(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
2018 年 4 月 5 日 (05.04.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/059578 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2017/104806

(22) 国际申请日: 2017 年 9 月 30 日 (30.09.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610873442.6 2016年9月30日 (30.09.2016) CN

(71) 申请人: 贵州白山云科技有限公司 (GUIZHOU BAISHANCLOUD TECHNOLOGY CO., LTD.) [CN/CN]; 中国北京市朝阳区酒仙桥北路甲10号电子城IT产业园201号楼E座5层, Beijing 100015 (CN)。

(72) 发明人: 苗辉 (MIAO, Hui); 中国北京市朝阳区酒仙桥北路甲10号电子城IT产业园201号楼E座5层, Beijing 100015 (CN)。 江桂林 (JIANG, Guilin); 中国北京市朝阳区酒仙桥北路甲10号电子城IT产业园201号楼E座5层, Beijing 100015 (CN)。 杨洋 (YANG, Yang); 中国北京市朝阳区酒仙桥北路甲10号电子城IT产业园201号楼E座5层, Beijing 100015 (CN)。 林胜恩 (LIN, Shengen); 中国北京市朝阳区酒仙桥北路甲10号电子城IT产业园201号楼E座5层, Beijing 100015 (CN)。

(74) 代理人: 北京名华博信知识产权代理有限公司 (BOXIN CHINA INTELLECTUAL PROPERTY); 中国北京市海淀区清河强佑新城翠微A座936, Beijing 100085 (CN)。

(54) **Title:** HTTPS ACCELERATION METHOD AND SYSTEM BASED ON CONTENT DISTRIBUTION NETWORK

(54) **发明名称:** 一种基于内容分发网络的HTTPS加速方法和系统

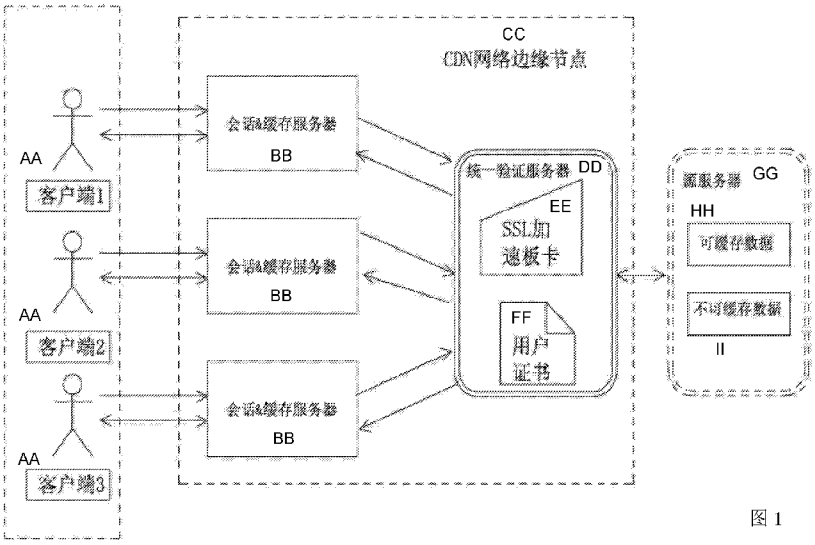

图 1

AA	Client end 1, Client end 2, Client end 3	FF	User certificate
BB	Session and buffer server	GG	Source server
CC	CDN network border node	HH	Bufferable data
DD	Centralized authentication server	II	Non-bufferable data
EE	SSL acceleration board card		

(57) **Abstract:** Embodiments of the present invention disclose an HTTPS acceleration method and system based on a content distribution network. The method comprises: step 1), a client end initiating an HTTPS access request to a CDN network border node, and the CND network border node allocating in balance a session and buffer server via a front-end load to perform three handshakes with the client end; step 2), during the handshaking process, the allocated session and buffer server performing HTTPS session management, and simultaneously performing interaction, by means of a private key and encryption/decryption of a user certificate, with a centralized

WO 2018/059578 A1

[见续页]

(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, 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))。

authentication server, and returning a result of the interaction to the client end; and step 3), after completing the handshaking process, the session and buffer server launching a buffer service to provide the client end with a CDN service, wherein, if data requested by the client end is bufferable, the data is acquired directly from the session and buffer server, and if the data requested by the client end is non-bufferable, the data is acquired from a source server.

(57) 摘要：本发明实施例公开一种基于内容分发网络的HTTPS加速方法和系统。此方法包括：步骤1：客户端向CDN网络边缘节点发起HTTPS访问请求；CDN网络边缘节点通过前端的负载均衡分配一台会话&缓存服务器与客户端进行三次握手；步骤2：握手过程中，分配好的会话&缓存服务器负责HTTPS会话管理，该会话&缓存服务器同时就私钥和用户证书的加解密工作与统一验证服务器进行交互，将交互结果返回客户端；步骤3：完成握手过程后，所述会话&缓存服务器开展缓存服务为客户端提供CDN服务；对于客户端所请求的数据，如果是为可缓存数据，直接在会话&缓存服务器获取，如果是不可缓存数据，向源服务器获取。

一种基于内容分发网络的HTTPS加速方法和系统

本申请要求在2016年9月30日提交中国专利局、申请号为201610873442.6、发明名称为“一种基于内容分发网络的HTTPS加速方法和系统”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

本发明实施例涉及一种网站优化方法，具体涉及一种基于内容分发网络（ContentDeliveryNetwork，CDN）的HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer）加速方法和系统。

背景技术

HTTPS安全协议是以安全为目标的HTTP通道，通过在HTTP下加入SSL层，能够实现传输加密，避免用户数据、交易数据等重要数据被窃取。HTTPS在保护用户隐私和防止流量劫持方面发挥着非常关键的作用。但与此同时，HTTPS也会降低用户访问速度，增加网站服务器的计算资源消耗。

在SSL会话中，计算量最大的部分是安全套接层（Secure Sockets Layer，SSL）握手阶段，SSL有两种主要的握手类型，一种是基于RSA，一种是基于Deiffie-Hellman（DH）。RSA和DH的公钥算法使用了很多CPU的处理能力且是握手中最慢的部分。一个笔记本电脑上可以每秒进行几百次RSA加密，对比每秒大约一千万次对称加密AES。这个阶段的主要工作是协商会话密钥，该密钥通常是对称密钥，将被贯穿应用于相应的会话过程中；与此同时，SSL握手本身的加密和签名则是包含在证书中的非对称密钥，使用这种非对称密钥比对称密钥对计算资源的消耗更大。

基于软件的SSL实现，服务器的处理器负责各个会话初始的密钥交换以及后续的数据加解密，这种密集的计算过程会使服务器承受极大的压力，使得其他事务处理能力大大降低。因此基于软件的SSL实现，只适用于管理少量SSL流量的场景；而CDN网络的特点，是节点规模小，每个节点的服务器数量较少，然而CDN节点分布较多，呈地理性发散分布。在CDN网络中做HTTPS加速，基于软件的SSL实现明显不能满足加速需求。

基于上述现状，CDN厂商提出了基于硬件的SSL加速方案，如SSL加速板卡

或SSL加速设备。

SSL加速板卡能够有效分担服务器CPU处理SSL事务的压力，一个或多个协处理器用于实现SSL计算，这些协处理器可能采用通用CPU，也可能采用定制的ASIC芯片和RISC指令集芯片。但是，对每个客户访问，都要分配一个插接有SSL加速板卡的服务器完成握手、加解密过程，浪费资源的同时，单机管理成本也高。另外，每台服务器上必须具备唯一性数字证书，这么多证书容易泄露，存在安全问题。

其次，SSL加速设备是嵌入SSL加速板卡的独立设备，对加密流量进行解密，并将解过密的数据信息发送给后台服务器；在相反方向上，负责加密由后台服务器发来的明文数据再将其转发给客户端；SSL加速设备终结了SSL会话，后台服务器可以完全被释放出来用于数据服务或者运行应用程序，但是SSL加速设备整体成本偏高，并不是一个理想的替代方案。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本发明实施例提出一种基于内容分发网络的 HTTPS 加速方法和系统，采用 SSL 加速板卡方案，解决了基于软件的 SSL 实现的性能承受压力大、事务处理能力低效的问题；并将 SSL 加速板卡部署在 CDN 网络边缘节点的服务器上，对证书实现集中式管理，且一张 SSL 加速板卡能够服务多个客户进行加解密工作，解决了每个加速板卡只绑定特定客户端请求的资源浪费、管理成本高的问题。

本发明实施例提供的基于内容分发网络的 HTTPS 加速方法，包括：该内容分发网络包括位于中心部分的内容分发网络 CDN 网管中心和域名系统 DNS 重定向解析中心、位于边缘部分的多个 CDN 网络边缘节点以及位于后端的源服务器；各 CDN 网络边缘节点分别部署了位于前端的会话&缓存服务器和位于后端的统一验证服务器；

该 HTTPS 加速方法包括:

步骤 1：客户端向 CDN 网络边缘节点发起 HTTPS 访问请求；CDN 网络边缘节点通过前端的负载均衡分配一台会话&缓存服务器与客户端进行三次握手；

步骤 2：握手过程中，分配好的会话&缓存服务器负责 HTTPS 会话管理，

该会话&缓存服务器同时就私钥和用户证书的加解密工作与统一验证服务器进行交互，将交互结果返回客户端；

步骤 3：完成握手过程后，所述会话&缓存服务器开展缓存服务为客户端提供 CDN 服务；对于客户端所请求的数据，如果是为可缓存数据，直接在会话&缓存服务器获取，如果是不可缓存数据，向源服务器获取。

上述方法还可包括：所述统一验证服务器上设有用户证书和私钥，集成至少一个 SSL 加速板卡，一台或者多台统一验证服务器对应一用户证书，该统一验证服务器被设置为处理加解密。

上述方法还可包括：如果有多个客户端，则通过该会话&缓存服务器将各客户端映射到一台统一验证服务器上。

上述方法还可包括：将统一验证服务器的比例数量随流量线性进行部署，将统一验证服务器线性扩展，每台统一验证服务器上插接至少一个 SSL 加速板卡。

上述方法还可包括：每台统一验证服务器上插接多个 SSL 加速板卡，不同 SSL 加速板卡构成主备关系。

本发明实施例还同时提供一种基于内容分发网络的 HTTPS 加速系统，该内容分发网络包括位于中心部分的 CDN 网管中心和 DNS 重定向解析中心、位于边缘部分的多个 CDN 网络边缘节点以及位于后端的源服务器；各 CDN 网络边缘节点分别部署了位于前端的会话&缓存服务器和位于后端的统一验证服务器；

该 HTTPS 加速系统包括如下单元：

HTTPS 访问请求发起单元，设置为执行：客户端向 CDN 网络边缘节点发起 HTTPS 访问请求；

三次握手发起单元，设置为执行：CDN 网络边缘节点通过前端的负载均衡，分配一台对应的会话&缓存服务器，与客户端进行三次握手；三次握手处理单元，设置为执行：握手过程中，分配好的会话&缓存服务器负责 HTTPS 会话管理，该会话&缓存服务器同时就私钥和用户证书的加解密工作与统一验证服务器进行交互，将交互结果返回客户端；

HTTPS 访问应答单元，设置为执行：完成握手过程后，所述会话&缓存服务器开展缓存服务为客户端提供 CDN 服务；对于客户端所请求的数据，如果是

可缓存数据，直接在会话&缓存服务器获取，如果是不可缓存数据，则向源服务器获取。

上述系统还可包括：所述统一验证服务器上设有用户证书和私钥，集成至少一个 SSL 加速板卡，一台或者多台统一验证服务器对应一用户证书，该统一验证服务器被设置为处理加解密。

上述系统还可包括：所述三次握手处理单元还设置为执行如下操作：如果有多个客户端，则通过该会话&缓存服务器将各客户端映射到一台统一验证服务器上。

上述系统还可包括：所述统一验证服务器的比例数量随流量线性进行部署，将统一验证服务器线性扩展，每台统一验证服务器上插接有至少一个 SSL 加速板卡。

上述系统还可包括：每台统一验证服务器上插接多个 SSL 加速板卡，不同 SSL 加速板卡构成主备关系。

本发明实施例有效地结合SSL加速板卡和CDN网络边缘节点各自的技术优势，具有以下优点：

（1）使用 SSL 加速板卡代替普通边缘服务器的加解密工作，使边缘服务器减轻负载，将 SSL 加速板卡部署到统一验证服务器上，大大降低了普通边缘服务器的 CPU 消耗，提高了效率。

（2）使用一张 SSL 加速卡来服务若干客户的加解密工作，从原来的一对一的服务到 1 对 N，这样对 CDN 厂商而言，大大节省了成本。

（3）从原来的一张 SSL 加速卡需要管理一个证书，到现在的 N 个客户使用一张 SSL 加速板卡，证书集中式管理，这样证书的管理量大大减少，单机管理成本大大降低。

（4）统一验证服务器除了通过插 SSL 加速板卡做加解密工作，还可以根据客户的不同需求情况，在统一验证服务器上部署软件，如 CDN 服务器申请证书方案、Cloudflare 的 keyless-SSL 方案等，本发明实施例都能有效支持；在实现与前端服务器同在边缘节点的交互，减少了服务器间往返 RTT，提高了效率。

（5）SSL 加速板卡可以在边缘统一验证服务器集群中线性扩展，以增加其事务处理能力，不影响集中管理，也节省了扩容成本。

附图说明

此处所说明的附图用来提供对本发明实施例的进一步理解，构成本申请的一部分，本发明实施例的示意性实施例及其说明用于解释本发明实施例，并不构成对本发明实施例的不当限定。在附图中：

图 1 为本发明实施例的客户端访问示意图。

具体实施方式

现结合附图和具体实施方式对本发明实施例进一步说明。

本发明实施例提供一种基于内容分发网络的 HTTPS 加速方法，该内容分发网络包括位于中心部分的 CDN 网管中心和 DNS 重定向解析中心、位于边缘部分的多个 CDN 网络边缘节点以及位于后端的源服务器。

中心部分的 CDN 网管中心和 DNS 重定向解析中心负责全局负载均衡，设备系统安装在管理中心机房。

CDN 网络边缘节点为 CDN 分发的载体，主要由缓存（Cache）和负载均衡器等组成，各 CDN 网络边缘节点分别部署了位于前端的会话&缓存和位于后端的统一验证服务器（UAS）。其中，会话&缓存服务器设有多个，负责 HTTPS 会话管理，并与后端统一验证服务器交互；完成交互后，则转变角色为缓存服务器，为客户提供 CDN 服务。在一个可选的例子中，该会话&缓存服务器使用配置的 OpenSSL 和 Nginx 软件完成上述功能。统一验证服务器设有多个，其含用户证书、私钥，集成了若干 SSL 加速板卡（如 Intel 或者 NAVIMN），是用户加解密的主要处理服务器。对 SSL 加速板卡，其单卡吞吐量通常可以达到 20Gbps，对 1024 位 RSA 和 2048 位 RSA 加解密，其处理速率分别为 35K-200Kqps 和 6K-35Kqps。统一验证服务器可以是在 Linux 上运行（RedHat/CentOS、Debian 和 Ubuntu，和其他的），其他的 Unix 操作系统（包含 FreeBSD）和微软 Windows 服务器。各统一验证服务器上的用户证书可共享，也就是说多个统一验证服务器可以使用同一个证书，也可以是各统一验证服务器对应一个用户证书。统一验证服务器是无状态的、允许客户端使用现成的硬件，并随着流量线性部署统一验证服务器的比例；通过运行多个统一验证服务器和通过 DNS 的负载均衡，

客户的站点可以被保持高可用的。

源服务器包含可缓存数据和不可缓存数据，可缓存数据用于与会话&缓存服务器更新缓存，不可缓存数据在客户端与边缘节点建立会话后回源使用。

基于内容分发网络，结合图 1 的示意图，本发明实施例的 HTTPS 加速方法包括如下步骤:

步骤 1: 客户端发起 HTTPS 访问，通过前端的负载均衡，分配一台对应的会话&缓存服务器，发起三次握手(RSA/DH)过程；其中，客户端为网络终端用户，可能采用当下流行的浏览器（Chrome、Firefox、IE 等）浏览网页，图中的客户端 1、客户端 2、客户端 3，分别指不同网站加速客户的客户端代表访问，如分别指新浪网、腾讯网、网易等不同网站加速客户；

步骤 2: 握手过程中，该会话&缓存服务器就私钥和用户证书的加解密工作与统一验证服务器交互（视不同方案实现而定），将交互结果返回客户端；对于多个客户端，通过会话&缓存服务器将各客户端映射到一台统一验证服务器上，使每个客户端分享统一验证服务器的硬件加速能力；

步骤 3: 完成握手过程后，会话&缓存服务器开展缓存服务为客户端提供 CDN 服务，客户端则正常使用 CDN 服务，对于客户端所请求的数据，如果是可缓存数据，直接在边缘节点的服务器获取，如果是不可缓存数据，向源服务器获取。

步骤 4: 统一验证服务器的数量可以随流量线性来部署统一验证服务器的比例，需要扩展时，可将统一验证服务器进行线性扩展，每台服务器上插上至少一个 SSL 加速板卡，以应对更大规模的 SSL 事务处理需求；或者形成主备，以应对故障处理。

本发明实施例还同时提供一种基于内容分发网络的 HTTPS 加速系统，该内容分发网络包括位于中心部分的 CDN 网管中心和 DNS 重定向解析中心、位于边缘部分的多个 CDN 网络边缘节点以及位于后端的源服务器；各 CDN 网络边缘节点分别部署了位于前端的会话&缓存服务器和位于后端的统一验证服务器；该 HTTPS 加速系统包括如下单元:

HTTPS 访问请求发起单元，设置为执行: 客户端向 CDN 网络边缘节点发起 HTTPS 访问请求;

三次握手发起单元，设置为执行：CDN 网络边缘节点通过前端的负载均衡，分配一台对应的会话&缓存服务器，与客户端进行三次握手；

三次握手处理单元，设置为执行：握手过程中，分配好的会话&缓存服务器负责 HTTPS 会话管理，该会话&缓存服务器同时就私钥和用户证书的加解密工作与统一验证服务器进行交互，将交互结果返回客户端；如果有多个客户端，则通过该会话&缓存服务器将各客户端映射到一台统一验证服务器上，使每个客户端分享统一验证服务器的硬件加速能力。

HTTPS 访问应答单元，设置为执行：完成握手过程后，所述会话&缓存服务器开展缓存服务为客户端提供 CDN 服务；对于客户端所请求的数据，如果是可缓存数据，直接在会话&缓存服务器获取，如果是不可缓存数据，则向源服务器获取。

其中，统一验证服务器上设有用户证书和私钥，并集成了若干 SSL 加速板卡，一台或者多台统一验证服务器对应一用户证书，该统一验证服务器设置为处理加解密；统一验证服务器的数量可以随流量线性来部署统一验证服务器的比例，需要扩展时，可将统一验证服务器进行线性扩展，每台服务器上插上若干 SSL 加速板卡，以应对更大规模的 SSL 事务处理需求；或者形成主备，以应对故障处理。

本发明实施例有效地结合SSL加速板卡和CDN网络边缘节点各自的技术优势，具有以下优点：

（1）使用 SSL 加速板卡代替普通边缘服务器的加解密工作，使边缘服务器减轻负载，将 SSL 加速板卡部署到统一验证服务器上，大大降低了普通边缘服务器的 CPU 消耗，提高了效率。

（2）使用一张 SSL 加速卡来服务若干客户的加解密工作，从原来的一对一的服务到 1 对 N，这样对 CDN 厂商而言，大大节省了成本。

（3）从原来的一张 SSL 加速卡需要管理一个证书，到现在的 N 个客户使用一张 SSL 加速板卡，证书集中式管理，这样证书的管理量大大减少，单机管理成本大大降低。

（4）统一验证服务器除了通过插 SSL 加速板卡做加解密工作，还可以根据客户的不同需求情况，在统一验证服务器上部署软件，如 CDN 服务器申请证书

方案、Cloudflare 的 keyless-SSL 方案等，本发明实施例都能有效支持；在实现与前端服务器同在边缘节点的交互，减少了服务器间往返 RTT，提高了效率。

（5）SSL 加速板卡可以在边缘统一验证服务器集群中线性扩展，以增加其事务处理能力，不影响集中管理，也节省了扩容成本。

本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围，均应涵盖在权利要求范围当中。

本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些组件或所有组件可以被实施为由处理器，如数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质（或非暂时性介质）和通信介质（或暂时性介质）。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

工业实用性

本发明实施例使用 SSL 加速板卡代替普通边缘服务器的加解密工作，使边缘服务器减轻负载，将 SSL 加速板卡部署到统一验证服务器上，大大降低了普通边缘服务器的 CPU 消耗，提高了效率。使用一张 SSL 加速卡来服务若干客户的加解密工作，从原来的一对一的服务到 1 对 N，这样对 CDN 厂商而言，大大

节省了成本。从原来的一张 SSL 加速卡需要管理一个证书，到现在的 N 个客户使用一张 SSL 加速板卡，证书集中式管理，这样证书的管理量大大减少，单机管理成本大大降低。

权利要求

1、一种基于内容分发网络的 HTTPS 加速方法，包括：该内容分发网络包括位于中心部分的内容分发网络 CDN 网管中心和域名系统 DNS 重定向解析中心、位于边缘部分的多个 CDN 网络边缘节点以及位于后端的源服务器；各 CDN 网络边缘节点分别部署了位于前端的会话&缓存服务器和位于后端的统一验证服务器；

该 HTTPS 加速方法包括：

步骤 1：客户端向 CDN 网络边缘节点发起 HTTPS 访问请求；CDN 网络边缘节点通过前端的负载均衡分配一台会话&缓存服务器与客户端进行三次握手；

步骤 2：握手过程中，分配好的会话&缓存服务器负责 HTTPS 会话管理，该会话&缓存服务器同时就私钥和用户证书的加解密工作与统一验证服务器进行交互，将交互结果返回客户端；

步骤 3：完成握手过程后，所述会话&缓存服务器开展缓存服务为客户端提供 CDN 服务；对于客户端所请求的数据，如果是为可缓存数据，直接在会话&缓存服务器获取，如果是不可缓存数据，向源服务器获取。

2、根据权利要求 1 所述的 HTTPS 加速方法，其中：所述统一验证服务器上设有用户证书和私钥，集成至少一个 SSL 加速板卡，一台或者多台统一验证服务器对应一用户证书，该统一验证服务器被设置为处理加解密。

3、根据权利要求 2 所述的 HTTPS 加速方法，其中：所述步骤 2 还包括以下过程：如果有多个客户端，则通过该会话&缓存服务器将各客户端映射到一台统一验证服务器上。

4、根据权利要求 1 或 2 或 3 所述的 HTTPS 加速方法，其中：该 HTTPS 加速方法还包括如下步骤：将统一验证服务器的比例数量随流量线性进行部署，将统一验证服务器线性扩展，每台统一验证服务器上插接至少一个 SSL 加速板卡。

5、根据权利要求 1 或 2 或 3 所述的 HTTPS 加速方法，其中：该 HTTPS 加速方法还包括如下步骤：每台统一验证服务器上插接多个 SSL 加速板卡，不同 SSL 加速板卡构成主备关系。

6、一种基于内容分发网络的 HTTPS 加速系统，该内容分发网络包括位于

中心部分的 CDN 网管中心和 DNS 重定向解析中心、位于边缘部分的多个 CDN 网络边缘节点以及位于后端的源服务器；各 CDN 网络边缘节点分别部署了位于前端的会话&缓存服务器和位于后端的统一验证服务器；

该 HTTPS 加速系统包括如下单元：

HTTPS 访问请求发起单元，设置为执行：客户端向 CDN 网络边缘节点发起 HTTPS 访问请求；

三次握手发起单元，设置为执行：CDN 网络边缘节点通过前端的负载均衡，分配一台对应的会话&缓存服务器，与客户端进行三次握手；

三次握手处理单元，用于执行：握手过程中，分配好的会话&缓存服务器负责 HTTPS 会话管理，该会话&缓存服务器同时就私钥和用户证书的加解密工作与统一验证服务器进行交互，将交互结果返回客户端；

HTTPS 访问应答单元，设置为执行：完成握手过程后，所述会话&缓存服务器开展缓存服务为客户端提供 CDN 服务；对于客户端所请求的数据，如果是可缓存数据，直接在会话&缓存服务器获取，如果是不可缓存数据，则向源服务器获取。

7、根据权利要求 6 所述的 HTTPS 加速系统，其中：所述统一验证服务器上设有用户证书和私钥，集成至少一个 SSL 加速板卡，一台或者多台统一验证服务器对应一用户证书，该统一验证服务器被设置为处理加解密。

8、根据权利要求 6 所述的 HTTPS 加速系统，其特征在于：所述三次握手处理单元还设置为执行如下操作：如果有多个客户端，则通过该会话&缓存服务器将各客户端映射到一台统一验证服务器上。

9、根据权利要求 6、7 或 8 所述的 HTTPS 加速系统，其中：所述统一验证服务器的比例数量随流量线性进行部署，将统一验证服务器线性扩展，每台统一验证服务器上插接有至少一个 SSL 加速板卡。

10、根据权利要求 6、7 或 8 所述的 HTTPS 加速系统，其中：每台统一验证服务器上插接多个 SSL 加速板卡，不同 SSL 加速板卡构成主备关系。

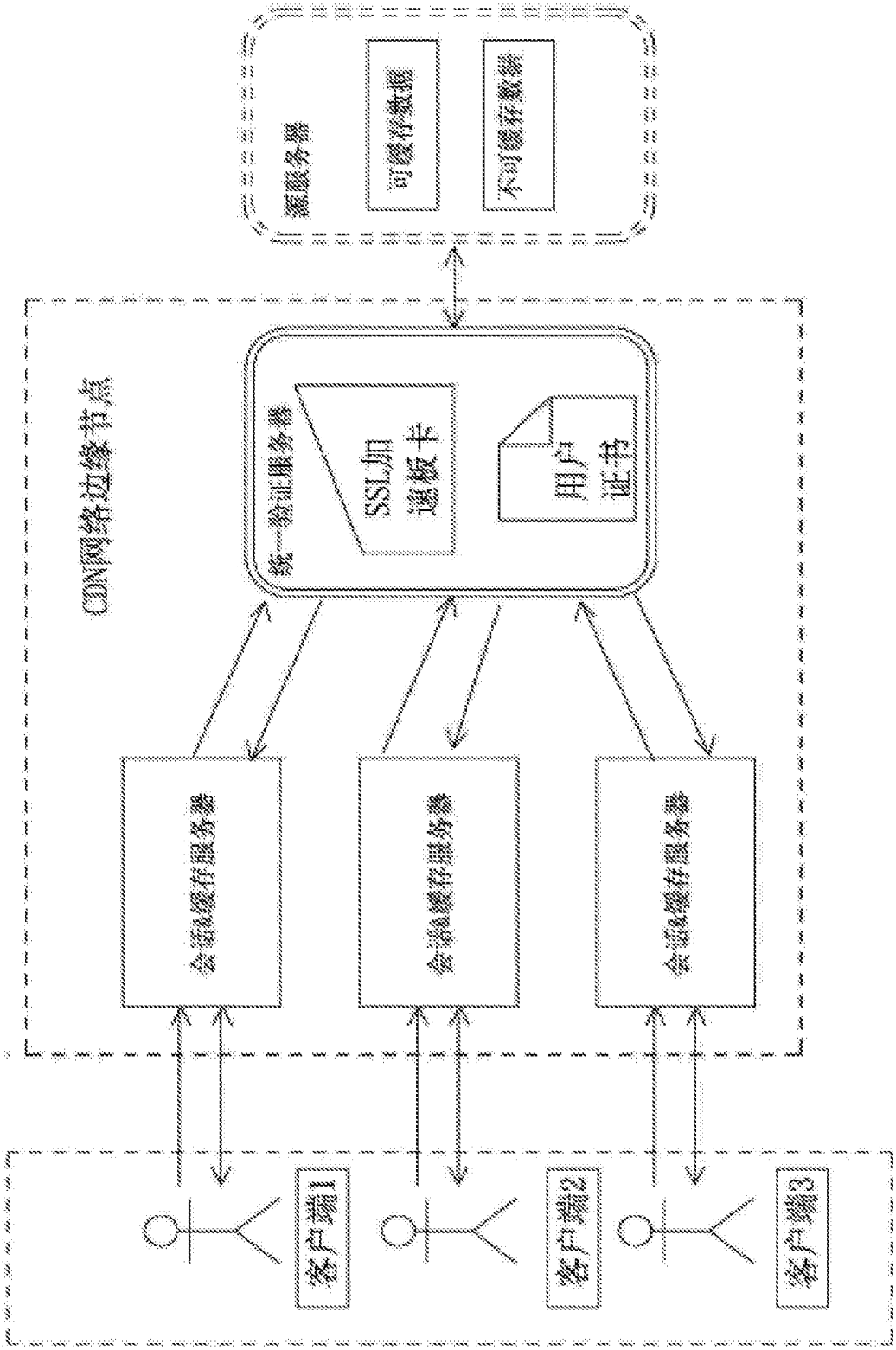
源服务器
可缓存数据
不可缓存数据
CDN网络边缘节点
统一验证服务器
SSL加速板卡
用户证书
会话缓存服务器
会话缓存服务器
会话缓存服务器
客户端1
客户端2
客户端3

图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/104806

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 9/32 (2006.01) i; H04L 29/08 (2006.01) n

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; H04Q; H04W

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, DWPI: 协处理, 加速, https, http, cdn, 内容分发, 重定向, 认证, 加密, 密钥, 秘钥, ssl

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7634650 B1 (XSIGO SYSTEMS) 15 December 2009 (15.12.2009), description, column 3, lines 59-62, column 4, lines 1-8, 13-15 and column 6, lines 16-46, and figure 2	1-10
PX	CN 106341417 A (GUIZHOU BAISHANCLOUD TECHNOLOGY CO., LTD.) 18 January 2017 (18.01.2017), claims 1-8, and description, paragraph [0020]	1-10
PA	CN 106027646 A (DU, Zaidong) 12 October 2016 (12.10.2016), entire document	1-10
PA	CN 106230782 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 14 December 2016 (14.12.2016), entire document	1-10
A	CN 104732164 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER et al.) 24 June 2015 (24.06.2015), entire document	1-10

☐ 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	Date of mailing of the international search report
21 November 2017	29 December 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer FAN, Chengbo Telephone No. (86-10) 62413571

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/104806

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 7634650 B1	15 December 2009	US 9264384 B1	16 February 2016
		US 8180949 B1	15 May 2012
		US 7937447 B1	03 May 2011
		US 8677023 B2	18 March 2014
		US 8291148 B1	16 October 2012
		US 7502884 B1	10 March 2009
		US 8041875 B1	18 October 2011
CN 106341417 A	18 January 2017	None	
CN 106027646 A	12 October 2016	None	
CN 106230782 A	14 December 2016	None	
CN 104732164 A	24 June 2015	None	

国际检索报告

国际申请号 PCT/CN2017/104806

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/32(2006.01)i; H04L 29/08(2006.01)n

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; H04Q; H04W

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,DWPI:协处理,加速,https,http,cdn,内容分发,重定向,认证,加密,密钥,秘钥,ssl

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	US 7634650 B1 (XSIGO SYSTEMS) 2009年 12月 15日 (2009-12-15) 说明书第3栏第59-62行，第4栏第1-8，13-15行，第6栏第16-46行以及附图2	1-10
PX	CN 106341417 A (贵州白山云科技有限公司) 2017年 1月 18日 (2017-01-18) 权利要求1-8及说明书第0020段	1-10
PA	CN 106027646 A (杜在东) 2016年 10月 12日 (2016-10-12) 全文	1-10
PA	CN 106230782 A (腾讯科技深圳有限公司) 2016年 12月 14日 (2016-12-14) 全文	1-10
A	CN 104732164 A (国家计算机网络与信息安全管理中心等) 2015年 6月 24日 (2015-06-24) 全文	1-10

☐ 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	国际检索报告邮寄日期
2017年 11月 21日	2017年 12月 29日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	范成博
传真号 (86-10)62019451	电话号码 (86-10)010-62413571

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/104806

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）
US	7634650	B1	2009年 12月 15日	US	9264384	B1	2016年 2月 16日
				US	8180949	B1	2012年 5月 15日
				US	7937447	B1	2011年 5月 3日
				US	8677023	B2	2014年 3月 18日
				US	8291148	B1	2012年 10月 16日
				US	7502884	B1	2009年 3月 10日
				US	8041875	B1	2011年 10月 18日
CN	106341417	A	2017年 1月 18日		无		
CN	106027646	A	2016年 10月 12日		无		
CN	106230782	A	2016年 12月 14日		无		
CN	104732164	A	2015年 6月 24日		无		