

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 1 月 30 日 (30.01.2020)



(10) 国际公布号
WO 2020/019477 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2018/107636

(22) 国际申请日: 2018 年 9 月 26 日 (26.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810851516.5 2018 年 7 月 27 日 (27.07.2018) CN

(71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(72) 发明人: 张驰(ZHANG, Chi); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司(SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: COMMUNICATION DATA ENCRYPTION METHOD AND APPARATUS

(54) 发明名称: 通信数据加密方法和装置

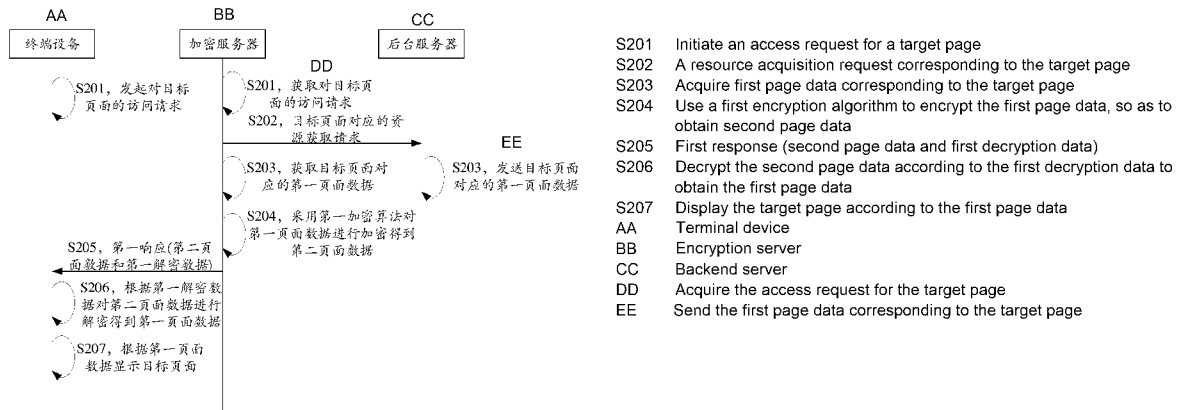


图 2

(57) Abstract: Disclosed in the present application are a communication data encryption method and apparatus. The method comprises: acquiring an access request for a target page, initiated by a terminal device; according to the access request, acquiring, from a backend server corresponding to the target page, first page data corresponding to the target page; using a first encryption algorithm to encrypt the first page data, so as to obtain second page data; sending, to the terminal device, a first response to the access request, so that the terminal device decrypts the second page data according to first decryption data to obtain the first page data, the first response comprising the second page data and the first decryption data, the first decryption data comprising decryption data corresponding to the first encryption algorithm. The present invention prevents, by encrypting page data returned by a backend server, a general scanning tool such as a scanner from directly acquiring the page data, improving the security of the backend server.

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请公开了通信数据加密方法和装置, 其中, 方法包括: 获取终端设备发起的对目标页面的访问请求; 根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据; 采用第一加密算法对所述第一页面数据进行加密得到第二页面数据; 向所述终端设备发送对所述访问请求的第一响应, 以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据, 所述第一响应包括所述第二页面数据以及所述第一解密数据, 所述第一解密数据为包含所述第一加密算法对应的解密数据。通过对后台服务器返回的页面数据进行加密, 避免扫描器等通用扫描工具直接获取到页面数据, 提高后台服务器的安全性。

通信数据加密方法和装置

本申请要求于 2018 年 07 月 27 日提交中国专利局、申请号为 2018108515165、申请名称为“通信数据加密方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及通信数据加密方法和装置。

背景技术

网站是依赖于 web 技术建立的应用，网站应用中的每一次信息交换都涉及 web 客户端和 web 服务端，其中，web 客户端的主要任务是向用户展现信息内容，其具体利用 html 语言、脚本程序、CSS、插件技术等实现对应的 web 页面展示；web 服务端为 web 客户端提供业务支持，其具体利用 PHP、ASP、JSP 等技术实现相应的功能。web 服务端和 web 客户端的交互流程一般为：web 客户端向 web 服务端发送请求，web 服务端基于 web 客户端发出的请求向 web 客户端返回该请求对应的数据（如 html 代码等）。

为了提高网站的安全性，一般会采用一定的加密技术对网站的某些数据进行加密，在目前的一些加密设计中，主要是通过通过对网站的 html 代码进行加密以避免网站的内容结构被轻易读取。但是，目前还有一些网站的各个功能之间的交互参数（如通过 post 表单提交的用户名、密码等）是以明文的形式进行传输，面临被监听的风险，网站的安全性不够高。

发明内容

本申请提供通信数据加密方法和装置，解决网站安全性不够高的问题。

第一方面，提供一种通信数据加密方法，包括：

获取终端设备发起的对目标页面的访问请求；

根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

第二方面，提供一种通信数据加密装置，包括：

访问请求获取模块，用于获取终端设备发起的对目标页面的访问请求；

页面数据获取模块，用于根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

加密模块，用于采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

请求响应模块，用于向所述终端设备发送对所述访问请求的第一响应，以使所述终端

设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据,所述第一响应包括所述第二页面数据以及所述第一解密数据,所述第一解密数据为包含所述第一加密算法的数据。

第三方面,提供另一种通信数据加密装置,包括处理器、存储器以及通信接口,所述处理器、存储器和通信接口相互连接,其中,所述通信接口用于接收或发送数据,所述存储器用于存储通信数据加密装置执行上述方法的应用程序代码,所述处理器被配置用于执行上述第一方面的方法。

第四方面,提供一种计算机存储介质,所述计算机存储介质存储有计算机程序,所述计算机程序包括程序指令,所述程序指令当被处理器执行时使所述处理器执行上述第一方面的方法。

本技术方案可以避免扫描器、爬虫工具等扫描页面的工具直接获取到页面数据,增加了网站的安全性。

附图说明

图1是本申请实施例提供的一种网站系统的架构示意图;

图2是本申请实施例提供的一种通信数据加密方法的流程示意图;

图3是本申请实施例提供的另一种通信数据加密方法的流程示意图;

图4是本申请实施例提供的一种通信数据加密装置的组成结构示意图;

图5是本申请实施例提供的另一种通信数据加密装置的组成结构示意图。

具体实施方式

下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,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,都属于本申请保护的范围。

本申请的技术方案适用于传统的以明文形式传输数据的网站系统,网站系统可包括网站客户端和网站服务端。网站客户端为面向用户的客户端,用于为用户提供服务。该网站客户端可以是通用型的客户端,通用型的客户端可以为多个网站服务器提供服务,例如可以为浏览器;该网站客户端也可以特定的客户端,该特定的客户端只用于为某个特定网站提供服务,例如为“腾讯视频”客户端。一般情况下,该网站客户端运行在用户的终端设备上,其中,终端设备包括但不限于手机、电脑、平板电脑、电子阅读器等具备网站浏览功能的电子设备。网站服务端用于管理并向网站客户端提供该网站系统的资源,网站服务端用于向网站客户端提供各种数据使得该网站客户端可以向用显示各种页面。该网站服务端可以由一台或多台服务器组成。本申请实施例通过在传统的以明文形式传输数据的网站系统中增加加密服务器,利用加密服务器对网站服务端与网站客户端之间交互的数据加密,以实现保障网站安全的目的。示例性地,本申请实施例的网站系统的架构可以如图1所示,网站系统包括运行在终端设备101上的网站客户端、加密服务器102以及网站服务器103,

其中,加密服务器 102 用于获取网站客户端与加密网站服务端之间的交互数据并进行加密。

本申请实施例的方法可以实现在图 1 所示的系统架构上,下面介绍本申请实施例的方法。

参见图 2,图 2 是本申请实施例提供的一种通信数据加密方法的流程示意图,如图所示,该方法包括:

S201,终端设备发起对目标页面的访问请求,加密服务器获取对目标页面的访问请求。

这里,终端设备通过运行在终端设备中的网站客户端发起对目标页面的访问请求,该目标页面为网站系统的其中一个页面。在该网站客户端为通用型的客户端的情况下,该目标页面可以为用户想要访问的任意一个网站系统的其中一个页面;在该网站客户端为特定的客户端的情况下,该目标页面为该网站客户端对应的网站系统的其中一个页面。

该目标页面对应一个统一资源定位符(uniform resource location, URL),该访问请求携带该 URL,该 URL 指向一个互联网协议(Internet protocol, IP)地址,该 IP 地址为该访问请求访问的地址。

本申请实施例中,该 URL 指向的 IP 地址可以有以下两种设计:

第一种设计,该 URL 指向的 IP 地址为加密服务器的 IP 地址。当终端设备发起对该目标页面的访问请求时,终端设备对该 URL 进行域名解析系统(domain name system, DNS)解析得到的 IP 地址为该加密服务器的 IP 地址。终端设备根据该加密服务器的 IP 地址向加密服务器发起对目标页面的访问请求,加密服务器通过接收的方式获取该对目标页面的访问请求。

第二种设计,该 URL 指向的 IP 地址为后台服务器的 IP 地址。当终端设备发起对该目标页面的访问请求时,终端设备对该 URL 进行 DNS 解析得到的 IP 地址为该后台服务器的 IP 地址。终端设备根据该后台服务器的 IP 地址向后台服务器发起对目标页面的访问请求,加密服务器通过流量劫持的方式截取该对目标页面的访问请求从而获取该对目标页面的访问请求。

S202,加密服务器向后台服务器发送目标页面对应的资源获取请求,后台服务器接收对目标页面的资源访问请求。

这里,后台服务器为该目标页面对应的后台服务器,也即包含该目标页面的网站系统的后台服务器。目标页面对应的资源获取请求用于请求该后台服务器返回该目标页面对应的第一页面数据,该第一页面数据被终端设备中的网站客户端运行时可以使得该网站客户端显示该目标页面。

本申请实施例中,加密服务器向后台服务器发送目标页面对应的资源获取请求有以下两种情况:

第一种情况,在对目标页面的访问请求中携带的 URL 指向的 IP 地址为上述第一种设计的情况下,可以在加密服务器中预置该后台服务器的 IP 地址,并将后台服务器的 IP 地址与目标访问请求关联,当加密服务器获取到目标访问请求时,根据与该目标访问请求关联的 IP 地址确定该目标访问请求对应的页面数据的资源在该后台服务器上,从而加密服务器可以根据与该目标访问请求对应的 IP 地址向该后台服务器发起目标页面对应的资

源获取请求,其中,目标访问请求是指与该后台服务器关联的访问请求,即该网站系统的相关请求。

例如,预先将“pingan.com”这一域名与后台服务器的IP地址相对应,后台服务器的IP地址为192.168.11.32,当加密服务器接收到访问请求中携带“pingan.com”这一域名的请求时,例如为www.pingan.com/login,由于这个请求中携带有“pingan.com”,则可以确定与这个请求对应的后台服务器的IP地址为192.168.11.32,则加密服务器向IP地址为192.168.11.32的后台服务器发起该访问请求对应的资源请求。

第二种情况,在目标页面的访问请求中携带的URL指向的IP地址为上述第二种设计的情况下,加密服务器在截取到该对目标页面的访问请求后,可以对该访问请求中的携带的URL进行DNS解析得到该后台服务器的IP地址,加密服务器可以根据解析得到的后台服务器的IP地址向后台服务器发起目标页面对应的资源获取请求。具体地,该目标页面对应的资源获取请求可以为该对目标页面的访问请求。

例如,加密服务器截取到的访问请求中携带的URL为www.pingan.com/login,加密服务器通过DNS方式解析该URL得到该URL对应的IP地址为202.132.11.32,则加密服务器向IP地址为202.132.11.32的服务器发起目标页面对应的资源请求。

S203,后台服务器发送目标页面对应的第一页面数据,加密服务器获取目标页面对应的第一页面数据。

这里,后台服务器根据该目标页面对应的资源获取请求从网站目录中找到该目标页面对应的网站文件,从该网站文件中获取第一页面数据,然后发送该第一页面数据。

本申请实施例中,在该访问请求中携带的URL为上述第一种设计的情况下,后台服务器向该加密服务器发送目标页面对应的第一页面数据,加密服务器通过接收的方式获取目标页面对应的第一页面数据;在该访问请求中携带的URL为上述第二种设计的情况下,后台服务器向该终端设备发送目标发送页面对应的第一页面数据,该加密服务器通过流量劫持的方式截取该对目标页面对应的第一页面数据。

可选地,如果该访问请求中携带的URL为上述第一种设计,在第一种可能的实现方式中,加密服务器与后台服务器可以基于HTTPS协议进行通信。其中,加密服务器可以基于HTTPS协议向后台服务器发送目标页面对应的资源获取请求,加密服务器可以基于HTTPS协议向加密服务器发送该目标页面对应的第一页面数据。在第二种可能的实现方式中,该加密服务器的访问方式可以为只允许加密服务器访问,即该后台服务器的访问白名单中有且只有该加密服务器的IP地址或MAC地址等证明该加密服务器的身份信息。以一种安全的方式保证加密服务器与后台服务器之间的交互过程的通信安全,进一步增强了网站系统的安全性。

S204,加密服务器采用第一加密算法对第一页面数据进行加密得到第二页面数据。

本申请实施例中,第一加密算法可以是对称算法,也可以是非对称算法,其中,第一加密算法包括但不限于数据加密标准(data encryption standard, DES)算法、3DES算法、RSA算法、高级加密标准(advanced encryption standard, AES)算法。

具体实现中,加密服务器从第一加密算法对应的密钥空间中选择其中一个密钥作为第一密钥,对该第一密钥和该第一页面数据进行该第一加密算法对应的运算,得到第二页

面数据。

S205, 加密服务器向终端设备发送第一响应, 终端设备接收第一响应, 第一响应包括第二页面数据和第一解密数据。

这里, 第一响应为对步骤 S201 的访问请求的响应。第一解密数据可以包括两部分数据, 第一部分数据为第二密钥, 第二部分数据为使该终端设备进行该第一加密算法对应的运算的数据。在该第一加密算法为对称算法的情况下, 该第二密钥与加密服务器对该第一页面数据进行加密时所使用的密钥相同, 即该第二密钥为加密服务器对该第一页面数据进行加密时所使用的密钥; 在该第一加密算法为非对称算法的情况下, 如果加密服务器对该第一页面数据进行加密时所使用的第一密钥为公钥, 则该第二密钥为该公钥对应的私钥, 如果该加密服务器对该第一页面数据进行加密时所使用的第一密钥为私钥, 则该第二密钥为该私钥对应的公钥。

在一种可能的方式中, 该使终端设备进行与该第一加密算法对应的运算的数据可以为该第一加密算法对应的解密脚本, 则该加密服务器向终端设备发送第一响应可以如下: 加密服务器确定第一加密算法对应的解密脚本; 加密服务器在第二页面数据中插入该第一加密算法对应的解密脚本, 并将插入第一加密算法对应的解密脚本后的第二页面数据携带在第一响应中发送给终端设备。

具体实现中, 可以在加密服务器预置至少一种加密算法 (指执行该加密算法的计算机程序), 并且在加密服务器中预置密钥空间、加密脚本以及解密脚本, 然后将密钥空间、加密脚本、解密脚本与加密算法对应。在发送第一响应时, 加密服务器可以选择与加密算法对应的解密脚本发送给终端设备, 以下进行具体说明:

第一种情况, 在加密服务器中预置一种加密算法。在这种情况下, 加密服务器中加密算法对应的加密脚本和解密脚本均只有一个, 加密服务器获取该唯一的解密脚本, 在第二页面数据中插入该唯一的解密脚本, 然后将插入解密脚本后的第二页面数据以及第二密钥发送给终端设备。

第二种情况, 加密服务器中预置有多种加密算法。在这种情况下, 加密服务器中加密算法有多种, 加密脚本和解密脚本有多个, 加密服务器可以根据加密算法与加密脚本以及解密脚本相互之间的对应关系选择与第一加密算法对应的解密脚本作为目标解密脚本, 然后在第二页面数据中插入该目标解密脚本, 然后将插入目标解密脚本后的第二页面数据以及第二密钥发送给终端设备。

S206, 终端设备根据第一解密数据对第二页面数据进行解密得到第一页面数据。

具体实现中, 终端设备从第一解密数据中分别获取第二密钥和使终端设备进行与该第一加密算法对应的运算的数据, 然后通过该使终端设备进行与第一加密算法的运算的数据对该第二密钥和该第二页面数据进行该第一加密算法对应的运算, 运算得到的数据为第一页面数据。

在使终端设备进行与该第一加密算法对应的运算的数据为第一加密算法对应的解密脚本的情况下, 终端设备运行该第一加密算法对应的解密脚本对该第二密钥和该第二页面数据进行该第一加密算法对应的运算得到第一页面数据。

S207, 终端设备根据第一页面数据显示目标页面。

本申请实施例中,加密服务器通过将终端设备向服务器发起的访问请求所对应的页面数据进行加密,并将加密方式所对应的解密数据连同加密后的页面数据一起发送给终端设备,使得终端设备可以采用该解密数据对加密后的页面数据进行解密从而能够显示该访问请求对应的目标页面,通过将页面数据加密的方式对后台服务器向终端设备返回的数据进行加密,避免了扫描器、爬虫工具等通用扫描工具能够直接获取到页面数据而获取到网站的信息,增加了后台服务器的安全性。

在上述图 2 对应的实施例中,加密服务器对后台服务器向终端设备返回的页面数据进行了加密,在一些可能的实现方式中,如果该目标页面为参数获取页面,在终端设备向后台服务器提交从目标页面获取到的参数信息的情况下,终端设备可以对终端设备向后台服务器提交的参数信息进行加密。加密服务器可以将用于加密该参数信息的加密数据携带在该目标页面对应的页面数据中发送给终端设备,即在该目标页面为参数页面获取页面的情况下,该第一响应还可以包括第一加密数据,该第一加密数据为包含第二加密算法的数据,该第一加密数据可以被终端设备用于加密数据。

第一加密数据可以包括两部分数据,第一部分数据为第三密钥,第二部分数据为使该终端设备进行与该第二加密算法对应的运算的数据。

第二加密算法可以为对称算法,也可以为非对称算法,在第二加密算法为对称算法的情况下,该第三密钥为对称密钥;在第二加密算法为非对称算法的情况下,该第二加密密钥为非对称密钥。第二加密算法包括但不限于 DES 算法、3DES 算法、RSA 算法、AES 算法。

第二加密算法与第三密钥可以有以下几种情况:

- 一、第二加密算法与第一加密算法相同,第三密钥与第一密钥相同。
- 二、第二加密算法与第一加密算法相同,第三密钥与第一密钥不同。
- 三、第二加密算法与第一加密算法不同,第三密钥与第一密钥相同。
- 四、第二加密算法与第一加密算法不同,第三密钥与第一密钥不同。

在上述四种情况中,除第一种情况外,其余三种情况均可以实现对终端设备与后台服务器之间交互的数据的动态加密。

在一种可能的实现方式中,该使终端设备进行与该第二加密算法对应的运算的数据可以为该第二加密算法对应的加密脚本,则该加密服务器向终端设备发送第一响应还可以包括:加密服务器确定第二加密算法对应的加密脚本;加密服务器在第二页面数据中插入该第二加密算法对应的解密脚本,然后将插入第一加密算法对应的解密脚本和第二加密算法对应的加密脚本后的第二页面数据携带在第一响应中发送给终端设备。

在第一加密算法与第二加密算法为相同的加密算法的情况下,该第二加密算法对应的加密脚本可以与该第一加密算法对应的解密脚本可以为同一个脚本。

在将第一加密数据携带在第一响应中发送给终端设备后,终端设备可以利用该第一加密数据对从该目标页面获取到的参数信息进行加密。参见图 3,图 3 是本申请实施例提供的另一种通信数据加密方法的流程示意图,该方法可以在上述步骤 S207 之后被执行,该方法包括:

S301,终端设备通过目标页面获取用户输入的第二参数。

本申请实施例中,目标页面为参数获取页面,参数获取页面是指用户可以输入数据并进行提交的页面,参数获取页面具体可以为登录页面、用户信息填写页面、用户意见提交页面,等等。第二参数为用户输入的信息,第二参数可以为用户通过登录页面输入的用户名、密码、验证码等,第二参数也可以为用户通过用户信息填写页面填写的姓名、性别、年龄等,第二参数还可以为用户提交的留言、建议等,不限于这里的描述。

S302,终端设备根据第一加密数据对第二参数进行加密得到第一参数。

具体实现中,终端设备可以从第一加密数据中分别获取第三密钥和使终端设备进行与该第二加密算法对应的运算的数据,然后通过该使终端设备进行与该第二加密算对应的运算的数据对该第三密钥和该第二参数进行该第二加密算法对应的运算,运算得到的数据为第一参数。

在使终端设备进行与该第二加密算法对应的运算的数据为第二加密算法对应的加密脚本的情况下,终端设备运行该第二加密算法对应的加密脚本对该第二密钥和该第二参数进行该第二加密算法对应的运算得到第一参数。

S303,终端设备发起参数提交请求,加密服务器获取参数提交请求,参数提交请求包括第一参数。

这里,参数提交请求中携带一个URL,该URL指向一个IP地址,该IP地址为该参数提交请求提交参数的地址。该URL指向的IP地址与访问请求中携带的URL指向的IP地址相同。终端设备发起参数提交请求以及加密服务器获取参数提交请求的具体实现方式可以参考前述终端设备发起访问请求以及加密服务器获取访问请求的描述,此处不再赘述。

S304,加密服务器对第一参数进行解密得到第二参数。

如前所述,第一加密数据由加密服务器发送给终端设备,当获取到该参数提交请求时,该参数提交请求中除了携带第一参数外,还携带终端设备的标识信息,加密服务器可以根据该参数提交请求确定终端设备的标识信息,然后根据终端设备的标识信息确定第一加密数据,根据第一加密数据确定第二加密算法,最后采用该第二加密算法对第一参数进行解密得到第二参数。其中,终端设备的标识信息可以为session信息或者cookie信息。

具体实现中,加密服务器在确定了第一加密数据后,在第三加密算法对应的密钥空间中确定与第一加密数据中的第三密钥对应的第四密钥,其中,在第三密钥为对称密钥的情况下,该第四密钥为该第三密钥,在第三密钥为非对称密钥的情况下,如果该第三密钥为公钥,则该第四密钥为该公钥对应的私钥,如果该第三密钥为私钥,则该第四密钥为该私钥对应的公钥;在确定第四密钥后,加密服务器对该第四密钥以及该第一参数进行该第二加密算法算法对应的运算得到第二参数。

S305,加密服务器将第二参数发送给后台服务器,后台服务器接收第二参数。

本申请实施例中,加密服务器将第二参数发送给后台服务器与加密服务器向后台服务器发送目标页面对应的资源获取请求类似,在一种可能的情况中,加密服务器可以根据该参数提交请求确定该参数提交请求对应的IP地址,根据该参数提交请求对应的IP地址向后台服务器发送该第二参数;在另一种可能的情况中,加密服务器对该参数提交请求中的URL进行解析得到该后台服务器的IP地址,然后根据该解析得到的IP地址向后台服务发送该第二参数。

S306, 后台服务器根据第二参数发送第三页面数据, 加密服务器获取第三页面数据。

这里, 后台服务器根据第二参数发送第三页面数据以及加密服务器获取第三页面数据的方式可参考前述步骤 S203 后台服务器发送目标页面对应的第一页面数据以及加密服务器获取目标页面对应的第一页面数据的描述, 此处不再赘述。

可选地, 在该参数提交请求携带的 URL 为上述第一种设计的情况下, 在在第一种可能的实现方式中, 加密服务器与后台服务器可以基于 HTTPS 协议进行通信。加密服务器基于 HTTPS 协议向后台服务器发送第二参数, 加密服务器基于 HTTPS 协议向加密服务器发送该第三页面数据。在第二种可能的实现方式中, 该加密服务器的访问方式可以为只允许加密服务器访问。通过安全手段保证加密服务器与后台服务器之间的交互过程的通信安全, 进一步增强了网站系统的安全性。

S307, 加密服务器采用第三加密算法对第三页面数据进行加密得到第四页面数据。

S308, 加密服务器向终端设备发送第二响应, 终端设备接收第二响应, 第二响应包括第四页面数据以及第二解密数据。

S309, 终端设备根据第二解密数据对第四页面数据解密得到第三页面数据。

S310, 终端设备显示第三页面数据对应的页面。

这里, 步骤 S307~S310 的具体实现方式与上述步骤 S204~S207 的具体实现方式类似, 可参考前述步骤 S204~S207 的描述, 此处不再赘述。

本申请实施例中, 加密服务器通过将加密数据携带在参数获取页面对应的页面数据中发送给终端设备, 使得终端设备可以采用该加密数据对通过参数获取页面获取到的参数进行加密, 从而避免这些参数在传输的过程中被获取到, 在不需要改变原有网站架构的情况下保证了参数的安全性和隐私性。。

上面介绍了本申请实施例的方法, 下面介绍本申请实施例的装置。

参见图 4, 图 4 是本申请实施例提供的一种通信数据加密装置的组成结构示意图, 该装置 40 可以为上述图 1 或图 2-图 3 所示的实施例中的加密服务器或加密服务器的一部分, 该装置 40 包括:

访问请求获取模块 401, 用于获取终端设备发起的对目标页面的访问请求;

页面数据获取模块 402, 用于根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据;

加密模块 403, 用于采用第一加密算法对所述第一页面数据进行加密得到第二页面数据;

请求响应模块 404, 用于向所述终端设备发送对所述访问请求的第一响应, 以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据, 所述第一响应包括所述第二页面数据以及所述第一解密数据, 所述第一解密数据为包含所述第一加密算法的数据。

在一种可能的设计中, 所述第一解密数据包括第一加密算法对应的解密脚本, 所述解密脚本被所述终端设备运行时使终端设备执行所述第一加密算法以进行解密;

该请求响应模块 404 具体用于:

确定所述第一加密算法对应的解密脚本;

在所述第二页面数据中插入所述第一加密算法对应的解密脚本,并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设备。

在一种可能的设计中,在所述目标页面为参数获取页面的情况下,所述第一响应还包括第一加密数据,所述第一加密数据为包含第二加密算法对应的数据。

在一种可能的设计中,该装置 40 还包括:

提交请求获取模块 405,用于获取所述终端设备发起的参数提交请求,所述参数提交请求包括第一参数,所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数,所述第二参数为所述终端设备通过所述目标页面获取到的参数;

解密模块 406,用于对所述第一参数进行解密得到所述第二参数;

发送模块 407,用于将所述第二参数发送给所述后台服务器。

在一种可能的设计中,所述解密模块 406 具体用于:

根据所述参数提交请求确定所述终端设备的标识信息;

根据所述终端设备的标识信息确定所述第一加密数据;

根据所述第一加密数据确定所述第二加密算法;

采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。

在一种可能的设计中,所述页面数据获取 402 还用于获取所述后台服务器根据所述第二参数返回的第三页面数据;

所述加密模块 403 还用于采用第三加密算法对所述第三页面数据进行加密得到第四页面数据;

所述请求响应模块 404 还用于向所述终端设备发送对所述参数提交请求的第二响应,以使所述终端设备根据第二解密数据对所述第四页面数据进行解密得到所述第三页面数据,所述第二响应包括所述第四页面数据和所述第二解密数据,所述第二解密数据为包含所述第三加密算法的数据。

在一种可能的设计中,所述发送模块 407 具体用于:基于安全套接字层的超文本传输 HTTPS 协议将所述第一参数发送给所述后台服务器;

所述页面数据获取模块 402 具体用于获取所述后台服务器基于所述 HTTPS 协议根据所述第二参数返回的第三页面数据。

需要说明的是,图 4 对应的实施例中未提及的内容可参见方法实施例的描述,这里不再赘述。

本申请实施例中,可以避免扫描器等通用扫描工具直接获取到页面数据而获取到网站的信息,增加了后台服务器的安全性。

参见图 5,图 5 是本申请实施例提供的另一种通信数据加密装置的组成结构示意图,该装置可以为上述图 1 或图 2-图 3 所示的实施例中的加密服务器或加密服务器的一部分,如图所示,该装置 50 包括处理器 501、存储器 502 以及通信接口 503。处理器 501 连接到存储器 502 和通信接口 503,例如处理器 501 可以通过总线连接到存储器 502 和通信接口 503。

处理器 501 被配置为支持所述通信数据加密装置执行图 2-图 3 所述的通信数据加密方法中加密服务器相应的功能。该处理器 501 可以是中央处理器(Central Processing Unit,

CPU), 网络处理器 (Network Processor, NP), 硬件芯片或者其任意组合。上述硬件芯片可以是专用集成电路 (Application-Specific Integrated Circuit, ASIC), 可编程逻辑器件 (Programmable Logic Device, PLD) 或其组合。上述 PLD 可以是复杂可编程逻辑器件 (Complex Programmable Logic Device, CPLD), 现场可编程逻辑门阵列 (Field-Programmable Gate Array, FPGA), 通用阵列逻辑 (Generic Array Logic, GAL) 或其任意组合。

存储器 502 存储器用于存储程序代码等。存储器 502 可以包括易失性存储器 (Volatile Memory, VM), 例如随机存取存储器 (Random Access Memory, RAM); 存储器 502 也可以包括非易失性存储器 (Non-Volatile Memory, NVM), 例如只读存储器 (Read-Only Memory, ROM), 快闪存储器 (flash memory), 硬盘 (Hard Disk Drive, HDD) 或固态硬盘 (Solid-State Drive, SSD); 存储器 502 还可以包括上述种类的存储器的组合。本申请实施例中, 存储器 502 用于存储通信数据加密的程序、各种加密脚本、解密脚本、密钥等。

所述通信接口 503 用于发送或接收数据。

处理器 501 可以调用所述程序代码以执行以下操作:

通过通信接口 503 获取终端设备发起的对目标页面的访问请求;

通过通信接口 503 根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据;

采用第一加密算法对所述第一页面数据进行加密得到第二页面数据;

通过通信接口 503 向所述终端设备发送对所述访问请求的第一响应, 以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据, 所述第一响应包括所述第二页面数据以及所述第一解密数据, 所述第一解密数据为包含所述第一加密算法的数据。

需要说明的是, 各个操作的实现还可以对应参照图 2-图 3 所示的方法实施例的相应描述; 所述处理器 501 还可以与通信接口 503 配合执行上述方法实施例中的其他操作。

本申请实施例还提供一种计算机可读存储介质, 所述计算机可读存储介质存储有计算机程序, 所述计算机程序包括程序指令, 所述程序指令当被计算机执行时使所述计算机执行如前述实施例所述的方法, 所述计算机可以为上述提到的通信数据加密装置的一部分。例如为上述的处理器 501。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程, 是可以通过计算机程序来指令相关的硬件来完成, 所述的程序可存储于一计算机可读取存储介质中, 该程序在执行时, 可包括如上述各方法的实施例的流程。其中, 所述的存储介质可为磁碟、光盘、只读存储记忆体 (Read-Only Memory, ROM) 或随机存储记忆体 (Random Access Memory, RAM) 等。

以上所揭露的仅为本申请较佳实施例而已, 当然不能以此来限定本申请之权利范围, 因此依本申请权利要求所作的等同变化, 仍属本申请所涵盖的范围。

权 利 要 求

1、一种通信数据加密方法，其特征在于，包括：

获取终端设备发起的对目标页面的访问请求；

根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

2、根据权利要求1所述的方法，其特征在于，所述第一解密数据包括第一加密算法对应的解密脚本，所述解密脚本被所述终端设备运行时使终端设备执行所述第一加密算法以进行解密；

所述向所述终端设备发送对所述访问请求的第一响应包括：

确定所述第一加密算法对应的解密脚本；

在所述第二页面数据中插入所述第一加密算法对应的解密脚本，并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设备。

3、根据权利要求1或2所述的方法，其特征在于，在所述目标页面为参数获取页面的情况下，所述第一响应还包括第一加密数据，所述第一加密数据为包含第二加密算法的数据。

4、根据权利要求3所述的方法，其特征在于，所述向所述终端设备发送对所述访问请求的第一响应之后，还包括：

获取所述终端设备发起的参数提交请求，所述参数提交请求包括第一参数，所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数，所述第二参数为所述终端设备通过所述目标页面获取到的参数；

对所述第一参数进行解密得到所述第二参数；

将所述第二参数发送给所述后台服务器。

5、根据权利要求4所述的方法，其特征在于，所述对所述第一参数进行解密得到所述第二参数包括：

根据所述参数提交请求确定所述终端设备的标识信息；

根据所述终端设备的标识信息确定所述第一加密数据；

根据所述第一加密数据确定所述第二加密算法；

采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。

6、根据权利要求4或5所述的方法，其特征在于，所述将所述第二参数发送给所述后台服务器之后还包括：

获取所述后台服务器根据所述第二参数返回的第三页面数据；

采用第三加密算法对所述第三页面数据进行加密得到第四页面数据；

向所述终端设备发送对所述参数提交请求的第二响应，以使所述终端设备根据第二解密数据对所述第四页面数据进行解密得到所述第三页面数据，所述第二响应包括所述第

四页面数据和所述第二解密数据,所述第二解密数据为包含所述第三加密算法的数据。

7、根据权利要求6所述的方法,其特征在于,所述将所述第二参数发送给所述后台服务器包括:

基于安全套接字层的超文本传输 HTTPS 协议将所述第二参数发送给所述后台服务器。

所述获取所述后台服务器根据所述第二参数返回的第三页面数据包括:

获取所述后台服务器根据所述第二参数基于所述 HTTPS 协议返回的第三页面数据。

8、一种通信数据加密装置,其特征在于,所述装置包括:

访问请求获取模块,用于获取终端设备发起的对目标页面的访问请求;

页面数据获取模块,用于根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据;

加密模块,用于采用第一加密算法对所述第一页面数据进行加密得到第二页面数据;

请求响应模块,用于向所述终端设备发送对所述访问请求的第一响应,以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据,所述第一响应包括所述第二页面数据以及所述第一解密数据,所述第一解密数据为包含所述第一加密算法的数据。

9、根据权利要求8所述的装置,其特征在于,所述第一解密数据包括第一加密算法对应的解密脚本,所述解密脚本被所述终端设备运行时使终端设备执行所述第一加密算法以进行解密;

请求响应模块具体用于:

确定所述第一加密算法对应的解密脚本;

在所述第二页面数据中插入所述第一加密算法对应的解密脚本,并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设备。

10、根据权利要求8或9所述的装置,其特征在于,在所述目标页面为参数获取页面的情况下,所述第一响应还包括第一加密数据,所述第一加密数据为包含第二加密算法对应的数据。

11、根据权利要求10所述的装置,其特征在于,所述装置还包括:

提交请求获取模块,用于获取所述终端设备发起的参数提交请求,所述参数提交请求包括第一参数,所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数,所述第二参数为所述终端设备通过所述目标页面获取到的参数;

解密模块,用于对所述第一参数进行解密得到所述第二参数;

发送模块,用于将所述第二参数发送给所述后台服务器。

12、根据权利要求11所述的装置,其特征在于,所述解密模块具体用于:

根据所述参数提交请求确定所述终端设备的标识信息;

根据所述终端设备的标识信息确定所述第一加密数据;

根据所述第一加密数据确定所述第二加密算法;

采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。

13、根据权利要求11或12所述的装置,其特征在于,所述页面数据获取还用于获

取所述后台服务器根据所述第二参数返回的第三页面数据；

所述加密模块还用于采用第三加密算法对所述第三页面数据进行加密得到第四页面数据；

所述请求响应模块还用于向所述终端设备发送对所述参数提交请求的第二响应，以使所述终端设备根据第二解密数据对所述第四页面数据进行解密得到所述第三页面数据，所述第二响应包括所述第四页面数据和所述第二解密数据，所述第二解密数据为包含所述第三加密算法的数据。

14、根据权利要求 13 所述的装置，其特征在于，所述发送模块具体用于：基于安全套接字层的超文本传输 HTTPS 协议将所述第一参数发送给所述后台服务器；

所述页面数据获取模块具体用于获取所述后台服务器基于所述 HTTPS 协议根据所述第二参数返回的第三页面数据。

15、一种通信数据加密装置，包括处理器、存储器以及通信接口，所述处理器、存储器和通信接口相互连接，其中，所述通信接口用于传输数据，所述存储器用于存储程序代码，所述处理器用于调用所述程序代码，执行以下操作：

获取终端设备发起的对目标页面的访问请求；

根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

16、根据权利要求 15 所述的装置，其特征在于，所述处理器执行所述第一解密数据包括第一加密算法对应的解密脚本，所述解密脚本被所述终端设备运行时使终端设备执行所述第一加密算法以进行解密；

所述处理器执行所述向所述终端设备发送对所述访问请求的第一响应的操作，包括：确定所述第一加密算法对应的解密脚本；

在所述第二页面数据中插入所述第一加密算法对应的解密脚本，并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设备。

17、根据权利要求 15 或 16 所述的装置，其特征在于，所述处理器还用于执行以下操作：所述第一响应还包括第一加密数据，所述第一加密数据为包含第二加密算法的数据。

18、根据权利要求 17 所述的装置，其特征在于，所述处理器还用于执行以下操作：

获取所述终端设备发起的参数提交请求，所述参数提交请求包括第一参数，所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数，所述第二参数为所述终端设备通过所述目标页面获取到的参数；

对所述第一参数进行解密得到所述第二参数；

将所述第二参数发送给所述后台服务器。

19、根据权利要求 18 所述的装置，其特征在于，所述处理器执行所述对所述第一参数进行解密得到所述第二参数的操作，包括：

根据所述参数提交请求确定所述终端设备的标识信息；

根据所述终端设备的标识信息确定所述第一加密数据；

根据所述第一加密数据确定所述第二加密算法；

采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。

20、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如权利要求 1-7 任一项所述的方法。

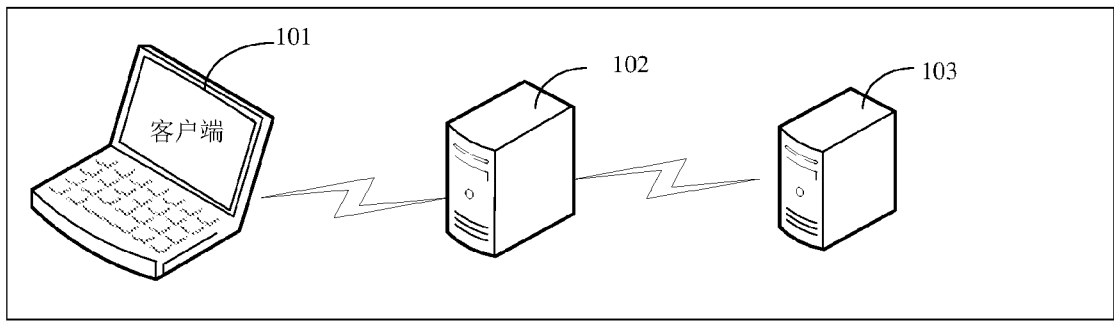


图 1

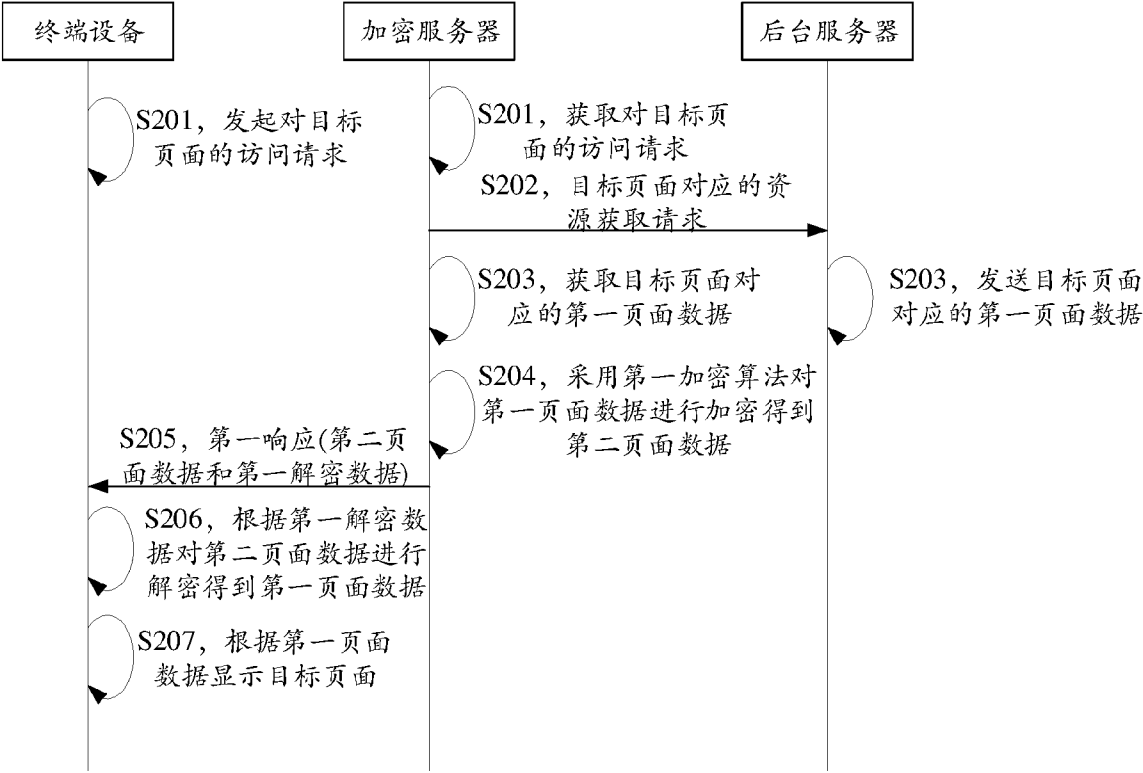


图 2

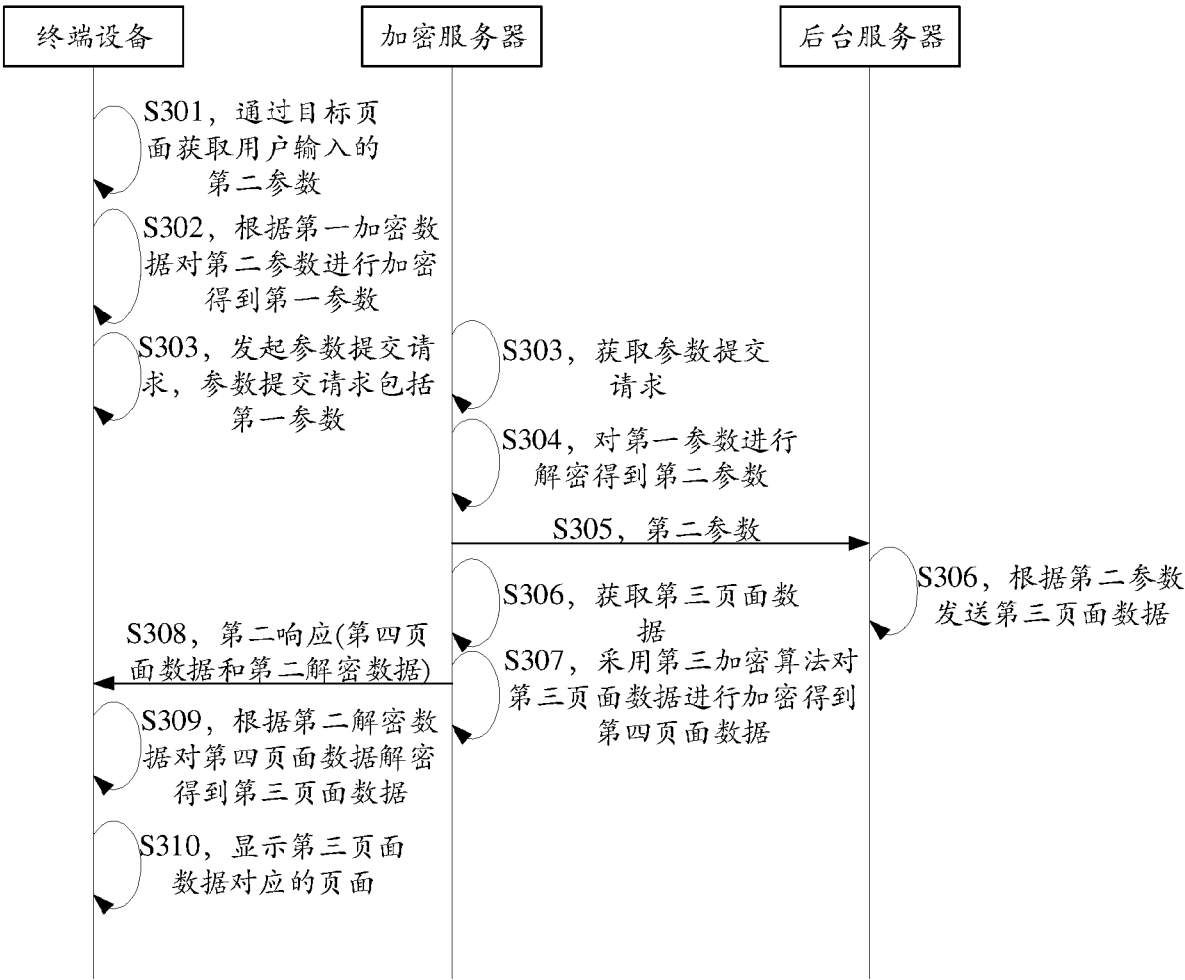


图 3

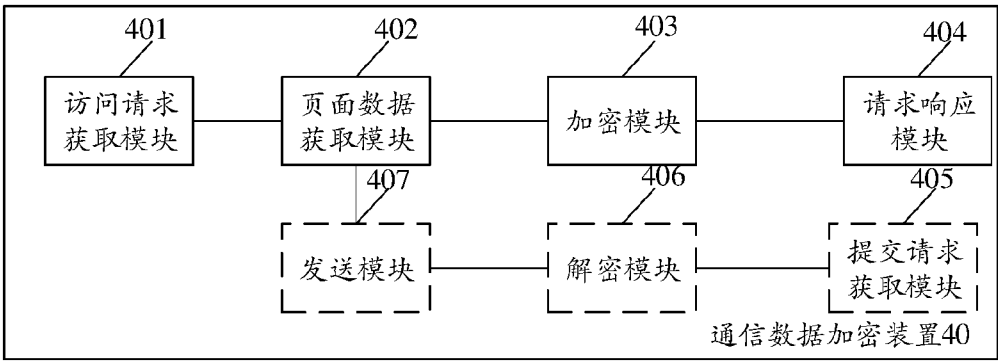


图 4

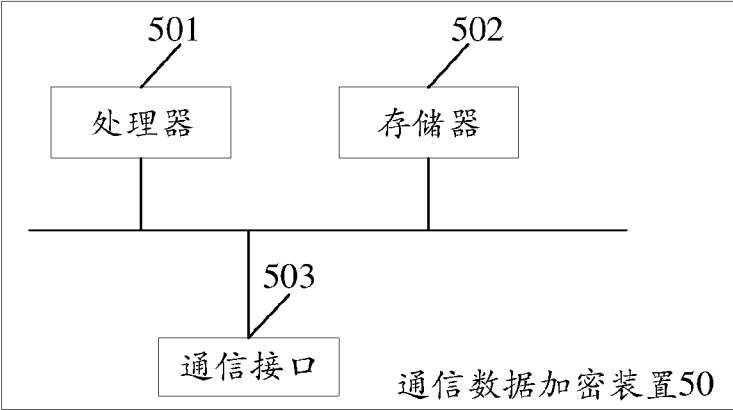


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/107636

A. CLASSIFICATION OF SUBJECT MATTER H04L 9/06(2006.01)i According to International Patent Classification (IPC) or to both national classification and IPC																				
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) CNPAT; CNKI; WPI; EPODOC; IEEE: 网页, 页面, 加密, 解密, 访问, 请求, 响应, 数据, 脚本, page, encrypt+, decrypt+, access +, request, response, data, script																				
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 107733633 A (CHENGDU KNOWNSEC INFORMATION TECHNOLOGY CO., LTD.) 23 February 2018 (2018-02-23) the abstract, and description, paragraphs [0022]-[0043]</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 106412024 A (NETEASE KOALA (HANGZHOU) TECHNOLOGY CO., LTD.) 15 February 2017 (2017-02-15) entire document</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 107330336 A (THE PLA INFORMATION ENGINEERING UNIVERSITY) 07 November 2017 (2017-11-07) entire document</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 107463840 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 12 December 2017 (2017-12-12) entire document</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 105187389 A (BEIJING SI-TECH INFORMATION TECHNOLOGY LTD.) 23 December 2015 (2015-12-23) entire document</td> <td>1-20</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	CN 107733633 A (CHENGDU KNOWNSEC INFORMATION TECHNOLOGY CO., LTD.) 23 February 2018 (2018-02-23) the abstract, and description, paragraphs [0022]-[0043]	1-20	A	CN 106412024 A (NETEASE KOALA (HANGZHOU) TECHNOLOGY CO., LTD.) 15 February 2017 (2017-02-15) entire document	1-20	A	CN 107330336 A (THE PLA INFORMATION ENGINEERING UNIVERSITY) 07 November 2017 (2017-11-07) entire document	1-20	A	CN 107463840 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 12 December 2017 (2017-12-12) entire document	1-20	A	CN 105187389 A (BEIJING SI-TECH INFORMATION TECHNOLOGY LTD.) 23 December 2015 (2015-12-23) entire document	1-20
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																		
X	CN 107733633 A (CHENGDU KNOWNSEC INFORMATION TECHNOLOGY CO., LTD.) 23 February 2018 (2018-02-23) the abstract, and description, paragraphs [0022]-[0043]	1-20																		
A	CN 106412024 A (NETEASE KOALA (HANGZHOU) TECHNOLOGY CO., LTD.) 15 February 2017 (2017-02-15) entire document	1-20																		
A	CN 107330336 A (THE PLA INFORMATION ENGINEERING UNIVERSITY) 07 November 2017 (2017-11-07) entire document	1-20																		
A	CN 107463840 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 12 December 2017 (2017-12-12) entire document	1-20																		
A	CN 105187389 A (BEIJING SI-TECH INFORMATION TECHNOLOGY LTD.) 23 December 2015 (2015-12-23) entire document	1-20																		
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.																				
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “E” earlier application or patent but published on or after the international filing date “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) “O” document referring to an oral disclosure, use, exhibition or other means “P” document published prior to the international filing date but later than the priority date claimed “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art “&” document member of the same patent family																				
Date of the actual completion of the international search 18 February 2019		Date of mailing of the international search report 27 February 2019																		
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/ CN) No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088 China Facsimile No. (86-10)62019451		Authorized officer Telephone No.																		

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/107636

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	107733633	A	23 February 2018	None	
CN	106412024	A	15 February 2017	None	
CN	107330336	A	07 November 2017	None	
CN	107463840	A	12 December 2017	None	
CN	105187389	A	23 December 2015	None	

国际检索报告

国际申请号

PCT/CN2018/107636

A. 主题的分类

H04L 9/06 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT;CNKI;WPI;EPDOC;IEEE:网页, 页面, 加密, 解密, 访问, 请求, 响应, 数据, 脚本, page, encrypt+, decrypt+, access+, request, response, data, script

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 107733633 A (成都创宇信息技术有限公司) 2018年 2月 23日 (2018 - 02 - 23) 摘要、说明书第22-43段	1-20
A	CN 106412024 A (网易无尾熊杭州科技有限公司) 2017年 2月 15日 (2017 - 02 - 15) 全文	1-20
A	CN 107330336 A (中国人民解放军信息工程大学) 2017年 11月 7日 (2017 - 11 - 07) 全文	1-20
A	CN 107463840 A (腾讯科技深圳有限公司) 2017年 12月 12日 (2017 - 12 - 12) 全文	1-20
A	CN 105187389 A (北京思特奇信息技术股份有限公司) 2015年 12月 23日 (2015 - 12 - 23) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2019年 2月 18日

国际检索报告邮寄日期

2019年 2月 27日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

颜悦

电话号码 86-(10)-53961643

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/107636

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	107733633	A	2018年 2月 23日	无	
CN	106412024	A	2017年 2月 15日	无	
CN	107330336	A	2017年 11月 7日	无	
CN	107463840	A	2017年 12月 12日	无	
CN	105187389	A	2015年 12月 23日	无	