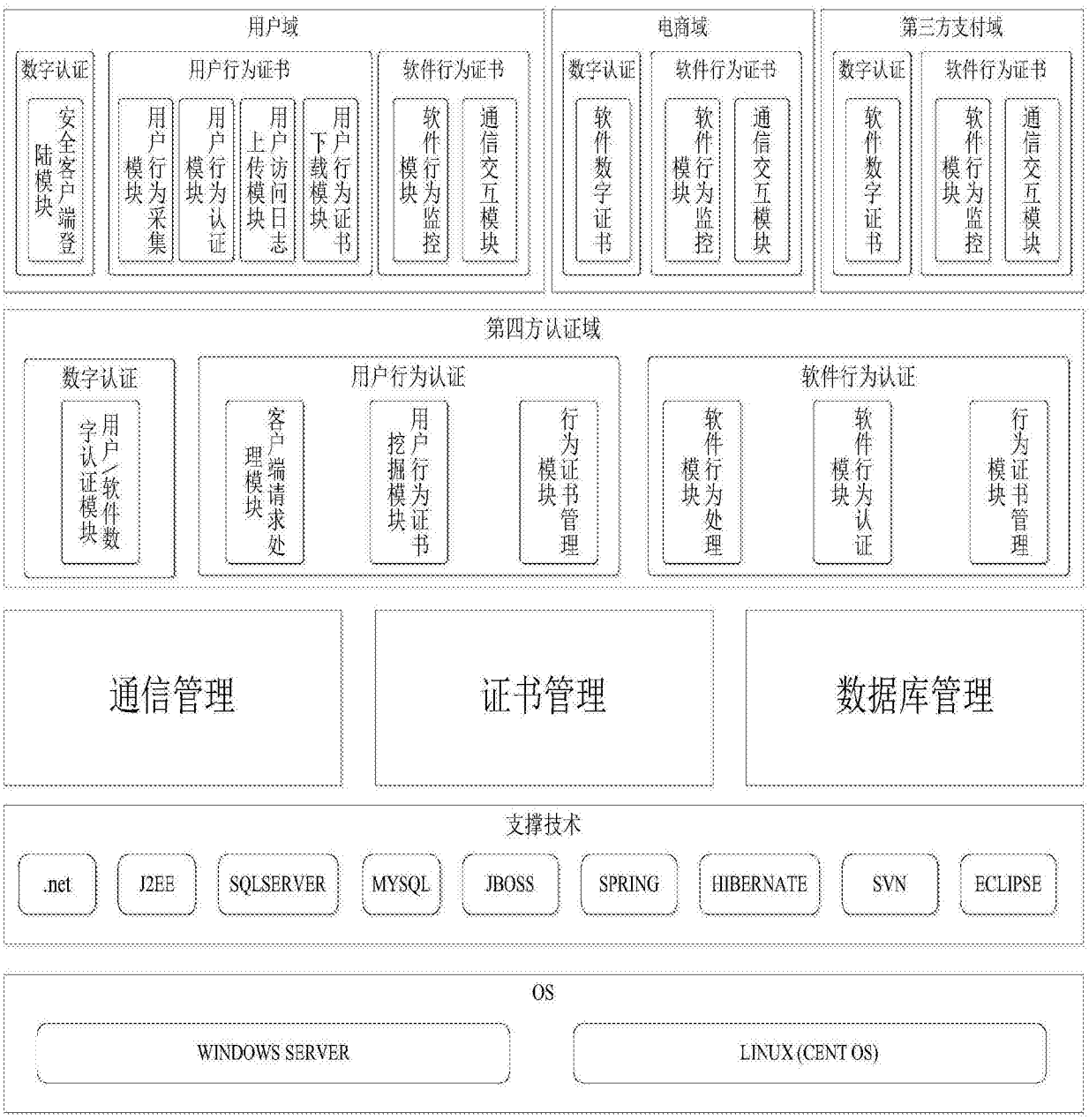

用户域
数字认证
安全客户端登陆模块
用户行为证书
用户行为采集模块
用户行为认证模块
用户访问日志上传模块
用户行为证书下载模块
软件行为证书
软件行为监控模块
通信交互模块
电商域
数字认证
软件数字证书
软件行为证书
软件行为监控模块
通信交互模块
第三方支付域
数字认证
软件数字证书
软件行为证书
软件行为监控模块
通信交互模块
第四方认证域
数字认证
用户/软件数字认证模块
用户行为认证
客户端请求处理模块
用户行为证书挖掘模块
行为证书管理模块
软件行为认证
软件行为处理模块
软件行为认证模块
行为证书管理模块
通信管理
证书管理
数据库管理
支撑技术
.net
J2EE
SQLSERVER
MYSQL
JBOSS
SPRING
HIBERNATE
SVN
ECLIPSE
OS
WINDOWS SERVER
LINUX (CENT OS)

图1

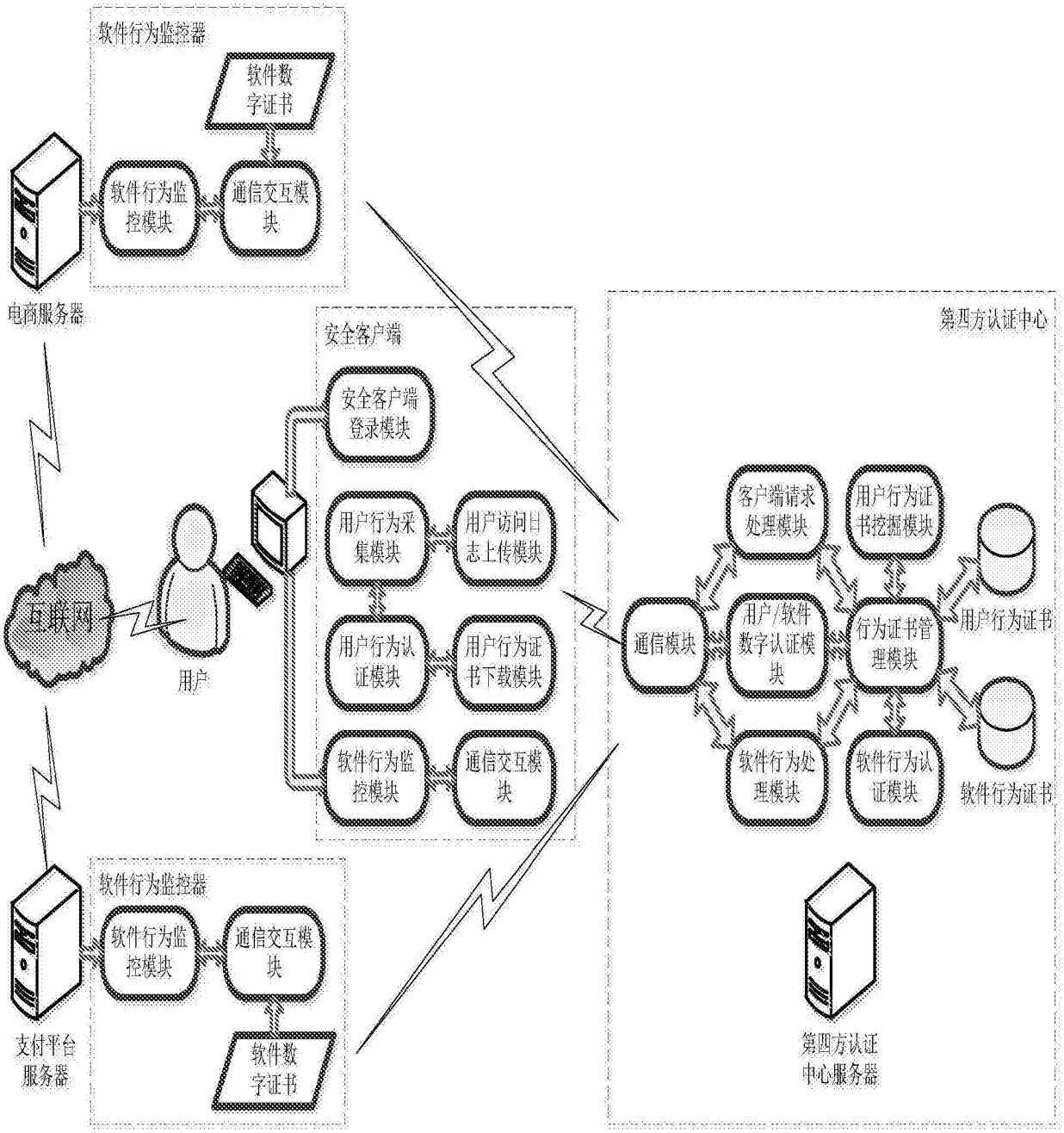

软件行为监控器
软件数字证书
软件行为监控模块
通信交互模块
电商服务器
安全客户端
安全客户端登录模块
用户行为采集模块
用户访问日志上传模块
用户行为认证模块
用户行为证书下载模块
软件行为监控模块
通信交互模块
互联网
用户
第四方认证中心
客户端请求处理模块
用户行为证书挖掘模块
通信模块
用户/软件数字认证模块
行为证书管理模块
用户行为证书
软件行为处理模块
软件行为认证模块
软件行为证书
第四方认证中心服务器
软件行为监控器
软件行为监控模块
通信交互模块
软件数字证书
支付平台服务器

图2

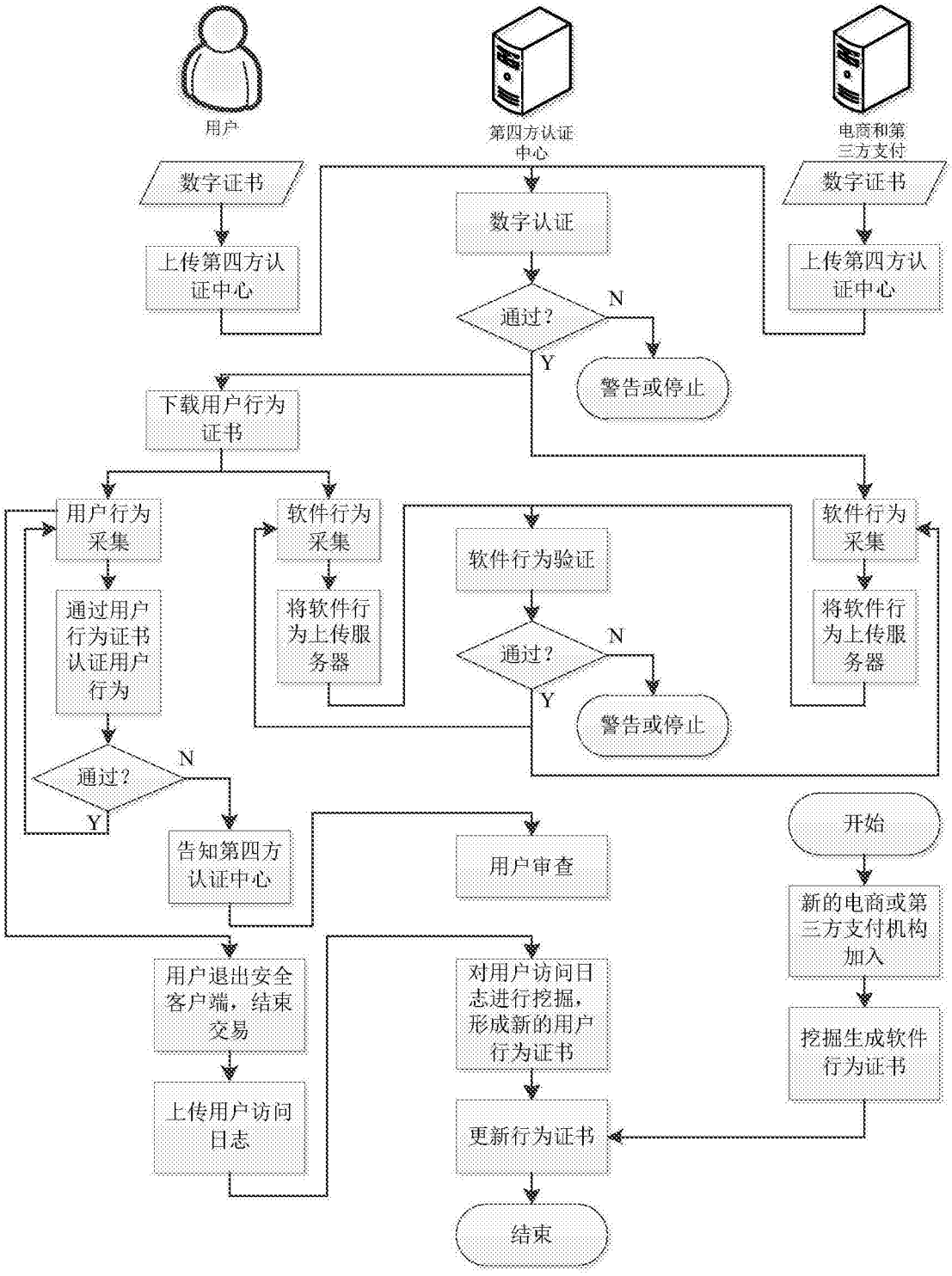

用户
第四方认证中心
电商和第三方支付
数字证书
数字认证
数字证书
上传第四方认证中心
通过？
N
Y
警告或停止
上传第四方认证中心
下载用户行为证书
用户行为采集
软件行为采集
软件行为采集
通过用户行为证书认证用户行为
将软件行为上传服务器
软件行为验证
将软件行为上传服务器
通过？
N
Y
警告或停止
通过？
N
Y
开始
告知第四方认证中心
用户审查
新的电商或第三方支付机构加入
用户退出安全客户端，结束交易
对用户访问日志进行挖掘，形成新的用户行为证书
挖掘生成软件行为证书
上传用户访问日志
更新行为证书
结束

图3