



- (51) **International Patent Classification:**
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
- (21) **International Application Number:**
PCT/MY2014/000099
- (22) **International Filing Date:**
9 May 2014 (09.05.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PI 2013002550 3 July 2013 (03.07.2013) MY
- (71) **Applicant:** MIMOS BERHAD [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (72) **Inventor:** SEAH, Boon Keong; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (74) **Agent:** MIRANDAH, Patrick; Patrick Mirandah Co. (Malaysia) Sdn Bhd, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): 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, DK, DM,

DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report (Art. 21(3))

[Continued on next page]

(54) **Title:** A SYSTEM AND METHOD FOR SYNCHRONIZING OF CACHE REMOTELY WITH PRE-FETCHING OF NON-PROTECTED CONTENTS AND PROTECTED CONTENTS

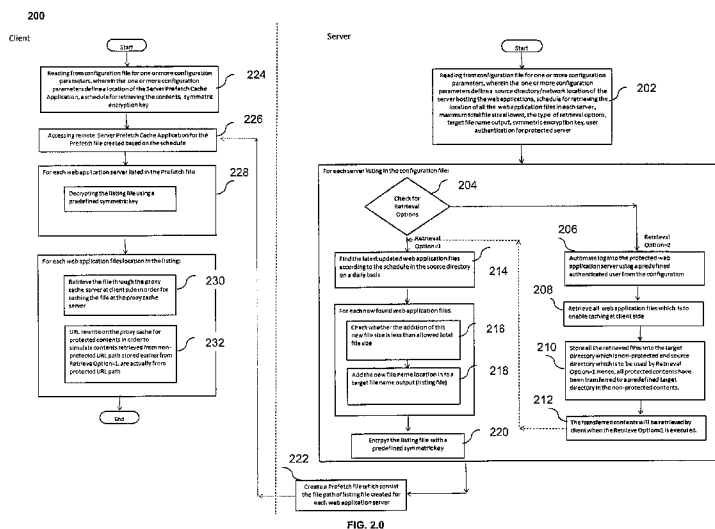


FIG. 2.0

(57) **Abstract:** Pre-fetching of both non-protected and protected contents for transparent caching is described in the present invention to improve user experience. A system (100) for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching comprising at least one proxy cache server (104, 104n) connected to a network at each client side of said system; at least one client prefetch cache application (106, 106n) connected to a network at each client side of said system; at least one server prefetch cache application (108) connected to a network at each server side of said system. The at least one client prefetch cache application (106, 106n) periodically check for server prefetch cache file listing to download files to client through said proxy cache server (104, 104n) located at client side; and the at least one server prefetch cache application (108) periodically check for both protected and non-protected of servers for new contents to be created with encrypted file listing location for retrieval by said client prefetch cache application (106, 106n). Utilization of the at least one Server Prefetch Cache Application and Client Prefetch Cache Application in both proxy cache server and application server wherein the need for enabling the file directory feature is no longer required. The present invention further provides encryption for generated resource reference path at

[Continued on next page]



-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

A SYSTEM AND METHOD FOR SYNCHRONIZING OF CACHE REMOTELY WITH PRE-FETCHING OF NON-PROTECTED CONTENTS AND PROTECTED CONTENTS

FIELD OF INVENTION

5

The present invention relates to a system and method for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching.

10 BACKGROUND ART

Prefetching of application contents is an effective solution to reduce user latency as proxy server in a cloud based system is able to cache web contents. However, there are some limitations as it may consume too much network bandwidth and system resources.

15 Crucial issues arise for accessing large web contents such as video file, image and adobe flex file in which a limited bandwidth such as 10 Mbps is used and is shared by at least 20 concurrent users. User's response time of accessing said web contents is impacted due to concurrent usage of shared bandwidth.

20 Currently, existing proxy server for caching web contents requires user to access web contents at the first time in order for proxy cache server to cache, and subsequent access will be through the proxy cache server. As the user is required to access the web contents at the first time, user response time will be delayed especially for large contents. There are applications residing at the client side to offload the web page which
25 will go through the proxy cache server with limitations such as web applications are required to enable directory browsing and enabling directory browsing will expose security risk to web applications. Further, index web page must have interlinked to all the link depth or else it will not be able to crawl all the URL files belonging to the web application. The public folder cannot cache within protected system due to the nature of
30 the implemented system which requires authentication. The said limitation drives to the need for web contents from remote site of a cloud-based system to be offloaded to proxy cache server to improve user experience.

One example of cache control method which allows a cache state in proxy server and a client use state to be synchronized which improves cache-efficiency regardless of time zones was proposed in United States Patent Publication No. US 2004/0073604 A1 hereby denoted as the US 604 Publication. The 604 Publication provide a cache control
5 method of a proxy server for relaying data between one or more clients to one communicating network and a data server connected to the other communication network with a white list. Offline file list are manually inserted at client into the white list. The white list is a useful registered URL used by the user frequently for a special purpose. However, the invention as proposed in the US 604 Publication is unable to
10 support multiple folders and multiple server location as offline file list is created at Client Side. In contrast, the present invention supports multiple folders and multiple server location for offline file creation. Further, no encryption of offline file list is provided as compared to the present invention which provides encryption on the offline file list with predefined symmetric keys. The US 604 Publication is only for non-protected contents
15 as compared to the present invention which provide both protected (authentication required to access the contents) and non-protected offline cache. The US 604 Publication does not provide standalone application as provided in the present invention wherein in the present invention the need of file directory is no longer required with Server Prefetch Cache Application and Client Prefetch Cache Application.

20 Another mechanism was proposed in United States Patent Publication No. US 2009/0100228 A1 hereby denoted as US 228 Publication. It relates generally to cache modeling in a prefetching system. The US 228 Publication provides a method for enhancing prefetch operations which includes fetching an object from a page on a web
25 server, caching instruction for the fetched object and identifying a prefetchable reference to the fetched object in a subsequent web page. The US 228 Publication does not provide encryption of offline file list as compared to the present invention which provides encryption on the offline file list with predefined symmetric keys. Further, the US 228 Publication does not provide automatic prefetching for non-peak time and does not
30 provide standalone application. In contrast, the present invention provides for standalone application, the Server Prefetch Cache Application and Client Prefetch Cache Application in which the need of file directory feature is no longer required.

Web prefetching control was proposed in an IEEE 2006 paper entitled "Web Prefetching Control Model Based on Prefetch-Cache Interaction" Lei Shi, Bing Song, Xiaoguang Ding, Zhimin Gu, and Lin Wei. Analysis of the effects of prefetching on the entire system resource based on prefetch-cache interaction and cost function of prefetching to
5 conclude the prefetching threshold which consists of delay cost and resource cost is provided. Three (3) adaptive prefetching control models are provided based on prefetch-cache interaction for replacing minimal cost items in cache, replacing the items that have zero cost in cache and replacing the average cost items in cache. It does not provide encryption of offline file list as compared to the present invention which provides
10 encryption on the offline file list with predefined symmetric keys. Further, it does not provide automatic prefetching for non-peak time and does not provide standalone application. In contrast, the present invention provides for standalone application, the Server Prefetch Cache Application and Client Prefetch Cache Application in which the need of file directory feature is no longer required.

15

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practice.

20

SUMMARY OF INVENTION

The present invention relates to a system and method for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent
5 caching to improve user experience.

One aspect of the present invention provides a system for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching. The system comprising at least one proxy cache server (104, 104n) connected
10 to a network at each client side of said system; at least one client prefetch cache application (106, 106n) connected to a network at each client side of said system; at least one server prefetch cache application (108) connected to a network at each server side of said system. At least one client prefetch cache application (106, 106n) periodically check for server prefetch cache file listing to download files to client through
15 said proxy cache server (104, 104n) located at client side; and at least one server prefetch cache application (108) periodically check for both protected and non-protected of servers for new contents to be created with encrypted file listing location for retrieval by said client prefetch cache application (106, 106n).

20 In a preferred aspect of the invention, there is provided that at least one client prefetch cache application (106, 106n) and at least one server prefetch application (108) operates as backend module and at least one prefetch cache application (106, 106n) further comprises prefetch files which consist of file path of listing created for each server application.

25 In yet another aspect of the invention there is provided a method (200) for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching. The method comprising steps of reading from configuration file by server for at least one configuration parameters (202); checking type of retrieval options
30 by server for retrieving application at server side (204); creating prefetch files consisting file path of listing file created for each server application (222); accessing said prefetch files from remote server prefetch cache application through network connection according to schedule defined in configuration file at client side (226); decrypting listing file using a predefined symmetric key as defined in said configuration file at client side

for each server application listed in said prefetch files (228); retrieving at least one file through proxy cache server at client side for caching file at proxy cache server for each application files located in said listing (230); and rewriting on proxy cache by resource reference for protected contents to simulate contents retrieved from non-protected path stored from non-protected contents (232). The resource reference used to rewrite on proxy cache is obtained from protected resource reference path. The step of checking type of retrieval options by server for retrieving application at server side (204) further comprises the following steps. If retrieval option is for protected application contents, said step (204) comprising steps of automating log into protected application server using a predefined authenticated user from said configuration (206); retrieving application files modified to enable caching at client side (208); storing retrieved files into target directory which is non-protected and source directory which is to be used by retrieval option for non-protected application contents (210); and retrieving transferred contents by client side upon executing retrieval option for non-protected application contents (212). If retrieval option is for non-protected application contents, said step (204) comprising steps of locating latest updated application files according to schedule in source directory on a daily basis (214). Further, if retrieval option is for non-protected application contents, for each new found application, said step continues by determining if addition of new file size is less than total allowed file size (216); adding name of new file location into a listing file (218). Thereafter, said listing file is encrypted with a predefined symmetric key (220).

A further preferred aspect of the invention provides for that the at least one configuration parameters defines source directory of server hosting applications, schedule for retrieving location of all application files in each server, maximum of total file size allowed, type of retrieval options, target file name output, symmetric encryption key, user authentication for protected server.

In another aspect of the invention there is provided that the type of retrieval options comprising retrieval from protected application contents or retrieval from non-protected application contents.

In yet another aspect of the invention is a method for accessing said prefetch files from remote server prefetch cache application through network connection according to

6

schedule defined in configuration file at client side comprising of client initially reading from configuration file for at least one configuration parameters which defines location of server prefetch cache application and schedule for retrieving contents and encryption key prior to accessing remote server at client side.

5

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

10

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific
5 embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1 illustrates the architecture of the system of the present invention.

FIG. 2 is a flowchart illustrating the methodology for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching of
15 the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent
5 caching to improve user experience.

Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present
10 invention and it is envisioned without departing from the scope of the appended claims.

Referring to FIG. 1.0, the system (100) according to the present invention is illustrated. FIG. 1.0 illustrates the general architecture of the system of the present invention. As illustrated in FIG. 1.0, the system (100) for synchronizing of cache remotely with pre-
15 fetching of both non-protected and protected contents for transparent caching comprising a proxy cache server (104, 104n) which is connected to a network at each client side of said system; a client prefetch cache application (106, 106n) connected to a network at each client side of said system; a server prefetch cache application (108) connected to a network at each server side of said system. The client prefetch cache
20 application (106, 106n) periodically checks for server prefetch cache file listing to download files to client through said proxy cache server (104, 104n) located at client side; and the server prefetch cache application (108) periodically checks for both protected and non-protected of servers for new contents to be created with encrypted file listing location for retrieval by said client prefetch cache application (106, 106n). Further,
25 the client prefetch cache application (106, 106n) and the server prefetch application (108) operates as backend module and the prefetch cache application (106, 106n) further comprises prefetch files which consist of file path of listing created for each server application.

Referring to FIG. 2.0, an embodiment of the method (200) of the invention is illustrated. Generally, to synchronize cache remotely with pre-fetching of both non-protected and protected contents for transparent caching, the invention includes the steps of the server reading from configuration file by server for at least one configuration parameters (202); the said configuration parameters defines source directory of server hosting applications,
30 schedule for retrieving location of all application files in each server, maximum of total

file size allowed, type of retrieval options, target file name output, symmetric encryption key, user authentication for protected server. Thereafter, the server will check for the type of retrieval options for retrieving application at server side (204) for each server listing in the configuration file. There are two types of retrieval options comprising
5 retrieval from protected application contents or retrieval from non-protected application contents. Upon confirmation of the type of retrieval option, the server will execute the required process to retrieve location of all application files in each server based on the type of retrieval option. If retrieval option is for protected application contents, the said server will automate log into protected application server using a predefined
10 authenticated user from said configuration (206) and retrieve application files modified to enable caching at client side (208). The retrieved files are stored into target directory which is non-protected and source directory which is to be used by retrieval option for non-protected application contents (210). Hence, all protected files have been transferred to a predefined target directory in the non-protected contents. The
15 transferred contents will be retrieved by client side upon execution of retrieval option for non-protected application contents (212) by said server.

Upon execution of retrieval option for non-protected application contents (212) by said server, the process continues wherein all transferred contents will be retrieved by client
20 side upon completion of the process of the server executing the required process for non-protected application contents. The server first locates for the latest updated application files according to schedule in the source directory on a daily basis (214). For each new found application, the server determines if addition of the new file size is less than the total allowed file size (216). Thereafter, the name of a new file location is added
25 into a listing file (218). The said listing file is encrypted with a predefined symmetric key (220). Upon completion of the process executed for both types of retrieval option, the server creates a prefetch file which consists of the file path of listing file created for each server application (222), said prefetch file will be used at the client side by the client wherein client access said prefetch files from remote server prefetch cache application
30 through network connection according to schedule defined in configuration file at client side (226). At the client side, prior to accessing prefetch files from remote server prefetch cache application through network connection according to schedule defined in configuration file, client initially reads from configuration file for configuration parameters

which defines location of server prefetch cache application and schedule for retrieving contents and encryption key prior to accessing remote server at client side.

5 Upon accessing remote server prefetch cache application, client decrypts listing file using a predefined symmetric key as defined in said configuration file at client side for each server application listed in said prefetch files (228). Thereafter, for each application files located in said listing; the files are retrieved through proxy cache server at client side for caching file at proxy cache server (230) and said proxy cache is rewritten by resource reference for protected contents to simulate contents retrieved from non-protected path stored from non-protected contents (232). The resource reference used to rewrite on proxy cache is obtained from protected resource reference path.

15 The present invention addresses current issues which drives to the need for application contents from remote site such as cloud based system to be offloaded to proxy cache server to improve user experience. The distinguishing features of the present invention lies in the synchronization of cache remotely with pre-fetching of both non-protected and protected contents which utilizes standalone applications namely; server prefetch cache application and client prefetch cache application.

20 Throughout this specification, unless the context requires otherwise, the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated step or element or integer or group of steps or elements or integers, but not the exclusion of any other step or element or integer or group of steps, elements or integers. Thus, in the context of this specification, the term "comprising" is used in an inclusive sense and thus should be understood as meaning "including principally, but not necessarily solely".

30 It will be appreciated that the foregoing description has been given by way of illustrative example of the invention and that all such modifications and variations thereto as would be apparent to persons of skill in the art are deemed to fall within the broad scope and ambit of the invention as herein set forth.

CLAIMS

1. A system (100) for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching comprising:
 - 5 at least one proxy cache server (104, 104n) connected to a network at each client side of said system;
 - at least one client prefetch cache application (106, 106n) connected to a network at each client side of said system;
 - at least one server prefetch cache application (108) connected to a
10 network at each server side of said system
 characterized in that
 the at least one client prefetch cache application (106, 106n) periodically check for server prefetch cache file listing to download files to client through said proxy cache server (104, 104n) located at client side; and
15 the at least one server prefetch cache application (108) periodically check for both protected and non-protected of servers for new contents to be created with encrypted file listing location for retrieval by said client prefetch cache application (106, 106n).
- 20 2. A system (100) according to Claim 1, wherein the at least one client prefetch cache application (106, 106n) and the at least one server prefetch application (108) operates as backend module.
- 25 3. A system (100) according to Claim 1, wherein the at least one prefetch cache application (106, 106n) further comprises prefetch files which consist of file path of listing created for each server application.
- 30 4. A method (200) for synchronizing of cache remotely with pre-fetching of both non-protected and protected contents for transparent caching comprising steps of:
 - reading from configuration file by server for at least one configuration parameters (202);
 - checking type of retrieval options by server for retrieving application at server side (204);

creating prefetch files consisting file path of listing file created for each server application (222);

accessing said prefetch files from remote server prefetch cache application through network connection according to schedule defined in configuration file at client side (226);

5 decrypting listing file using a predefined symmetric key as defined in said configuration file at client side for each server application listed in said prefetch files (228);

retrieving at least one file through proxy cache server at client side for caching file at proxy cache server for each application files located in said listing (230); and

10 rewriting on proxy cache by resource reference for protected contents to simulate contents retrieved from non-protected path stored from non-protected contents (232)

15 characterized in that

checking type of retrieval options by server for retrieving application at server side (204) further comprises the following steps:

If retrieval option is for protected application contents:

20 automating log into protected application server using a predefined authenticated user from said configuration (206);

retrieving application files modified to enable caching at client side (208);

25 storing retrieved files into target directory which is non-protected and source directory which is to be used by retrieval option for non-protected application contents (210); and

retrieving transferred contents by client side upon executing retrieval option for non-protected application contents (212)

30 If retrieval option is for non-protected application contents:

locating latest updated application files according to schedule in source directory on a daily basis (214);

for each new found application:

- determining if addition of new file size is less than
total allowed file size (216);
adding name of new file location into a listing file
(218); and
5 encrypting said listing file with a predefined symmetric key
(220).
5. A method according to Claim 4, wherein the at least one configuration
parameters defines source directory of server hosting applications, schedule for
10 retrieving location of all application files in each server, maximum of total file size
allowed, type of retrieval options, target file name output, symmetric encryption
key, user authentication for protected server.
6. A method (200) according to Claim 4, wherein type of retrieval options
15 comprising retrieval from protected application contents or retrieval from non-
protected application contents.
7. A method according to Claim 4, wherein accessing said prefetch files from
remote server prefetch cache application through network connection according
20 to schedule defined in configuration file at client side (226) comprising of client
initially reading from configuration file for at least one configuration parameters
which defines location of server prefetch cache application and schedule for
retrieving contents and encryption key prior to accessing remote server at client
side.
- 25 8. A method according to Claim 4, wherein resource reference used to rewrite on
proxy cache is obtained from protected resource reference path.

100

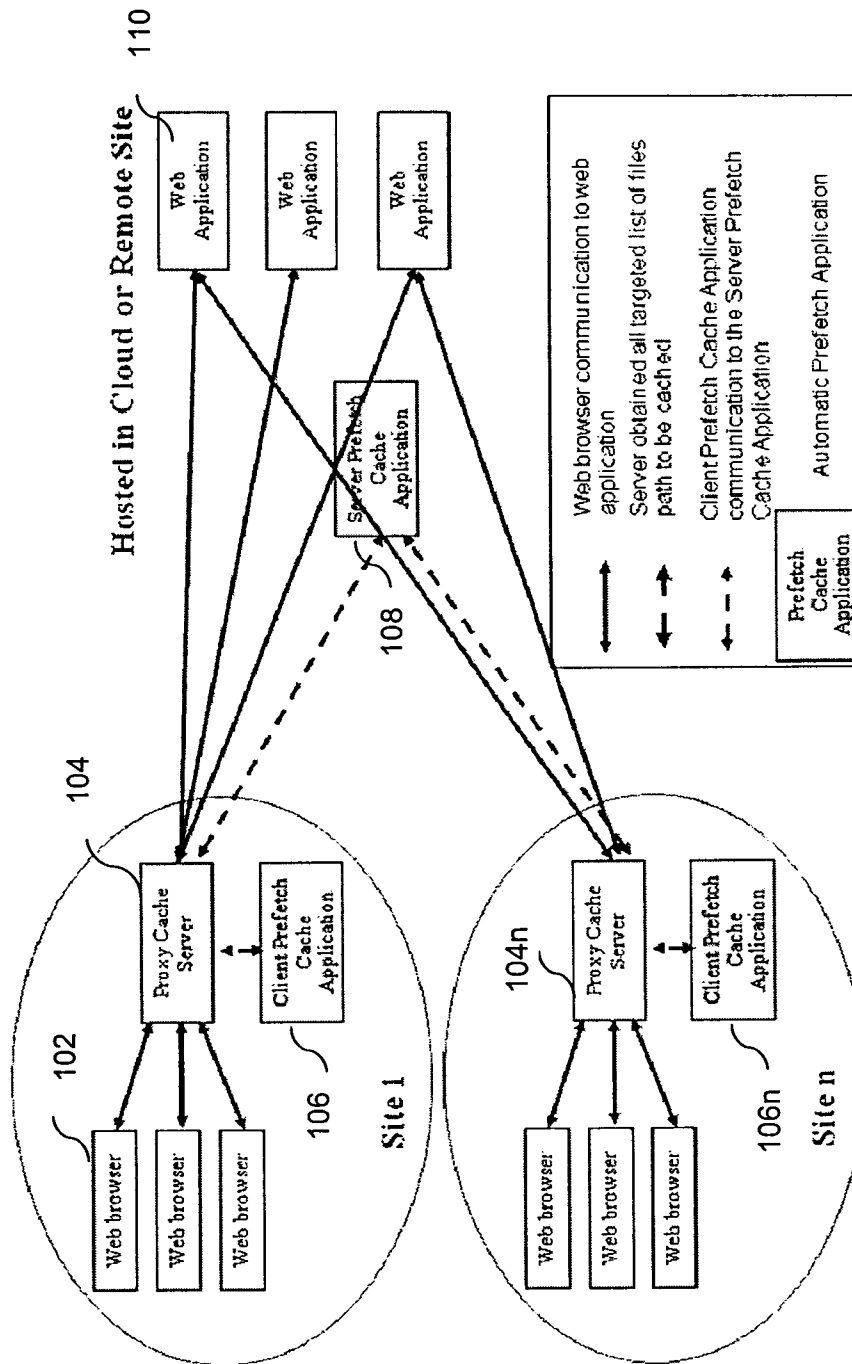


FIG. 1.0

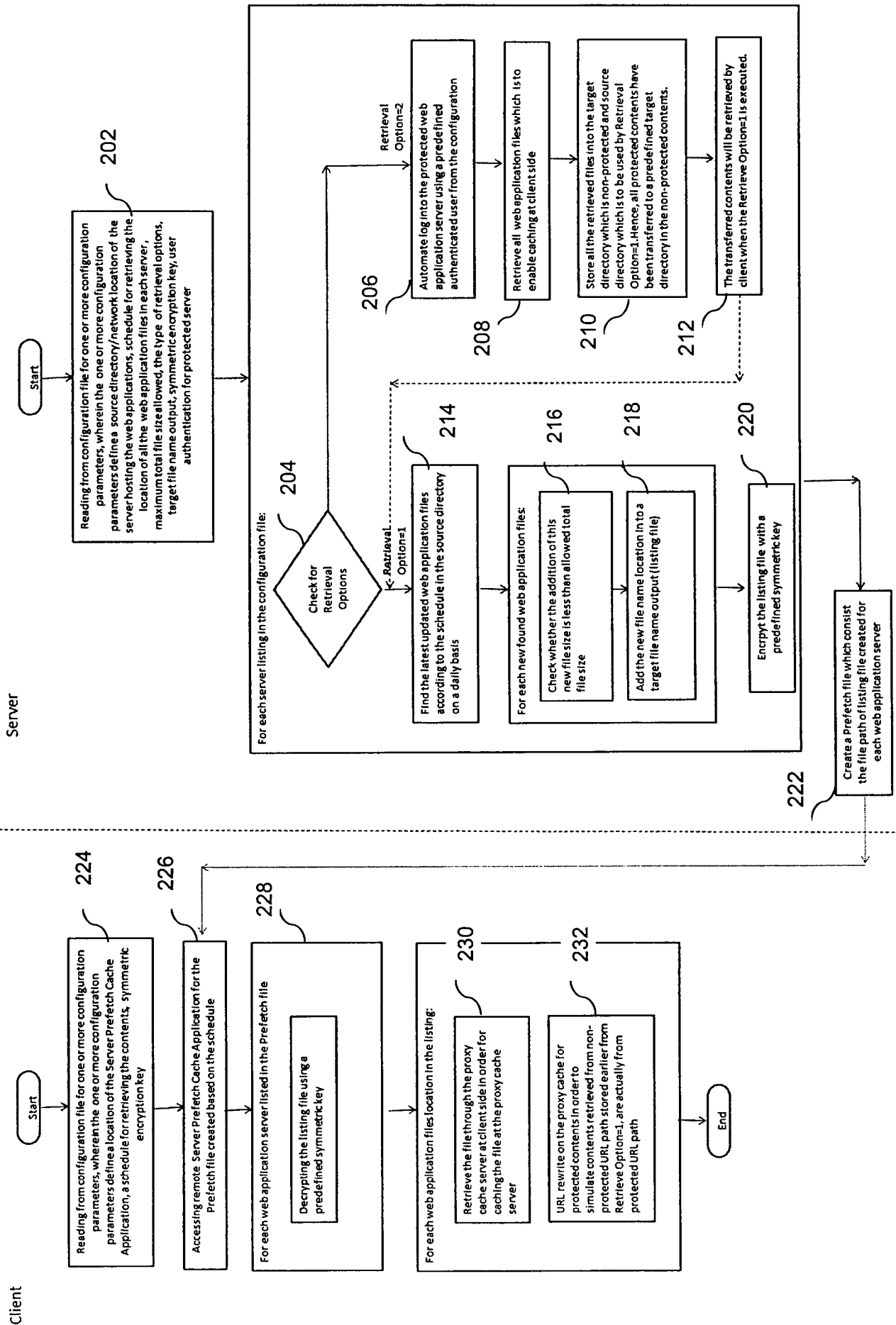


FIG. 2.0

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2014/000099

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/08 H04L29/06
ADD.

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 G06F

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)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JOHANN MARQUEZ ET AL: "A web caching and prefetching simulator", SOFTWARE, TELECOMMUNICATIONS AND COMPUTER NETWORKS, 2008. SOFTCOM 2008. 16TH INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 25 September 2008 (2008-09-25), pages 346-350, XP031360148, ISBN: 978-953-6114-97-9 ----- -/--	1-8



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

22 October 2014

Date of mailing of the international search report

11/11/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Manea, Anda

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2014/000099

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Anonymous: "Perforce 2012.2 System Administrator's Guide - Chapter.9: Perforce Proxy", Perforce Software. 1 October 2012 (2012-10-01), pages 173-181, XP002731508, Retrieved from the Internet: URL:ftp://ftp.perforce.com/pub/perforce/r12.2/doc/manuals/p4sag/p4sag.pdf [retrieved on 2014-10-22] page 173, last paragraph page 177, paragraph 1 page 181, paragraph 1-3 -----	4-8