(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102708321 A
(43)申请公布日 2012.10.03

(21)申请号 201210138249.X

(22)申请日 2012.05.07

(71)申请人 成都国腾实业集团有限公司
地址 610041 四川省成都市高新技术开发区西部园区西芯大道3号

(72)发明人 武志学 李志 赵阳 周静 吴开强

(74)专利代理机构 成都金英专利代理事务所（普通合伙） 51218
代理人 袁英

(51)Int.Cl.
G06F 21/00(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)

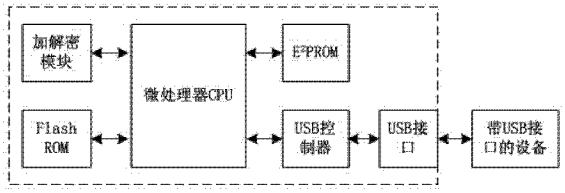
权利要求书 1 页 说明书 2 页 附图 1 页

(54)发明名称

云终端安全钥匙

(57)摘要

本发明公开了一种云终端安全钥匙，它包括机壳和置于机壳内的机芯电路，所述的机芯电路包括微处理器，以及与微处理器连接的E^2PROM、FlashROM、USB控制器、加解密模块，所述的机壳上设有USB接口，USB控制器通过USB接口与外部带USB接口的设备连接。本发明采用可信密码学技术，既能防范通信被截获破解，又支持对加解密“算法”和密钥本身进行可信模式识别认证，采用非对称密钥算法对网上数据进行加密解密、用户身份与终端绑定、完整性认证检查，用户使用任意可接入网络的PC或笔记本的USB接口，自动启动该设备内的加、解密程序，验证终端用户账户和密码的合法性，保障云终端用户和云计算服务器之间的对话安全。



CN 102708321 A

1. 云终端安全钥匙，其特征在于：它包括机壳和置于机壳内的机芯电路，所述的机芯电路包括微处理器、E^2PROM、Flash ROM、USB 控制器和加解密模块，所述的机壳上设有一个或多个 USB 接口，微处理器分别通过内部总线与 E^2PROM、Flash ROM、USB 控制器、加解密模块电连接，USB 控制器通过 USB 接口与外部带 USB 接口的设备连接。

云终端安全钥匙

技术领域

[0001] 本发明涉及一种云终端安全钥匙。

背景技术

[0002] 云计算(cloud computing)是一种基于互联网的计算方式,通过这种方式,共享的软硬件资源和信息可以按需提供给计算机和其他设备。云计算的核心思想是将大量用网络连接的计算资源统一管理和调度,构成一个计算资源池,按用户需求向用户提供服务。

[0003] 云计算为用户提供了一种新的高效率计算模式,兼有互联网服务的便利、廉价和大型机的能力。它的目的是将资源集中于互联网上的数据中心,由这种云中心提供应用层、平台层和基础设施层的集中服务。云计算强调信息资源的聚集、优化、动态分配和回收,旨在节约信息化成本、降低能耗、减轻用户信息化的负担,提高数据中心的效率。云计算的出现解决了特定大规模数据处理问题。

[0004] 云计算由于其用户、信息资源的高度集中。用户的数据存储、处理、网络传输等都与云计算系统有关,如果发生关键或隐私信息丢失、窃取,对用户来说无疑是致命的,如何保证云服务提供商内部的安全管理和访问控制机制符合客户的安全需求,如何实施有效的安全审计,对数据操作进行安全监控,如何避免云计算环境中多用户共存带来的潜在风险都成为云计算环境所面临的安全挑战。

[0005] 目前人们利用云计算服务器的强大计算能力,加强终端用户授权的安全,当终端用户申请授权时,云服务器可针对每个不同的用户,采用不同的加密体系进行授权加密,终端设备只需要进行加密体系和用户身份的确认,即可实现解密。

发明内容

[0006] 本发明的目的即在于克服现有技术的不足,提供一种云终端安全钥匙,是安全开启云大门的方便之匙,是云平台接入的终端设备。通过使用云终端安全钥匙,启动安全钥匙系统,用户可以使用任意可接入网络的 PC 或笔记本设备,安全便捷的连接到云计算服务器端专有的云桌面中,有效利用系统的计算资源,用户登录后进行远程接入认证,授权后登入云平台,使用云端服务,进行各种操作,而不必担心通常的病毒、文件丢失或被窃取,以及设备丢失所带来的安全问题。

[0007] 本发明的目的通过以下技术方案来实现 :云终端安全钥匙,它包括机壳和置于机壳内的机芯电路,所述的机芯电路包括微处理器、E^2PROM、Flash ROM、USB 控制器和加解密模块,所述的机壳上设有一个或多个USB 接口,微处理器分别通过内部总线与E^2PROM、Flash ROM、USB 控制器、加解密模块电连接,USB 控制器通过 USB 接口与外部带 USB 接口的设备连接。

[0008] 本发明的有益效果是 :

(1)本发明提供一种软硬件高度集成的一体化的云终端安全钥匙,遵照国家云计算建设技术指标与安全规范设计产品要求,是一种对软硬件进行加密的安全产品,内置微型处

理器 CPU，采用非对称密钥算法，对网上数据进行加密解密、用户身份与终端绑定、完整性认证检查和密码验证；

（2）本发明提供一种云终端安全钥匙，为了防止用户终端与数据中心的互动通信被第三者截获破解，把密码学技术扩展为可信密码学技术，该技术既能防范通信被截获破解，又支持对加解密“算法”和密钥本身进行可信模式识别认证；

（3）本发明提供一种云终端安全钥匙，任意插入可以接入网络的 PC 或笔记本的 USB 接口，自动启动该设备内的加密和解密程序，验证终端用户账户和密码的合法性，保障云终端用户和云计算服务器之间的对话安全。

附图说明

[0009] 图 1 为本发明的结构框图。

具体实施方式

[0010] 下面结合附图对本发明做进一步的描述，但本发明的保护范围不局限于以下所述。

[0011] 如图 1 所示，云终端安全钥匙，它包括机壳和置于机壳内的机芯电路，所述的机芯电路包括微处理器 CPU、E^2PROM、Flash ROM、USB 控制器和加解密模块，所述的机壳上设有一个或多个 USB 接口，微处理器 CPU 分别通过内部总线与 E^2PROM、Flash ROM、USB 控制器、加解密模块电连接，USB 控制器通过 USB 接口与外部带 USB 接口的设备连接，所述的外部带 USB 接口的设备可为 PC、笔记本电脑等。

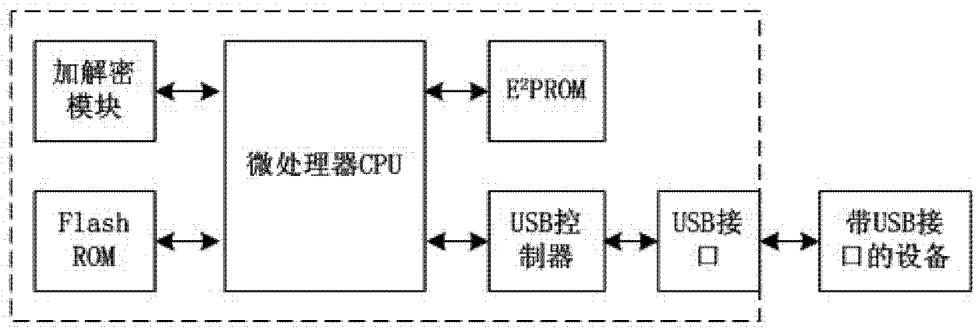


图 1