



(12) 发明专利申请

(10) 申请公布号 CN 103532927 A

(43) 申请公布日 2014. 01. 22

(21) 申请号 201310326064. 6

(22) 申请日 2013. 07. 30

(71) 申请人 北京中科金财科技股份有限公司
地址 100083 北京市海淀区学院路 51 号楼
首亨科技大厦 6 层

(72) 发明人 姜啸宇 朱烨东

(74) 专利代理机构 北京联瑞联丰知识产权代理
事务所(普通合伙) 11411
代理人 郑自群

(51) Int. Cl.
H04L 29/06(2006. 01)
H04W 12/00(2009. 01)
G06F 21/50(2013. 01)

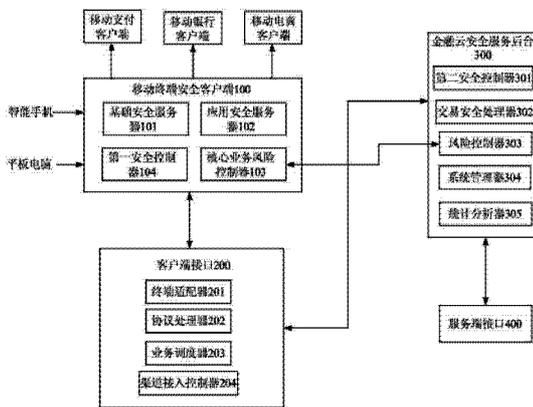
权利要求书2页 说明书4页 附图2页

(54) 发明名称

一种基于移动终端的金融云安全服务平台和数据保护方法

(57) 摘要

本发明提出了一种基于移动终端的金融云安全服务平台和数据保护方法,该平台包括:移动终端安全客户端、客户端接口、金融云安全服务后台和服务端接口,移动终端安全客户端通过客户端接口与金融云安全服务后台进行安全通信,并通过服务端接口实现和第三方的安全连接以及数据传输,移动终端安全客户端用于为移动终端提供防护服务,金融云安全服务后台能够对移动金融交易的危险进行实时采集、分析和处理,本发明可以对引起移动金融安全问题的各个阶段或各种因素,进行不同级别的安全防护和安全管理,确保移动金融业务的全程安全,保障移动金融交易各参与方的权益。



1. 一种基于移动终端的金融云安全服务平台,其特征在于,包括:移动终端安全客户端、客户端接口、金融云安全服务后台和服务端接口,所述移动终端安全客户端通过所述客户端接口与所述金融云安全服务后台进行通信,并通过服务端接口实现和第三方的安全连接和数据传输,其中:

所述移动终端安全客户端用于为移动终端提供防护服务,包括基础安全服务器、应用安全服务器、核心业务风险控制器和第一安全控制器;

所述金融云安全服务后台能够对移动金融交易的危险进行实时采集、分析和处理,包括第二安全控制器、交易安全处理器、风险控制器、系统管理器和统计分析器。

2. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述移动终端安全客户端为移动支付客户端、移动银行客户端或移动电商客户端。

3. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述基础安全服务器采用脱壳技术、自我保护技术、修复技术、实时升级技术、云查杀技术、主动防御技术、启发技术或/和虚拟机技术,结合特征代码法、校验和法、行为检测法和软件模拟法来实现对网络威胁的发现及处理,针对移动金融交易的网络环境中存在的威胁,进行网络层的安全防护,可用于禁止未知风险进程运行、快速鉴定未知风险程序、木马高启发式鉴定、防止页面被篡改、拦截钓鱼、防止键盘输入被记录或/和自动清除痕迹。

4. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述应用安全服务器采用动态软键盘技术,保证输入的安全,防止恶意程序监听或探测用户的屏幕按键选择,能够阻止应用层出现的威胁,保障移动金融交易顺利完成,并针对移动银行或移动支付进行安全分析,提供移动支付或移动银行交易信息的防篡改、交易信息的按键确认、交易信息的签名或/和加密服务。

5. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述核心业务风险控制器采用监控识别技术、统计分析技术或/和人工智能技术,为移动银行或移动支付提供监督以及业务风险控制,通过对风险规则的解析和风险设置,向客户端接口发送预警信息。

6. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述第一安全控制器通过PKI加密技术、安全沙箱和安全文件系统构建自身的安全防护体系,保障移动终端安全客户端不受病毒或木马的攻击。

7. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述客户端接口包括终端适配器、协议处理器、业务调度器和渠道接入控制器。

8. 根据权利要求1所述的一种基于移动终端的金融云安全服务平台,其特征在于,所述第三方为银行、银联、银商或支付公司。

9. 一种基于移动终端的金融云安全服务平台中的数据保护方法,其特征在于,包括:

步骤A:移动终端安全客户端接收来自智能手机或者平板电脑的移动金融应用或者事件;

步骤B:将接收到的移动金融应用或者事件依次通过基础安全服务器进行网络层防护、应用安全服务器进行应用层防护、核心业务风险控制器进行业务层防护;

步骤C:通过客户端接口与金融云安全服务后台进行通信;

步骤D:金融云安全服务后台接收客户端接口转发过来的数据,同时通过服务端接口

实现和第三方安全连接以及数据传输。

一种基于移动终端的金融云安全服务平台和数据保护方法

技术领域

[0001] 本发明涉及移动通讯领域,特别是指一种基于移动终端的金融云安全服务平台和数据保护方法。

背景技术

[0002] 随着金融业务信息化水平的提高和移动终端智能化进程的加快,越来越多的金融业务被植入了移动终端应用中,它的发展已经成为金融业务的一个新趋势。但是,因为网络自身的潜在危险,移动金融业务的开展也受到了极大的威胁,因此引起的各种金融纠纷也是层出不穷。一方面,银行和电商希望抓住这个商机,获取更多的利益,用户也乐于享受这种金融服务带来的方便、快捷,但是,移动金融业务的安全问题始终困扰着大家,严重阻碍了移动金融业务的发展。

发明内容

[0003] 本发明提出一种基于移动终端的金融云安全服务平台和数据保护方法,确保移动金融业务的全程安全,保障移动金融交易各参与方的权益。

[0004] 本发明的技术方案是这样实现的:

[0005] 一种基于移动终端的金融云安全服务平台,其特征在于,包括:移动终端安全客户端、客户端接口、金融云安全服务后台和服务端接口,移动终端安全客户端通过客户端接口与金融云安全服务后台进行通信,并通过服务端接口实现和第三方的安全连接和数据传输,其中:

[0006] 移动终端安全客户端用于为移动终端提供防护服务,包括基础安全服务器、应用安全服务器、核心业务风险控制器和第一安全控制器;

[0007] 金融云安全服务后台能够对移动金融交易的危险进行实时采集、分析和处理,包括第二安全控制器、交易安全处理器、风险控制器、系统管理器和统计分析器。

[0008] 优选的,移动终端安全客户端为移动支付客户端、移动银行客户端或移动电商客户端。

[0009] 优选的,基础安全服务器采用脱壳技术、自我保护技术、修复技术、实时升级技术、云查杀技术、主动防御技术、启发技术或/和虚拟机技术,结合特征代码法、校验和法、行为检测法和软件模拟法来实现对网络威胁的发现及处理,针对移动金融交易的网络环境中存在的威胁,进行网络层的安全防护,可用于禁止未知风险进程运行、快速鉴定未知风险程序、木马高启发式鉴定、防止页面被篡改、拦截钓鱼、防止键盘输入被记录或/和自动清除痕迹。

[0010] 优选的,应用安全服务器采用动态软键盘技术,保证输入的安全,防止恶意程序监听或探测用户的屏幕按键选择,能够阻止应用层出现的潜在威胁,保障移动金融交易地顺利完成,并针对移动银行或移动支付进行安全分析,提供移动支付、移动银行交易信息的防篡改、交易信息的按键确认、交易信息的签名或/和加密服务。

[0011] 优选的,核心业务风险控制器采用监控识别技术、统计分析技术或 / 和人工智能技术,为移动银行或移动支付提供监督以及业务风险控制,通过对风险规则的解析和风险设置,向客户端接口发送预警信息。

[0012] 优选的,第一安全控制器通过 PKI 加密技术、安全沙箱和安全文件系统构建自身的安全防护体系,保障移动终端安全客户端不受病毒或木马的攻击。

[0013] 优选的,客户端接口包括终端适配器、协议处理器、业务调度器和渠道接入控制器。

[0014] 优选的,第三方为银行、银联、银商或支付公司。

[0015] 一种基于移动终端的金融云安全服务平台中的数据保护方法,其特征在于,包括:

[0016] 步骤 A:移动终端安全客户端接收来自智能手机或者平板电脑的移动金融应用或者事件;

[0017] 步骤 B:将接收到的移动金融应用或者事件依次通过基础安全服务器进行网络层防护、应用安全服务器进行应用层防护、核心业务风险控制器进行业务层防护;

[0018] 步骤 C:通过客户端接口与云安全后台进行通信;

[0019] 步骤 D:金融云安全服务后台接收客户端接口转发过来的数据,同时通过服务端接口实现和第三方安全连接以及数据传输。

[0020] 本发明可以对引起移动金融安全问题的各个阶段或各种因素,进行不同级别的安全防护和安全管理,确保移动金融业务的全程安全,保障移动金融交易各参与方的权益。

附图说明

[0021] 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。

[0022] 图 1 为本发明一种基于移动终端的金融云安全服务平台的整体框架图;

[0023] 图 2 为本发明一种基于移动终端的金融云安全服务平台的数据保护方法流程图。

[0024] 图中:

[0025] 100、移动终端安全客户端;101、基础安全服务器;102、应用安全服务器;103、核心业务风险控制器;104、第一安全控制器;200、客户端接口;201、终端适配器;202、协议处理器;203、业务调度器;204、渠道接入控制器;300、金融云安全服务后台;301、第二安全控制器;302、交易安全处理器;303、风险控制器;304、系统管理器;305、统计分析器;400、服务端接口。

具体实施方式

[0026] 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作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。

[0027] 如图 1 所示,移动终端安全客户端 100 可以为移动支付、移动银行或移动 电商客户端提供三层防护服务,切实保障移动金融交易的安全,它能够监听来自智能手机或者平板电脑的移动金融应用或者事件,然后将其依次交由基础安全服务器 101、应用安全服务器 102、核心业务风险控制器 103 进行分级别的安全管理和安全防护。

[0028] 基础安全服务器 101 用于针对网络中的一些病毒或未知进程进行查杀,查杀方法是针对文件、内存和行为三大方面,通过软件技术如脱壳技术、自我保护技术、修复技术、实时升级技术、云查杀技术、主动防御技术、启发技术或 / 和虚拟机技术等,结合病毒发现方法,如特征代码法、校验和法、行为检测法或 / 和软件模拟法来实现对网络威胁的发现及处理。脱壳即去掉软件的外衣,通过脱壳技术可以查找隐藏较深的病毒,云查杀技术即通过将多台接入网络的客户端数据共享,可以在几秒钟之内快速处理数据,因此查杀病毒的时间更快,范围更广。

[0029] 基础安全服务器 101 提供的功能主要有:禁止未知风险进程运行、快速鉴定未知风险程序、木马高启发式鉴定、防止页面被篡改、拦截钓鱼、防止键盘输入被记录或 / 和自动清除痕迹。它主要是针对移动金融交易的网络环境中存在的威胁,进行网络层的安全防护,保障移动金融交易在一个安全的网络环境中进行。

[0030] 应用安全服务器 102 结合具体的金融应用,对交易流程中的一些敏感数据,如银行卡号或密码进行加解密处理,同时,采用动态软键盘技术,保证输入的安全,防止恶意程序监听或探测用户的屏幕按键选择,并且,通讯报文采用数字证书全程加密,防止数据在传输过程中被窃取。动态软键盘即通过软件模拟的键盘的功能,并且按键键位可以动态的随机显示。

[0031] 应用安全服务器 102 用于针对移动银行或移动支付进行安全分析,提供移动支付、移动银行交易信息的防篡改、交易信息的按键确认或交易信息的签名及加密防护服务,它主要是针对移动金融交易的具体应用,能够有效阻止应用层出现的潜在威胁,保障移动金融交易地顺利完成。

[0032] 核心业务风险控制器 103 通过监控识别技术、统计分析技术或 / 和人工智能技术对异常行为进行检测,建立相应的案例库和风险模型,通过有序的规则对其进行解析,当达到风险设置的级别后,如频繁性交易,就可以发出风险预警和采取一定的控制措施,如给当前账户发送短消息。

[0033] 核心业务风险控制器 103 能够为移动银行或移动支付提供事后监督以及业务风险控制,通过对风险规则的解析和风险设置,能够向移动金融客户端发送预警信息,同时能够和风险控制器 103 进行数据的传输和交互,把前端采集到的风险信息交由金融云安全服务后台 300 处理,丰富风险案例库并制定具体的风险控制措施,而金融云安全服务后台 300 也能够实时地对前端的风险规则和风险设置进行更新,从而规避业务处理过程中出现的风险。

[0034] 安全控制器 104 通过 PKI 加密技术、安全沙箱和安全文件系统构建自身的安全防护体系,保障移动终端安全客户端不受病毒或木马的攻击,同时,安全控制器 104 接收客户端三层防护体系处理后的结果,然后通过客户端接口 200 和移动金融云安全服务后台 300 进行安全通信,完成数据的转发处理。PKI 是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范,用户可利用 PKI 加密技术进行安全通信。

[0035] 客户端接口 200 用于移动终端安全客户端 100 的数据接收和转发处理、终端适配、协议适配和渠道接入控制。其中,终端适配器 201 用于手机支付平台网关子系统对手机终端类型的通信和接入适配;协议处理器 202 负责通信协议管理,手机客户端与手机支付网关子系统采用 https 的数据连接方式进行信息传递;业务调度器 203 用于保障整个事件处理流程的有序进行,确保系统资源能够被有效利用;渠道接入控制器 204 负责移动终端安全客户端 100 渠道号的管理和接入控制,确保移动终端安全客户端 100 分发渠道的接入控制和管理。

[0036] 金融云安全服务后台 300 能够对移动金融交易的危险进行实时采集、分析和处理,实现信息在移动智能终端、交易支付、网络传输等过程中的安全防护。金融云安全服务后台 300 支持国际和国内加密算法,覆盖移动平台,能够为移动金融安全客户端 100 提供服务支撑,实现安全管理、应用安全、IT 支撑系统安全、基础设施安全和安全运维功能。金融云安全服务后台 300 包括安全控制器 301、交易安全处理器 302、风险控制器 303、系统管理器 304 和统计分析器 305。其中,安全控制器 301 负责金融云安全服务后台 300 的安全控制,包括证书管理、数据的加密、数据的解密、签名或验签;交易安全处理器 302 负责安全交易的后台处理;风险控制器 303 能够为移动终端安全客户端 100 提供风险的控制服务,包括风险监控、风险案例库管理、风险控制措施实施、风险模型配置和风险名单管理;系统管理器 304 负责对整个金融云安全服务平台的系统管理,包括权限管理、配置管理、机构管理、用户管理和客户端管理;统计分析器 305 负责为项目提供各种统计报表进行分析,包括运营统计报表、风险事件监测报表和日志报表。

[0037] 本发明实施例的一种基于移动终端的金融云安全服务平台的数据保护方法,如图 2 所示,首先,移动终端安全客户端 100 接收来自智能手机或者平板电脑的移动金融应用或者事件;此后,将接收到的移动金融应用或者事件依次通过基础安全服务器进行网络层防护、应用安全服务器进行应用层防护、核心业务风险控制器进行业务层防护并通过客户端接口 200 与金融云安全服务后台 300 进行通信;金融云安全服务后台 300 接收客户端接口 200 转发过来的数据,同时通过服务端接口 400 实现和银行、银联、银商或支付公司的安全连接以及数据传输,然后在金融云安全服务后台 300 中进行交易安全、风险控制、系统管理和统计分析处理,从而保障移动金融交易地顺利完成。

[0038] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,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。

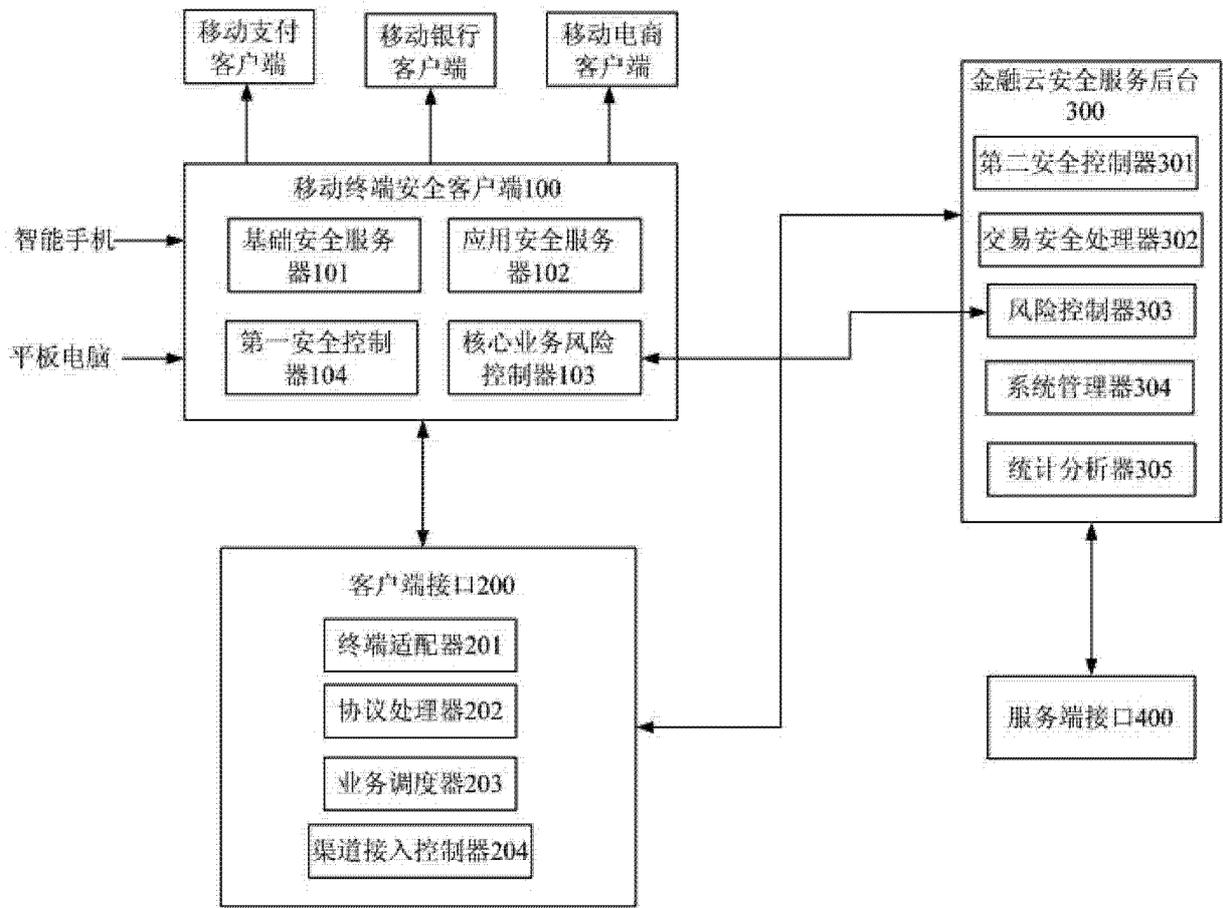


图 1

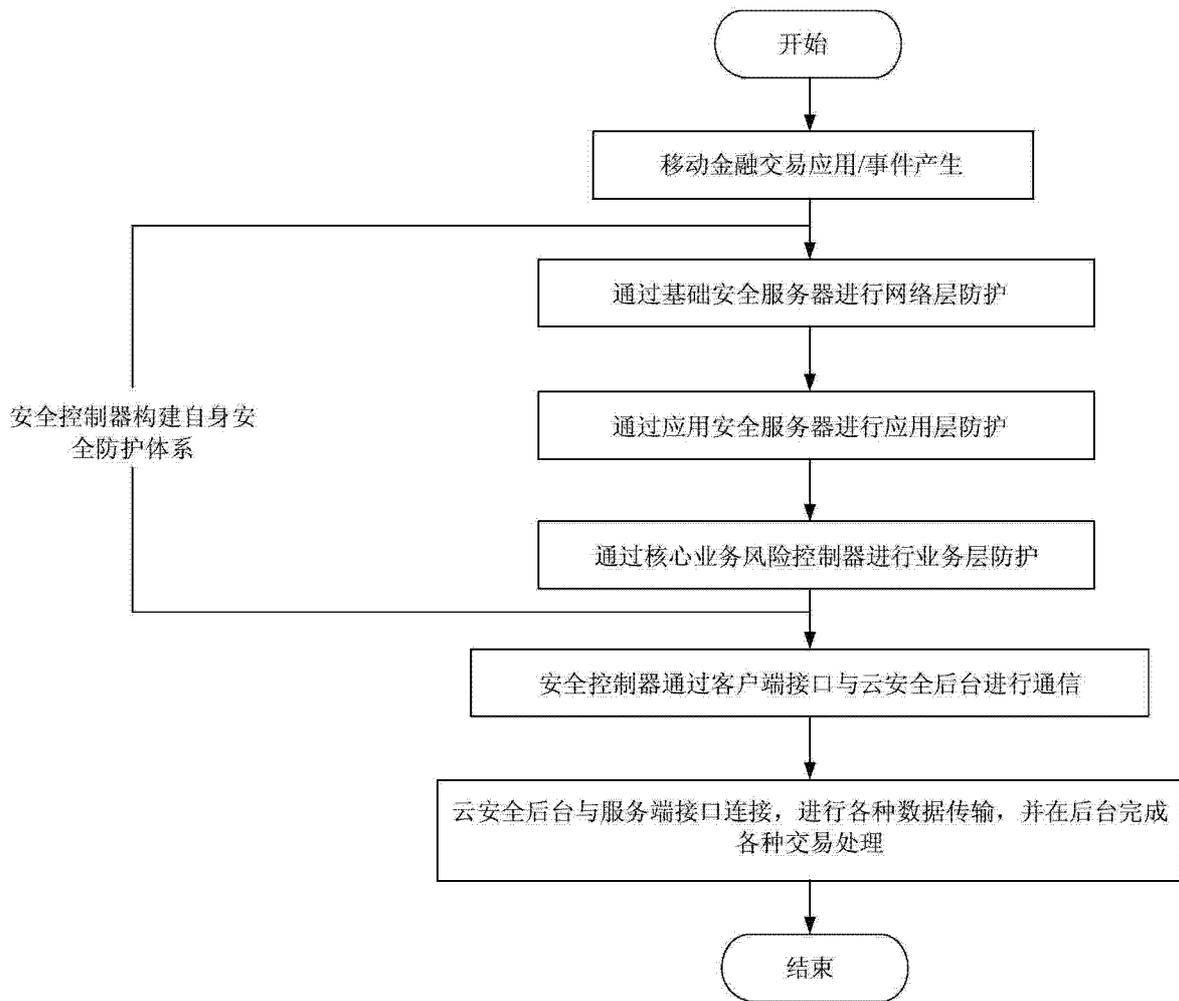


图 2