(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 106982191 A
(43)申请公布日 2017.07.25

(21)申请号 201610029953.X

(22)申请日 2016.01.18

(71)申请人 天津赞普科技股份有限公司
地址 300000 天津市滨海新区华苑产业区榕苑路2号4-302

(72)发明人 梁肇亮 张寿权 王洋 杨勇健

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04W 12/06(2009.01)
H04W 12/08(2009.01)
H04W 84/12(2009.01)
H04W 88/08(2009.01)

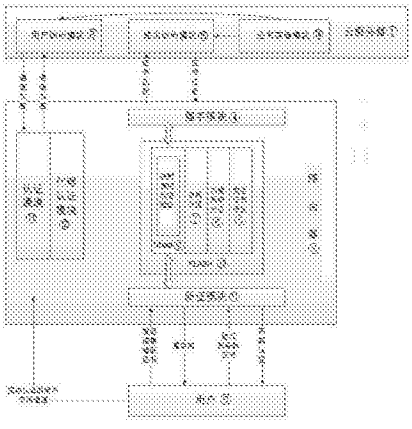
权利要求书2页 说明书4页 附图3页

(54)发明名称

用于商业WiFi的内嵌证书安全认证通讯机制

(57)摘要

本发明属于路由器技术领域，尤其涉及一种用于商业WiFi的内嵌证书安全认证通讯机制，包括用户、云服务器、路由器；所述用户用于通过使用设备内嵌证书与路由器建立基于SSL安全套接字握手的连接方式；所述云服务器包括证书存储模块、路由访问模块、用户访问模块；路由器包括握手模块、代理认证模块、认证通道、验证模块、嵌入设备Flash。本发明中用户访问网络，需接入路由，而在接入路由的时候，用户可以通过证书来判断设备的安全性，而这种判断也可由客户端来完成，防止用户访问假路由器。



CN 106982191 A

1.一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于，包括用户、云服务器、路由器；

所述用户用于通过使用设备内嵌证书与路由器建立基于SSL安全套接字握手的连接方式，可以通过证书来判断设备的安全性，用户通过307报文将用户重定向到认证服务器，用户与服务器之间的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密；

所述云服务器包括证书存储模块、路由访问模块、用户访问模块；所述证书存储模块内嵌了与路由器相互匹配的证书，所述路由访问模块用于通过对路由器进行证书匹配验证，防止假路由器伪装欺骗云服务器，所述用户访问模块用于将与用户的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密处理；

所述路由器内嵌了与云服务器相互匹配的证书，可以通过证书判断云服务器是不是他人伪造的云服务器，防止假云服务器伪装欺骗路由器，路由器包括握手模块、代理认证模块、认证通道、验证模块、嵌入设备Flash；所述嵌入设备Flash由 Uboot分区、系统分区、功能系统分区、安全证书分区组成，用于使用存储方式固定地址定位方式对证书和该设备的MAC地址进行存储，并且使用BAS64对该分区数据进行加密。

2.根据权利要求1所述的一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于：所述Uboot分区用于根据系统引导支持NFS挂载、RAMDISK形式的根文件系统、基本辅助功能强大的操作系统接口功能、CRC32校验可校验FLASH中内核、RAMDISK镜像文件是否完好、上电自检功能SDRAM、FLASH大小自动检测、SDRAM故障检测、特殊功能XIP内核引导。

3.根据权利要求1所述的一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于：所述系统分区用于系统内嵌配置、系统的故障检测还有系统的核心功能管理。

4.根据权利要求1所述的一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于：所述功能系统分区用于系统的功能列表、根据系统的需求进行升级、并有云备份和云配置的功能。

5.根据权利要求1所述的一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于：所述安全证书分区用于系统直接内嵌CA认证证书，HTTPS安全传输认证，结合现有浏览器内置证书认证检测，防止钓鱼设备冒充欺骗，并且支持第三方APP无缝结合接口，三方APP只需要对内嵌证书进行核对就可以防止钓鱼AP的欺骗服务。

6.根据权利要求1所述的一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于：所述Uboot分区中内置一个启动映射进程，在设备启动时通过Uboot分区调用启动映射进程，将安全证书分区内容加载到一段指定内存地址位中，在系统启动后将所述指定内存地址位移交给证书验证进程；证书验证进程通过连接云端认证服务器向服务器提交本机MAC地址和证书加密分区内容，由云端认证服务器进行解密，然后将对应的解密秘钥发还给证书验证进程，证书验证进程根据秘钥对数据解密，同时将解密结果中的设备MAC地址信息和本机设备进行验证，然后将解密数据以虚拟文件的形式映射到认证服务指定的目录中，之后进入正常认证业务流程，认证业务流程也会对解密的证书和设备MAC地址进行校验，通过307报文将用户重定向到认证服务器，服务器提供的证书会在用户的浏览器或是客户端中被验证出来，从而用户可以看到自己的上网环境是否安全。

7.根据权利要求1所述的一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于：所述证书安全分区内将要存储的BAS64加密信息和设备的MAC地址，预先生成，然后使用芯片烧写器对固定位地址内信息直接替换。

用于商业WiFi的内嵌证书安全认证通讯机制

技术领域

[0001] 本发明属于路由器技术领域，尤其涉及用于商业WiFi的内嵌证书安全认证通讯机制。

背景技术

[0002] 现在市场上几乎100%的免费WiFi网络运营商，都没有解决免费WiFi系统安全接入的问题。由于免费WiFi为了满足“开放性”这个业务主体性质，主要以开放的免认证的WiFi热点为基础依托，使用明文Http流进行认证，不会对认证过程数据进行加密，只通过域名和MAC地址对认证服务器与接入节点设备(AP)进行简单识别，并且使用无密码保护的免认证WiFi接入模式WiFi。

[0003] 目前的路由器认证机制使用免密码认证的WiFi接入模式，全部数据都是明文传输，且由于WiFi的工作特点，全部数据以广播模式进行传输，别人可以简单的使用从网络上下载的网络监听工具来获取到全部用户的通讯数据，然后通过数据分析软件的解析，近而得到用户使用行为与隐私信息，根据数据分析软件处理和解密能力甚至可以清楚地截取用户消费密码等重要信息，其安全性能非常差。

发明内容

[0004] 本发明提供一种用于商业WiFi的内嵌证书安全认证通讯机制，以解决上述背景技术中目前的路由器认证机制使用免密码认证的WiFi接入模式，全部数据都是明文传输，安全性能差的问题。

[0005] 本发明所解决的技术问题采用以下技术方案来实现：本发明提供一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于，包括用户、云服务器、路由器；

所述用户用于通过使用设备内嵌证书与路由器建立基于SSL安全套接字握手的连接方式，可以通过证书来判断设备的安全性，用户通过307报文将用户重定向到认证服务器，用户与服务器之间的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密；

所述云服务器包括证书存储模块、路由访问模块、用户访问模块；所述证书存储模块内嵌了与路由器相互匹配的证书，所述路由访问模块用于通过对路由器进行证书匹配验证，防止假路由器伪装欺骗云服务器，所述用户访问模块用于将与用户的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密处理；

所述路由器内嵌了与云服务器相互匹配的证书，可以通过证书判断云服务器是不是他人伪造的云服务器，防止假云服务器伪装欺骗路由器，路由器包括握手模块、代理认证模块、认证通道、验证模块、嵌入设备Flash；所述嵌入设备Flash由 Uboot分区、系统分区、功能系统分区、安全证书分区组成，用于使用存储方式固定地址定位方式对证书和该设备的MAC地址进行存储，并且使用BAS64对该分区数据进行加密。

[0006] 进一步的，所述Uboot分区用于根据系统引导支持NFS挂载、RAMDISK形式的根文件系统、基本辅助功能强大的操作系统接口功能、CRC32校验可校验FLASH中内核、RAMDISK镜像文件是否完好、上电自检功能SDRAM、FLASH大小自动检测、SDRAM故障检测、特殊功能XIP内核引导；

进一步的，所述系统分区用于系统内嵌配置、系统的故障检测还有系统的核心功能管理；

进一步的，所述功能系统分区用于系统的功能列表、根据系统的需求进行升级、并有云备份和云配置的功能；

进一步的，所述安全证书分区用于系统直接内嵌CA认证证书，HTTPS安全传输认证，结合现有浏览器内置证书认证检测，防止钓鱼设备冒充欺骗，并且支持第三方APP无缝结合接口，三方APP只需要对内嵌证书进行核对就可以防止钓鱼AP的欺骗服务。

[0007] 进一步的，所述Uboot分区中内置一个启动映射进程，在设备启动时通过Uboot分区调用启动映射进程，将安全证书分区内容加载到一段指定内存地址位中，在系统启动后将所述指定内存地址位移交给证书验证进程；证书验证进程通过连接云端认证服务器向服务器提交本机MAC地址和证书加密分区内容，由云端认证服务器进行解密，然后将对应的解密秘钥发还给证书验证进程，证书验证进程根据秘钥对数据解密，同时将解密结果中的设备MAC地址信息和本机设备进行验证，然后将解密数据以虚拟文件的形式映射到认证服务指定的目录中，之后进入正常认证业务流程，认证业务流程也会对解密的证书和设备MAC地址进行校验，通过307报文将用户重定向到认证服务器，服务器提供的证书会在用户的浏览器或是客户端中被验证出来，从而用户可以看到自己的上网环境是否安全。

[0008] 进一步的，所述证书安全分区内将要存储的BAS64加密信息和设备的MAC地址，预先生成，然后使用芯片烧写器对固定位地址内信息直接替换。

[0009] 本发明的有益效果为：

1、本发明将路由器和云服务器内嵌入了相互匹配的证书，防止了恶意攻击、大量连接等问题，大大提高了整体的安全性。

[0010] 2、本发明中用户访问网络，需接入路由，而在接入路由的时候，用户可以通过证书来判断设备的安全性，而这种判断也可由客户端来完成，防止用户访问假路由器。

[0011] 3、本发明中用户可以在路由器或是交换机内验证证书的安全性，而不是仅仅的通过由服务器提供的portal页面，防止了热点利用服务器证书进行欺骗。

[0012] 4、本发明通过307报文将用户重定向到认证服务器，服务器提供的证书会在用户的浏览器或是客户端中被验证出来，从而用户可以看到自己的上网环境是否安全。

[0013] 5、本发明用户与服务器之间的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密，不仅从途径上阻止了监听，更是从内容上彻底阻止了监听。

[0014] 6、本发明的云服务器可以通过证书对路由器进行验证而防止了恶意攻击、大量连接等问题，因为证书阻挡了一部分的验证不能通过的设备，今儿大大地节约了设备的负载量。

[0015] 7、本发明在数据通讯层面上提供了的基于该嵌入数字证书且兼容IEEE802.1X标准的“基于证书的通信加密”，可以大大加大的本地数据监听的难度，进一步在用户接入阶

段对用户数据提供保护。

附图说明

[0016] 图1是本发明的内嵌证书安全认证通讯机制结构框图；

图2是本发明的内嵌证书安全认证通讯机制的连接图；

图3是本发明的内嵌证书安全认证通讯机制的流程图。

具体实施方式

[0017] 以下结合附图对本发明做进一步描述：

图中：1-云服务器，2-路由器，3-用户，4-握手模块，5-安全证书分区，6-功能系统分区，7-系统分区，8-用户访问模块，9- Uboot分区，10-嵌入设备Flash，11-验证模块，12-，代理认证模块，13-认证通道，14-证书存储模块，15-路由访问模块。

[0018] 实施例：

本实施例包括：一种用于商业WiFi的内嵌证书安全认证通讯机制，其特征在于，包括用户3、云服务器1、路由器2；

用户3用于通过使用设备内嵌证书与路由器2建立基于SSL安全套接字握手的连接方式，可以通过证书来判断设备的安全性，用户3通过307报文将用户3重定向到认证服务器，用户3与服务器之间的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密；

云服务器1包括证书存储模块14、路由访问模块15、用户访问模块8；证书存储模块14内嵌了与路由器2相互匹配的证书，路由访问模块15用于通过对路由器2进行证书匹配验证，防止假路由器2伪装欺骗云服务器1，用户访问模块8用于将与用户3的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密处理；

路由器2内嵌了与云服务器1相互匹配的证书，可以通过证书判断云服务器1是不是他人伪造的云服务器1，防止假云服务器1伪装欺骗路由器2，路由器2包括握手模块4、代理认证模块12、认证通道13、验证模块11、嵌入设备Flash10；嵌入设备Flash10由 Uboot分区9、系统分区7、功能系统分区76、安全证书分区5组成，用于使用存储方式固定地址定位方式对证书和该设备的MAC地址进行存储，并且使用BAS64对该分区数据进行加密。

[0019] Uboot分区用于根据系统引导支持NFS挂载、RAMDISK形式的根文件系统、基本辅助功能强大的操作系统接口功能、CRC32校验可校验FLASH中内核、RAMDISK镜像文件是否完好、上电自检功能SDRAM、FLASH大小自动检测、SDRAM故障检测、特殊功能XIP内核引导；

系统分区7用于系统内嵌配置、系统的故障检测还有系统的核心功能管理；

功能系统分区76用于系统的功能列表、根据系统的需求进行升级、并有云备份和云配置的功能；

安全证书分区5用于系统直接内嵌CA认证证书，HTTPS安全传输认证，结合现有浏览器内置证书认证检测，防止钓鱼设备冒充欺骗，并且支持第三方APP无缝结合接口，三方APP只需要对内嵌证书进行核对就可以防止钓鱼AP的欺骗服务。

[0020] Uboot分区中内置一个启动映射进程，在设备启动时通过Uboot分区调用启动映射

进程，将安全证书分区5内容加载到一段指定内存地址位中，在系统启动后将指定内存地址位移交给证书验证进程；证书验证进程通过连接云端认证服务器向服务器提交本机MAC地址和证书加密分区内容，由云端认证服务器进行解密，然后将对应的解密秘钥发还给证书验证进程，证书验证进程根据秘钥对数据解密，同时将解密结果中的设备MAC地址信息和本机设备进行验证，然后将解密数据以虚拟文件的形式映射到认证服务指定的目录中，之后进入正常认证业务流程，认证业务流程也会对解密的证书和设备MAC地址进行校验，通过307报文将用户3重定向到认证服务器，服务器提供的证书会在用户3的浏览器或是客户端中被验证出来，从而用户3可以看到自己的上网环境是否安全。

[0021] 证书安全分区内将要存储的BAS64加密信息和设备的MAC地址，预先生成，然后使用芯片烧写器对固定位地址内信息直接替换。

[0022] 工作原理：用户访问网络，需接入路由，而在接入路由的时候，用户可以通过证书来判断设备的安全性，而这种判断也可由终端应用来完成；服务器和客户端之间各内嵌了证书，而且这对证书是互相匹配的，终端可以对服务器进行验证，服务器也可以对终端进行验证，终端可以通过证书判断服务器是不是他人伪造的服务器，而服务器可以通过对终端进行验证而防止了恶意攻击、大量连接等问题，防止服务器伪装欺骗终端设备，并且防止终端设备伪装欺骗服务器；路由器通过307报文将用户重定向到认证服务器，服务器提供的证书会在用户的浏览器或是客户端中被验证出来，根据对第三方CA证书发行机构与证书有效期进行判定，通过结合现有浏览器内置证书自动检测机制，从而用户可以直接看到自己的上网环境是否安全；对用户到服务器之间的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密，使得破解的难度大大增加，从而保障了传输的安全，不仅从途径上阻止了监听，更是从内容上彻底阻止了监听；通过使用设备内嵌证书为用户提供基于SSL安全套接字握手的连接方式，从传输通道与内容层面做到每用户独立连接通道和数据传输加密，完全阻止了本地用户间数据监听。

[0023] 有益效果：本发明将路由器和云服务器内嵌入了相互匹配的证书，防止了恶意攻击、大量连接等问题，大大提高了整体的安全性；用户访问网络，需接入路由，而在接入路由的时候，用户可以通过证书来判断设备的安全性，而这种判断也可由客户端来完成，防止用户访问假路由器；用户可以在路由器或是交换机内验证证书的安全性，而不是仅仅的通过由服务器提供的portal页面，防止了热点利用服务器证书进行欺骗；通过307报文将用户重定向到认证服务器，服务器提供的证书会在用户的浏览器或是客户端中被验证出来，从而用户可以看到自己的上网环境是否安全；用户与服务器之间的传输信息通过使用基于RSA机制与SSL安全证书进行加密处理，页面和接口被证书加密，使用256位密钥进行加密，不仅从途径上阻止了监听，更是从内容上彻底阻止了监听；云服务器可以通过证书对路由器进行验证而防止了恶意攻击、大量连接等问题，因为证书阻挡了一部分的验证不能通过的设备，今儿大大地节约了设备的负载量；在数据通讯层面上提供了的基于该嵌入数字证书且兼容IEEE802.1X标准的“基于证书的通信加密”，可以大大加大的本地数据监听的难度，进一步在用户接入阶段对用户数据提供保护。

[0024] 利用本发明所述的技术方案，或本领域的技术人员在本发明技术方案的启发下，设计出类似的技术方案，而达到上述技术效果的，均是落入本发明的保护范围。

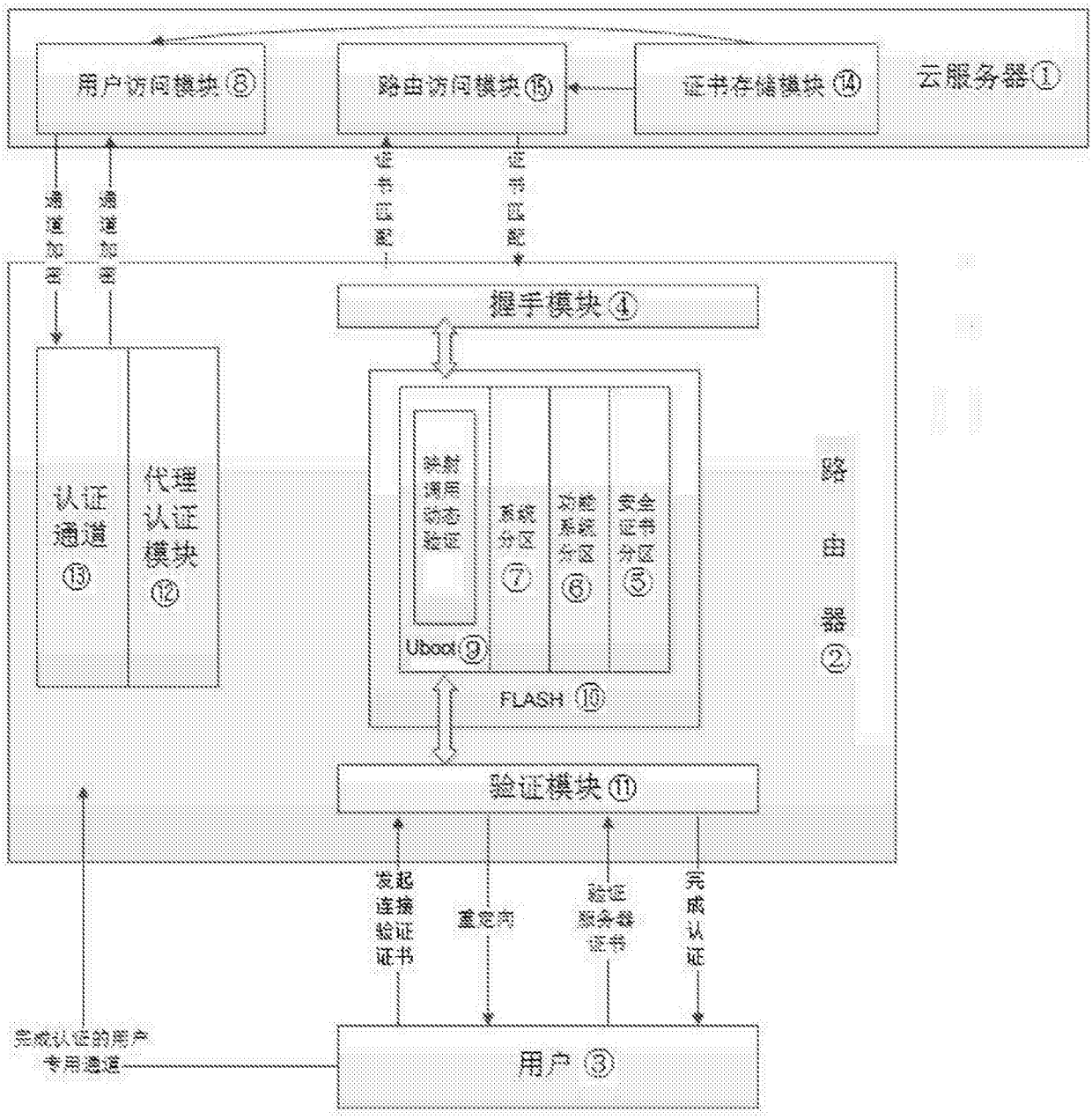

云服务器①
用户访问模块⑧
路由访问模块⑮
证书存储模块⑭
握手模块④
认证通道⑬
代理认证模块⑫
Uboot⑨
系统分区⑦
功能系统分区⑥
安全证书区⑤
FLASH⑩
验证模块⑪
路由器②
用户③
完成认证的用户专用通道

图1

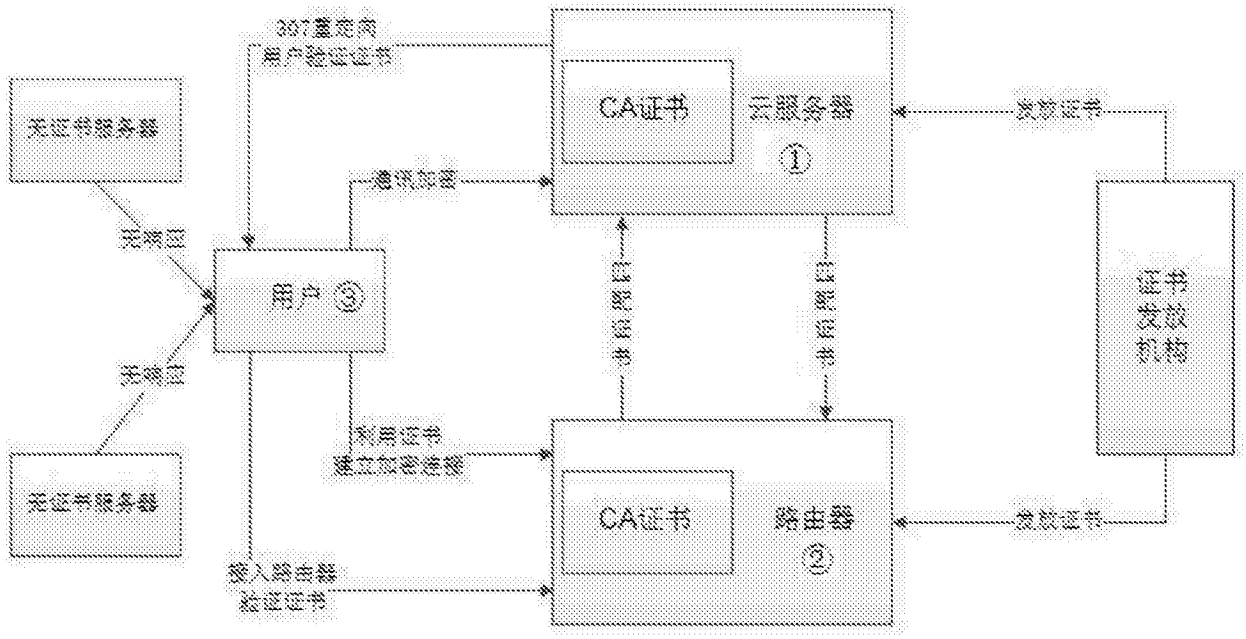

307重定向
用户验证证书
CA证书
云服务器
①
发放证书
无证书服务器
通讯加密
用户 ③
证书发放机构
无响应
无响应
利用证书
建立加密连接
CA证书
路由器
②
发放证书
接入路由器
验证证书

图2

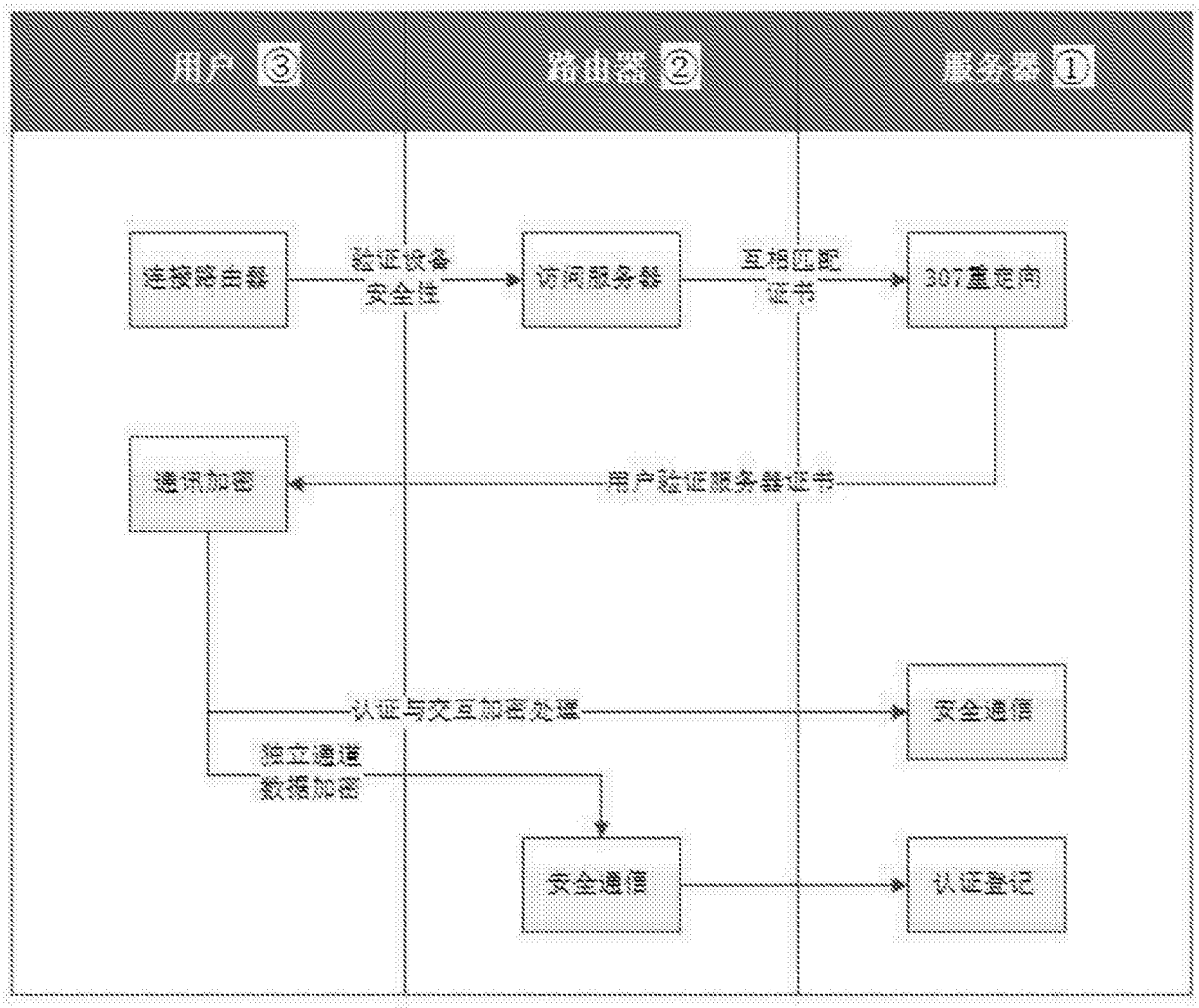

用户 3
路由器 2
服务器 1
连接路由器
验证设备安全性
访问服务器
互相匹配证书
307重定向
通讯加密
用户验证服务器证书
认证与交互加密处理
安全通信
建立通道数据加密
安全通信
认证登记

图3