



- (51) **International Patent Classification:**
G06F 17/30 (2006.01) *G06F 12/14* (2006.01)
G06F 21/30 (2013.01)
- (21) **International Application Number:**
PCT/US2016/016461
- (22) **International Filing Date:**
3 February 2016 (03.02.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
201510062422.6 5 February 2015 (05.02.2015) CN
- (71) **Applicant:** ALIBABA GROUP HOLDING LIMITED
[—/US]; Forth Floor, One Capital Place, P.O. Box 847,
George Town, Grand Cayman (KY).
- (72) **Inventor:** LIN, Xiaobin; Alibaba Group Legal Depart-
ment, 5/F, Building 3, No. 969 West Wen Yi Road, Yu
Hang District, Hangzhou, 311121 (CN).
- (74) **Agent:** JIA, Alexandra, C.; Murabito Hao & Barnes LLP,
2 N. Market St., 3rd Floor, San Jose, CA 95113 (US).

- (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, 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, ST, 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).

Published:

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

(54) **Title:** SYSTEM, METHOD AND DATABASE PROXY SERVER FOR SEPARATING OPERATIONS OF READ AND WRITE

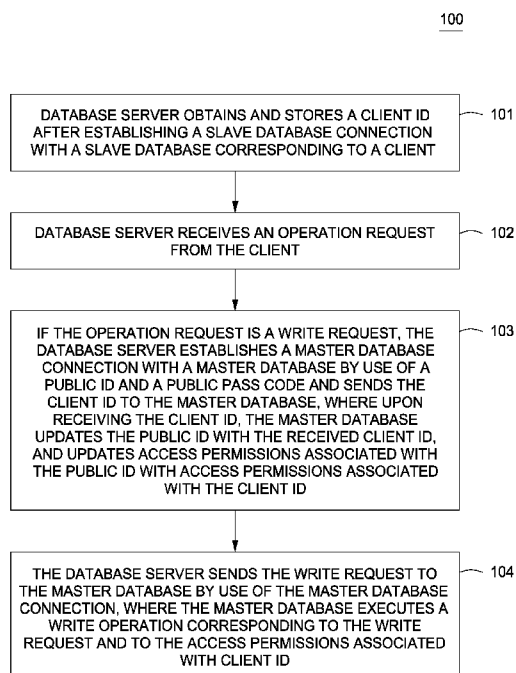


FIG. 1

(57) **Abstract:** A method of separating read operations from write operations includes obtaining and storing a client ID after establishing a slave database connection with a slave database corresponding to a client, and receiving an operation request from the client. If the operation request is a write request, the method also includes establishing a master database connection with a master database by use of a public ID and a public passcode and sending the client ID to the master database, where upon receiving, the master database updates the public ID with the received client ID, and updates access permissions associated with the public ID with access permissions associated with the client ID. The method further includes sending the write request to the master database by use of the master database connection, where a write operation corresponding to the write request and to the access permissions associated with client ID is executed.

SYSTEM, METHOD AND DATABASE PROXY SERVER FOR SEPARATING OPERATIONS OF READ AND WRITE

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefits to Chinese Patent Application No. 201510062422.6, filed on Feb. 5, 2015, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present invention relates generally to communication technologies, and more particularly to a system, method and database proxy server for separating read operations and write operations.

BACKGROUND

[0003] Databases are warehouses that organize, store and manage data according to data structures. Data are stored collectively in a database in certain formats, providing data access for a multitude of clients. In order to facilitate multiple clients sharing databases and alleviate the limits imposed by one single database servicing multiple clients, currently a master database will be designated, which is duplicated into multiple slave databases having identical datasets as the master database. Further, techniques separating read operations from write operations are applied to the database system, i.e., a read request from a client (e.g., a query statement executed by the client) is directed to the slave databases; while a write request from the client (e.g., an update statement executed by the client) is directed to the master database.

[0004] The present techniques separating read operations from write operations can be implemented as the following. First, a database proxy server receives from a client a communication request for a connection to a slave database, where the request includes a client ID and a client passcode. Based upon the client ID, the database proxy server sends the request to a corresponding slave database. Upon receiving the request, the slave database obtains the client ID and the client passcode from the request, and performs verification of the client. If the client passes the verification, the slave database accordingly establishes a slave database connection with the database proxy server. Subsequently, the database proxy server receives from the client operation requests. If receiving a read request, the database proxy server executes a read operation

corresponding to the read request against the slave database directly. If receiving a write request, the database proxy server establishes a master database connection with the master database by use of a public ID and a public passcode, and executes a write operation corresponding to the write request against the master database.

[0005] However, with the present techniques to separate read operations and write operations, multiple clients all rely on one common public ID to establish connections with the master database. The public ID has its access permissions set as the super set of all the clients' access permissions. Consequently, some clients can end up performing operations outside of their access permissions configured with the master database, over-extending their access permissions and imposing potential security risks. For example, client A has an original access permission configured as writing to only the A part of the master database. Client B has an original access permission configured as writing to both the A part and the B part of the master database. When client A and client B both utilize a common public ID to establish connections with the master database, the access permission associated with the public ID is set accordingly as writing to both the part A and the part B of the master database. Therefore, client A ends up being able to write to the part B of the database as well.

SUMMARY

[0006] According to an exemplary embodiment of the present disclosure, a method of separating a read operation from a write operation includes the step of a database server obtaining and storing a client ID after establishing a slave database connection with a slave database corresponding to a client. The method also includes the step of receiving an operation request from the client, and if the operation request is a write request, the method further includes the steps of the database server establishing a master database connection with a master database by use of a public ID and a public passcode, and sending the client ID to the master database. Upon receiving the client ID, the master database updates the public ID with the received client ID and updates access permissions associated with the public ID with access permissions associated with the client ID. The method further includes the database server sending the write request to the master database by use of the master database connection, where the master database executes a write operation corresponding to the write request and to the access permissions associated with client ID.

[0007] Alternatively, the step of obtaining and storing a client ID of the method includes the database server receiving a slave database connection request from the client, the connection request

including a client ID and a client passcode. The step further includes the database server sending the connection request to the slave database corresponding to the client such that, upon receiving the connection request, the slave database obtains the client ID and the client passcode from the connection request. The slave database verifies the client by use of the obtained client ID and client passcode, and if the client is successfully verified, establishes the slave database connection with the database server. The step further includes obtaining and storing the client ID from the connection request.

[0008] Further alternatively, the method includes, after the step of the database server receiving an operation request from the client, if the operation request is a read request, the database server sending the read request through the slave database connection to the slave database corresponding to the client, where a read operation corresponding to the read request is executed against the slave database.

[0009] Still further alternatively, the step of establishing a master database connection with a master database by use of a public ID and a public passcode of the method includes the database server sending the public ID and the public passcode to the master database such that, upon receiving the public ID and the public passcode, the master database verifies the database server by use of the received public ID and public passcode. If the database server is successfully verified, the master database establishes the master database connection with the database server.

[0010] Yet further alternatively, the method further includes, after the step of the establishing the master database connection with the master database by use of the public ID and the public passcode, the database server caching the master database connection with the master database.

[0011] According to another exemplary embodiment of the present disclosure, a database server includes an obtaining module, a receiving module, an establishment module and a writing module. The obtaining module is configured for obtaining and storing a client ID after establishing a slave database connection with a slave database corresponding to a client. The receiving module is configured for receiving an operation request from the client. The establishment module is configured for, if the operation request is a write request, establishing a master database connection with a master database by use of a public ID and a public passcode and sending the client ID to the master database, where upon receiving the client ID, the master database updates the public ID with the received client ID, and access permissions associated with the public ID with access permissions associated with the client ID. And, the writing module is configured for sending the write request to the master database by use of the master database connection, where the master database executes a

write operation corresponding to the write request and to the access permissions associated with client ID.

[0012] Alternatively, the obtaining module of the database server includes a receiving module, a sending module and a storing module. The receiving module is configured for receiving a slave database connection request from the client, the connection request including a client ID and a client passcode. The sending module is configured for sending the connection request to the slave database corresponding to the client, where upon receiving the connection request, the slave database obtains the client ID and the client passcode from the connection request, verifies the client by use of the obtained client ID and client passcode. If the client is successfully verified, the slave database establishes the slave database connection with the database server. And, the storing module is configured for obtaining and storing the client ID from the connection request.

[0013] Further alternatively, the database server further includes a read module configured for, if the operation request is a read request, sending the read request through the slave database connection to the slave database corresponding to the client. Subsequently, a read operation corresponding to the read request is executed against the slave database.

[0014] Still further alternatively, the establishment module includes a setup module configured for sending the public ID and the public passcode to the master database, where upon receiving the public ID and the public passcode, the master database verifies the database server by use of the received public ID and public passcode. If the database server is successfully verified, the master database establishes the master database connection with the database server.

[0015] Yet further alternatively, the database server further includes a cache module configured for, after establishing the master database connection with the master database by use of the public ID and the public passcode, caching the master database connection with the master database.

[0016] According to yet another exemplary embodiment of the present disclosure, a system for separating a read operation from a write operation includes a database server and a master database. The database server includes an obtaining module, a receiving module, an establishment module and a write module. The receiving module is configured for receiving an operation request the client. The establishment module is configured for, if the operation request is a write request, establishing a master database connection with the master database by use of a public ID and a public passcode and sending the client ID to the master database. The write module is configured for, after the master database updates access permissions associated with the public ID with access permissions associated with the client ID, sending the write request to the master database by use of the master

database connection, where the master database executes a write operation corresponding to the write request and to the access permissions associated with the client ID. The master database includes an update module configured for receiving the client ID, updating the public ID with the received client ID, and updating the access permissions associated with the public ID with the access permissions associated with the client ID.

[0017] Alternatively, the obtaining module of the system includes a receiving module, a sending module and a storing module. The receiving module is configured for receiving a slave database connection request from the client, the connection request including a client ID and a client passcode. The sending module is configured for sending the connection request to a slave database corresponding to the client. The storing module is configured for, after the slave database connection is established with the slave database, obtaining and storing the client ID from the connection request. Correspondingly, the system further includes a slave database. The slave database include a first verification module configured for receiving the slave database connection request, obtaining the client ID and the client passcode from the connection request, and verifying the client with the obtained client ID and client passcode. If the client is verified successfully, the slave database connection is established with the database server.

[0018] Further alternatively, the database server of the system further includes a read module configured for, if the operation request is a read request, sending the read request through the slave database connection to the slave database corresponding to the client, where a read operation corresponding to the read request is executed against the slave database.

[0019] Still further alternatively, the establishment module of the system includes a setup module configured for sending the public ID and the public passcode to the master database. The master database of the system further includes a second verification module configured for receiving the public ID and the public passcode, verifying the database server by use of the received public ID and public passcode. If the database server is successfully verified, the master database establishes the master database connection with the database server.

[0020] Yet further alternatively, the database server of the system includes a cache module configured for, after establishing the master database connection with the master database by use of the public ID and the public passcode, caching the master database connection with the master database.

[0021] Compared to the present techniques, the present disclosure provides for several technical effects. First, after the database server establishes a slave database connection with a slave database

corresponding to a client, upon receiving a read request, the database server uses a public ID and a public passcode to establish a master database connection with the master database and sends the client ID to the master database. Upon receiving the client ID, the master database updates the present user's ID (i.e., the public ID) to the client ID, and the access permissions associated with the present user's ID (i.e., the public ID) to the access permissions associated with the client ID such that the client cannot operate against the master database exceeding the access permissions configured for the client and thus the security of the system can be enhanced.

[0022] Secondly, after establishing a master database connection with the master database by use of a public ID and a public passcode, the database server caches such master database connection. Subsequently, after establishing a slave database connection with the slave database corresponding to other clients, when the database server receives a write request from those other clients, the database server can communicate with the master database through the cached master database connection. Those subsequent write operations can be performed without executing the verification by use of the public ID and the public passcode or the establishment of a connection with the master database. By doing so, the database server is able to speed up the time to complete a write request. Nevertheless, it is not necessary for embodiments of the present disclosure to incorporate all the effects described above.

DESCRIPTION OF THE DRAWINGS

[0023] The accompanying drawings, which are incorporated in and form a part of this specification and in which like numerals depict like elements, illustrate embodiments of the present disclosure and, together with the description, serve to explain the principles of the disclosure.

[0024] FIG. 1 is a flow chart of a first exemplary method of separating read operations from write operations in accordance with an embodiment of the present disclosure;

[0025] FIG. 2 is an illustration of an exemplary separation of read operations from write operations in accordance with an embodiment of the present disclosure;

[0026] FIG. 3 is a flow chart of a second exemplary method of separating read operations from write operations in accordance with an embodiment of the present disclosure;

[0027] FIG. 4 is a flow chart of a third exemplary method of separating read operations from write operations in accordance with an embodiment of the present disclosure;

[0028] FIG. 5 is a block diagram of a first exemplary database proxy server in accordance with an embodiment of the present disclosure;

[0029] FIG. 6 is a block diagram of a second exemplary database proxy server in accordance with an embodiment of the present disclosure;

[0030] FIG. 7 is a block diagram of a third exemplary database proxy server in accordance with an embodiment of the present disclosure;

[0031] FIG. 8 is a system block diagram of a first exemplary system of separation of read operations from write operations in accordance with an embodiment of the present disclosure;

[0032] FIG. 9 is a system block diagram of a second exemplary system of separation of read operations from write operations in accordance with an embodiment of the present disclosure;

[0033] FIG. 10 is a system block diagram of a third exemplary system of separation of read operations from write operations in accordance with an embodiment of the present disclosure;

[0034] FIG. 11 is a system block diagram of a fourth exemplary system of separation of read operations from write operations in accordance with an embodiment of the present disclosure; and

[0035] FIG. 12 is a system block diagram of a fifth exemplary system of separation of read operations from write operations in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0036] In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. However, it will become obvious to those skilled in the art that the present disclosure may be practiced without these specific details. The descriptions and representations herein are the common means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the present disclosure.

[0037] Reference herein to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one embodiment of the disclosure. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Used herein, the terms “upper”, “lower”, “top”, “bottom”, “middle”, “upwards”, and “downwards” are intended to provide relative positions for the purposes of description, and are not intended to designate an absolute frame of reference. Further, the order of blocks in process flowcharts or diagrams

representing one or more embodiments of the disclosure do not inherently indicate any particular order nor imply any limitations in the disclosure.

[0038] Embodiments of the present disclosure are discussed herein with reference to FIGS. 1-12. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the disclosure extends beyond these limited embodiments.

[0039] Referring to FIG. 1, a flow chart of an exemplary method of separating a read operation from a write operation is shown in accordance with an embodiment of the present disclosure. Method 100 starts in step 101, where database proxy server obtains and stores a client ID after establishing a slave database connection with a slave database corresponding to a client. The client ID is the only identification associated with the client and can be represented in the forms such as the name of the client or the source IP of the client (e.g., username@userhost), etc. In step 102, the database proxy server received from the client operation requests. Operation requests can include read requests and write requests. For example, when the client executes a query statement, a read request is sent accordingly; when the client executes an update statement, a write request is sent instead.

[0040] In step 103, when an operation request is a write request, the database proxy server uses a public ID and a public passcode to establish with a master database a master database connection, through which the client ID is sent to the master database. Upon receiving the client ID, the master database updates the present user under the public ID to the received client ID, and the access permissions associated with the present user under the public ID to the access permissions associated with the client ID.

[0041] In particular, the public ID is a public account assigned to the database server proxy. The database proxy server sends the public ID and the public passcode to the master database, which verifies the database proxy server based upon the received public ID and public passcode. If the verification is successful, the master database establishes a master database connection with the database proxy server.

[0042] After the establishment of the master database connection, the database proxy server can cache such master database connection. In particular, with a cached master database connection, when the database proxy server receives a slave database connection request from other clients, after establishing a slave connection with the slave database corresponding to the clients, and upon receiving a write request from those other clients, the database proxy server can communicate with

the master database through the cached master database connection, without executing the establishment of another master database connection or the verification of the master database again by use of the public ID and the public passcode. By doing so, the database proxy server is able to speed up the time to complete write requests.

[0043] The master database updates the present user from the public ID to the client ID, and the access permissions for the present user from the access permissions associated with the public ID to the access permissions associated with the client ID. For example, the public user account can be replaced with the client account, for example, by use of a statement “change user to username@userhost.”

[0044] In step 104, the database proxy server sends the write request through the master database connection to the master database. A write operation to the master database corresponding to the write request and within the access permissions associated with the client ID is executed. In particular, such a write operation can be an operation of INSERT, UPDATE, DELETE, etc.

[0045] The connecting with the master database, updating the public ID to the client ID, updating the access permissions associated with the public ID to the access permissions associated with the client ID are all initiated by the database proxy server. Therefore, it is after the database proxy server updates the access permissions associated with the public ID to the ones associated with the client ID that the database proxy server will send the write request through the master database connection to the master database. As a result, a write operation to the master database would not exceed the access permissions associated with the client that sends the write request.

[0046] Referring to FIG. 2, an illustration of an exemplary separation of read operations from write operations is shown in accordance with an embodiment of the present disclosure. The database server proxy 202 is an intermediary layer between the clients 204 and a database system including the master database (master database) 206 and the plurality of slave databases (slave database) 208. The database proxy server 202 is responsible for receiving requests from the clients 204, and communicating directly with the databases. The database proxy server 202 maintains the meta-data of the databases, including the information such as the physical addresses and status of the data, making the storage distribution of the data in the databases transparent to the clients 204.

[0047] Referring to FIG. 3, a flow chart of an exemplary method of separating read operations from write operations is shown in accordance with an embodiment of the present disclosure. Method 300 starts in step 101a, where the database proxy server receives a slave database connection request from a client. The slave database connection request includes a client ID and a

client passcode. The client ID can be transmitted without encryption, while the client passcode is transmitted with encryption. The database proxy server can obtain the client ID without decryption from the slave database request.

[0048] In step 101b, the database proxy server sends the slave database connection request to the slave database corresponding to the client. The slave database receives the request and obtains the client ID and the client passcode from the request. Based upon the client ID and the client passcode, the client is verified by the slave database. If the verification is successful, the slave database establishes a slave database connection with the database proxy server.

[0049] In particular, there are a plurality of slave databases, and the mapping relationship between a client and a slave database can be pre-configured according to the number and/or location of the clients and slave databases. Upon receiving a slave database connection request, the database proxy server sends the request to the slave database corresponding to the client according to the pre-configured mapping relationship.

[0050] As the client passcode is transmitted with encryption, the slave database and the database proxy server can have methods for encryption pre-configured for the client. When the slave database receives a request for a slave database connection, it decrypts the request based on the decryption methods corresponding to the pre-configuration to obtain the client passcode from the slave database connection request. Further, the slave database caches a relationship mapping between the client IDs and the client passcodes. The slave database can also query such a mapping to verify the obtained client IDs and client passcodes.

[0051] In step 101c, the database proxy server obtains the client ID from the slave database connection request and stores the client ID obtained. In particular, as the client ID is transmitted without encryption, the database proxy server can obtain the client ID directly from the slave database connection request.

[0052] Referring to FIG. 4, a flow chart of an embodiment of separating read operations from write operations is shown in accordance with an embodiment of the present disclosure. The database proxy server establishes a slave database connection with a slave database corresponding to the client, obtains and stores the client ID in step 101. After the database proxy server receives an operation request from the client in step 102, when the operation request is a read request, the database proxy server sends the read request through the slave database connection to the slave database corresponding to the client and executes a read operation corresponding to the read request against the slave database in step 105.

[0053] In particular, when the operation request is a read request, the database proxy server uses the established slave database connection directly to execute a read operation corresponding to the read request against the slave database. Such read requests include read operations, query operations, etc.

[0054] On the other hand, after the database proxy server receives an operation request from the client in step 102, when the operation request is a write request, the database proxy server uses a public ID and a public passcode to establish with a master database a master database connection, through which the client ID is sent to the master database. Upon receiving the client ID, the master database updates the present user's ID (i.e., the public ID) to the received client ID, and the access permissions associated with the present user under the public ID to the access permissions associated with the client ID. Therefore, without the access permissions exceeding the ones associated with the client ID, the client cannot operate against the master database outside the access permissions configured and the security of the system can be enhanced.

[0055] After establishing a master database connection with the master database using the public ID and the public passcode, the database proxy server caches the master database connection. When the database proxy server receives write requests from other clients after establishing slave database connections with those clients, it communicates with the master database directly through the cached master database connection, without executing the establishment or the verification by use of the public ID and the public passcode. By doing so, the database server is able to speed up the time to complete write requests.

[0056] Referring to FIG. 5, a block diagram of an exemplary database proxy server is shown in accordance with embodiments of the present disclosure. The database proxy server 500 includes an obtaining module 201, a receiving module 202, an establishment module 203, and a write module 204. The obtaining module 201 is configured for, after the database proxy server establishes a slave database connection with a slave database corresponding to the client, obtaining and storing the client ID. The receiving module 202 is configured for receiving an operation request from the client. The establishment module 203 is configured for, when the operation request is a write request, establishing a master database connection with the master database by use of the public ID and the public passcode such that upon receiving the client ID, the master database updates the present user's ID, i.e., the public ID to the received client ID, the access permissions for the present user associated with the public ID to the access permissions associated with the client ID. The write operation module 204 is configured for sending the write request to the master database through the

master database connection, and executing a write operation corresponding to the write request and within the access permissions associated with the client ID.

[0057] Further, the obtaining module 201 can also include a receiving module, a sending module and a storing module. The receiving module is configured for receiving from the client a slave database connection request, which includes a client ID and a client passcode. The sending module is configured for sending the slave database connection request to the slave database corresponding to the client such that the slave database receives the request and obtains from the request both the client ID and the client passcode. The slave database further verifies the client based on the obtained client ID and the client passcode. If the client is successfully verified, a slave database connection is established with the database proxy server. The storing module is configured for obtaining the client ID from the slave database connection request and storing the obtained client ID.

[0058] Referring to FIG. 6, a block diagram of another exemplary database proxy server is shown in accordance with embodiments of the present disclosure. The database proxy server 600 includes a read operation module 205 in addition to an obtaining module 201, a receiving module 202, an establishment module 203 and a write module 204. The read operation module is configured for, when the operation request is a read request, sending the read request through the slave database connection to the slave database corresponding to the client, and executing against the slave database a read operation corresponding to the read request.

[0059] Further, the establishment module 203 can include a setup module configured for sending the public ID and the public passcode to the master database such that upon receiving, the master database uses the public ID and the public passcode to verify the database proxy server. If the verification is successful, the master database establishes a master database connection with the database proxy server.

[0060] Referring to FIG. 7, a block diagram of another exemplary database proxy server is shown in accordance with embodiments of the present disclosure. The database proxy server 700 includes a cache module 206 in addition to an obtaining module 201, a receiving module 202, an establishment module 203, a write operation module 204 and a read operation module 205. The cache module 206 is configured for, after establishing a master database connection with the master database by use of the public ID and the public passcode, caching the master database connection with the master database.

[0061] In accordance with embodiments of the method of separating read operations from write operations of the present disclosure, the database proxy server establishes a slave database

connection with a slave database corresponding to the client. When the operation request is a write request, the database proxy server uses a public ID and a public passcode to establish with a master database a master database connection, through which the client ID is sent to the master database. Upon receiving the client ID, the master database updates the present user's ID, i.e., the public ID to the received client ID, and the access permissions for the present user associated with the public ID to the access permissions associated with the client ID. Therefore, without the access permissions exceeding the ones associated with the client ID, the client cannot operate against the master database outside the access permissions and the security of the system can be enhanced.

[0062] After establishing a master database connection with the master database using the public ID and the public passcode, the database proxy server caches the master database connection. When the database proxy server receives write requests from other clients after establishing slave database connections with those clients, it communicates with the master database directly through the cached master database connection, without executing the establishment or the verification by use of the public ID and the public passcode. By doing so, the database server is able to speed up the time to complete write requests.

[0063] Referring to FIG. 8, a block diagram of an exemplary system for separating read operations from write operations is shown in accordance with embodiments of the present disclosure. The system 800 includes a database proxy server 30 and a master database 40. The database proxy server 30 includes an obtaining module 301, a receiving module 302, an establishment module 303 and a write operation module 304. The obtaining module 301 is configured for, after the database proxy server 30 establishing a slave database connection with a slave database 50 corresponding to the client, obtains and stores the client ID. The receiving module 302 is configured for receiving an operation request from the client. The establishment module 303 is configured for, when the operation request is a write request, establishing a master database connection with the master database 40 by use of the public ID and the public passcode, and sending the client ID to the master database 40.

[0064] The master database 40 includes an update module 401, configured for receiving the client ID, updating the present user's ID, i.e., the public ID to the received client ID, and updating the present user's access permissions for the present user associated with the public ID to the access permissions associated with the client ID.

[0065] The write operation module 304 is configured for, after the update module 401 of the master database 40 updates the access permissions associated with the present user under the public

ID to the ones associated with the client ID, sending the write request to the master database 40 through the master database connection, and executing a write operation corresponding to the write request and within the access permissions associated with the client ID to the master database 40.

[0066] Further, the obtaining module 301 can include a receiving module, a sending module and a storing module. The receiving module is configured for receiving from the client a slave database connection request, which includes a client ID and a client passcode. The sending module is configured for sending the slave database connection request to the slave database 50 corresponding to the client.

[0067] Referring to FIG. 9, a block diagram of another exemplary system for separating read operations from write operations is shown in accordance with embodiments of the present disclosure. The system 900 includes a slave database 50 including a first verification module 501, in addition to a database proxy server 30 and a master database 40. The database proxy server 30 includes an obtaining module 301, a receiving module 302, an establishment module 303 and a write operation module 304. The master database 40 includes an update module 401.

[0068] Correspondingly, the obtaining module 301 also includes a storing module configured for, after the first verification module 501 of the slave database 50 establishes a slave database connection with the database proxy server 30, obtaining the client ID from the slave database connection request, and storing the obtained client ID.

[0069] Referring to FIG. 10, a block diagram of another exemplary system for separating read operations from write operations is shown in accordance with embodiments of the present disclosure. The system 1000 includes a database proxy server 30 including a read operation module 305 in addition to a master database 40. The database proxy server 30 also includes an obtaining module 301, a receiving module 302, an establishment module 303 and a write operation module 304. The master database 40 includes an update module 401. The read module 305 is configured for, when the operation request is a read request, sending the read request through the slave database connection to the slave database 50 corresponding to the client, and executing a read operation corresponding to the read request against the slave database 50. Correspondingly, the establishment module 303 includes a setup module configured for sending the public ID and the public passcode to the master database 40.

[0070] Referring to FIG. 11, a block diagram of another exemplary system for separating read operations from write operations is shown in accordance with embodiments of the present disclosure. The system 1100 includes a second verification module 402 of the master database 40.

The database proxy server 30 includes an obtaining module 301, a receiving module 302, an establishment module 303 and a write operation module 304. The second verification module 402 is configured for receiving the public ID and the public passcode, and verifying the database proxy server 30 based on the received public ID and the public passcode. If the verification is successful, a master database connection is established with the database proxy server 30.

[0071] Referring to FIG. 12, a block diagram of another exemplary system for separating read operations from write operations is shown in accordance with embodiments of the present disclosure. The system 1200 includes a cache module 306 of the database proxy server 30. The database proxy server 30 also includes an obtaining module 301, a receiving module 302, an establishment module 303 and a write operation module 304. The master database 40 includes an update module 401. The cache module 306 is configured for, after establishing a master database connection with the master database 40 by use of the public ID and the public passcode, caching the master database connection.

[0072] In accordance with embodiments of the method of separating read operations from write operations of the present disclosure, the database proxy server establishes a slave database connection with a slave database corresponding to the client. When the operation request is a write request, the database proxy server uses a public ID and a public passcode to establish with a master database a master database connection, through which the client ID is sent to the master database. Upon receiving the client ID, the master database updates the present user's ID, i.e., the public ID to the received client ID, and the access permissions associated with the present user under the public ID to the access permissions associated with the client ID. Therefore, without the access permissions exceeding the ones associated with the client ID, the client cannot operate against the master database outside the configured access permissions and the security of the system can be enhanced.

[0073] After establishing a master database connection with the master database using the public ID and the public passcode, the database proxy server caches the master database connection. When the database proxy server receives write requests from other clients after establishing slave database connections with those clients, it communicates with the master database directly through the cached master database connection, without executing the establishment or the verification processes by use of the public ID and the public passcode. By doing so, the database server is able to speed up the time to complete write request.

[0074] The database proxy server and the system for separating read operations from write operations correspond to the method of separating read operations from write operations, details are substantially the same as illustrated above and will not be repeated here. Further, the method of separating read operations from write operations can also be applied to multiple clients having different access permissions, as well as multiple cloud based clients.

[0075] Embodiments of the present disclosure can be implemented using software, hardware, firmware, and/or the combinations thereof. Regardless of being implemented using software, hardware, firmware or the combinations thereof, instruction code can be stored in any kind of computer readable media (for example, permanent or modifiable, volatile or non-volatile, solid or non-solid, fixed or changeable medium, etc.). Similarly, such medium can be implemented using, for example, programmable array logic (PAL), random access memory (RAM), programmable read only memory (PROM), read only memory (ROM), electrically erasable programmable ROM (EEPROM), magnetic storage, optical storage, digital versatile disc (DVD), or the like.

[0076] It is necessary to point out that, modules or blocks described by embodiments of the present disclosures are logical modules or logical blocks. Physically, a logical module or logical block can be a physical module or a physical block, a part of a physical module or a physical block, or the combinations of more than one physical modules or physical blocks. Physical implementation of those logical module or logical blocks is not of essence. The realized functionalities realized by the modules, blocks and the combinations thereof are key to solving the problems addressed by the present disclosure. Further, in order to disclose the novelties of the present disclosure, the above described embodiments do not disclose about those modules or blocks not too related to solving the problems addressed by the present disclosure, which does not mean that the above described embodiments cannot include other modules or blocks.

[0077] It is also necessary to point out that, in the claims and specification of the present disclosure, terms such as first and second only are for distinguishing an embodiment or an operation from another embodiment or operation. It does not require or imply that those embodiments or operations having any such real relationship or order. Further, as used herein, the terms “comprising,” “including,” or any other variation intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Absent further limitation, elements recited by the phrase “comprising

a” does not exclude a process, method, article, or apparatus that comprises such elements from including other same elements.

[0078] While the foregoing disclosure sets forth various embodiments using specific block diagrams, flowcharts, and examples, each block diagram component, flowchart step, operation, and/or component described and/or illustrated herein may be implemented, individually and/or collectively, using a wide range of hardware, software, or firmware (or any combination thereof) configurations. In addition, any disclosure of components contained within other components should be considered as examples because many other architectures can be implemented to achieve the same functionality.

[0079] The process parameters and sequence of steps described and/or illustrated herein are given by way of example only and can be varied as desired. For example, while the steps illustrated and/or described herein may be shown or discussed in a particular order, these steps do not necessarily need to be performed in the order illustrated or discussed. The various example methods described and/or illustrated herein may also omit one or more of the steps described or illustrated herein or include additional steps in addition to those disclosed.

[0080] While various embodiments have been described and/or illustrated herein in the context of fully functional computing systems, one or more of these example embodiments may be distributed as a program product in a variety of forms, regardless of the particular type of computer-readable medium used to actually carry out the distribution. The embodiments disclosed herein may also be implemented using software modules that perform certain tasks. These software modules may include script, batch, or other executable files that may be stored on a computer-readable storage media or in a computing system. These software modules may configure a computing system to perform one or more of the example embodiments disclosed herein. One or more of the software modules disclosed herein may be implemented in a cloud computing environment. Cloud computing environments may provide various services and applications via the Internet. These cloud-based services (e.g., software as a service, platform as a service, infrastructure as a service, etc.) may be accessible through a Web browser or other remote interface. Various functions described herein may be provided through a remote desktop environment or any other cloud-based computing environment.

[0081] Although the present disclosure and its advantages have been described in detail, it should be understood that various changes substitutions, and alterations can be made herein without departing from the spirit and scope of the disclosure as defined by the appended claims. Many

modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the disclosure and its practical applications, to thereby enable others skilled in the art to best utilize the disclosure and various embodiments with various modifications as may be suited to the particular use contemplated.

[0082] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present disclosure, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present disclosure. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

[0083] Embodiments according to the present disclosure are thus described. While the present disclosure has been described in particular embodiments, it should be appreciated that the disclosure should not be construed as limited by such embodiments, but rather construed according to the below claims.

WHAT IS CLAIMED IS:

1. A method of separating a read operation from a write operation, the method comprising the steps of:

obtaining and storing a client ID, by a database server, after establishing a slave database connection with a slave database corresponding to a client;

receiving an operation request by the database server from the client;

if the operation request is a write request, the database server establishing a master database connection with a master database by use of a public ID and a public passcode and sending the client ID to the master database, wherein upon receiving the client ID, the master database updates the public ID with the received client ID, and updates access permissions associated with the public ID with access permissions associated with the client ID; and

sending, by the database server, the write request to the master database by use of the master database connection, wherein the master database executes a write operation corresponding to the write request and to the access permissions associated with the client ID.

2. The method of claim 1, wherein the step of obtaining and storing a client ID comprises the steps of:

receiving by the database server a slave database connection request from the client, wherein the connection request includes a client ID and a client passcode;

sending, by the database server, the connection request to the slave database corresponding to the client, wherein upon receiving the connection request, the slave database obtains the client ID and the client passcode from the connection request, verifies the client by use of the obtained client ID and client passcode, and if the client is successfully verified, establishes the slave database connection with the database server; and

obtaining and storing, by the database server, the client ID from the connection request.

- 25 3. The method of claim 1, after the step of receiving an operation request from the client, further comprising the step of:
- if the operation request is a read request, the database server sending the read request through the slave database connection to the slave database corresponding to the client, wherein a read operation corresponding to the read request is executed against the slave database.
- 30 4. The method of claim 1, wherein the step of the database server establishing a master database connection with a master database by use of a public ID and a public passcode comprises the step of:
- sending, by the database server, the public ID and the public passcode to the master database, wherein upon receiving the public ID and the public passcode, the master database
- 35 verifies the database server by use of the received public ID and public passcode, and if the database server is successfully verified, establishes the master database connection with the database server.
5. The method of claim 1, after the step of the database server establishing a master database connection with a master database by use of a public ID and a public passcode, further
- 40 comprising the step of caching by the database server the master database connection with the master database.
6. A database server comprising a processor and a non-transitory machine readable medium storing instructions, which when executed causes the processor to perform operations, the operations comprising:
- 45 an obtaining module configured for obtaining and storing a client ID after establishing a slave database connection with a slave database corresponding to a client;
- a receiving module configured for receiving an operation request from the client;
- an establishment module configured for, if the operation request is a write request, establishing a master database connection with a master database by use of a public ID and a
- 50 public passcode and sending the client ID to the master database, wherein upon receiving the client ID, the master database updates the public ID with the received client ID, and updates

access permissions associated with the public ID with access permissions associated with the client ID; and

55 a writing module configured for sending the write request to the master database by use of the master database connection, wherein the master database executes a write operation corresponding to the write request and to the access permissions associated with the client ID.

7. The database server of claim 6, wherein the obtaining module comprises:

a receiving module configured for receiving a slave database connection request from the client, wherein the connection request includes a client ID and a client passcode;

60 a sending module configured for sending the connection request to a slave database corresponding to the client, wherein upon receiving the connection request, the slave database obtains the client ID and the client passcode from the connection request, verifies the client by use of the obtained client ID and client passcode, and if the client is successfully verified, establishes the slave database connection with the database server; and

65 a storing module configured for obtaining and storing the client ID from the connection request.

8. The database server of claim 6, wherein the operations further comprise:

70 a read module configured for, if the operation request is a read request, sending the read request through the slave database connection to the slave database corresponding to the client, wherein a read operation corresponding to the read request is executed against the slave database.

9. The database server of claim 6, wherein the establishment module comprises:

75 a setup module configured for sending the public ID and the public passcode to the master database, wherein, upon receiving the public ID and the public passcode, the master database verifies the database server by use of the received public ID and public passcode, and if the database server is successfully verified, establishes the master database connection with the database server.

10. The database server of claim 6, wherein the operations further comprise a cache module
80 configured for, after establishing the master database connection with the master database by use
of the public ID and the public passcode, caching the master database connection with the master
database.

11. A system for separating a read operation from a write operation, the system comprising a
database server and a master database, wherein the database server comprises:

85 a processor; and

a non-transitory computer-readable medium operably coupled to the processor, the non-
transitory computer-readable medium having computer-readable instructions stored thereon to be
executed when accessed by the processor, the instructions comprising:

an obtaining module configured for obtaining and storing a client ID after

90 establishing a slave database connection with a slave database corresponding to a client;

a receiving module configured for receiving an operation request the client; and

an establishment module configured for, if the operation request is a write request,
establishing a master database connection with the master database by use of a public ID
and a public passcode and sending the client ID to the master database; and

95 a write module configured for, after the master database updates access
permissions associated with the public ID with access permissions associated with the
client ID, sending the write request to the master database by use of the master database
connection, wherein the master database executes a write operation corresponding to the
write request and to the access permissions associated with the client ID.

100 12. The system of claim 11, wherein the master database comprises:

a processor; and

a non-transitory computer-readable medium operably coupled to the processor, the non-
transitory computer-readable medium having computer-readable instructions stored thereon to be
105 executed when accessed by the processor, the instructions comprising:

an update module configured for receiving the client ID and updating the public ID with the received client ID, and for updating the access permissions associated with the public ID with the access permissions associated with the client ID.

13. The system of claim 12, wherein the obtaining module comprises:

110 a receiving module configured for receiving a slave database connection request from the client, wherein the connection request includes a client ID and a client passcode;

a sending module configured for sending the connection request to a slave database corresponding to the client; and

115 a storing module configured for, after the slave database connection is established with the slave database, obtaining and storing the client ID from the connection request.

14. The system of claim 13 further comprising a slave database, the slave database comprising a first verification module configured for receiving the slave database connection request, obtaining the client ID and the client passcode from the connection request, and verifying the client with the obtained client ID and client passcode, wherein, if the client is
120 verified successfully, the slave database connection is established with the database server.

15. The system of claim 12, wherein the database server further comprises a read module configured for, if the operation request is a read request, sending the read request through the slave database connection to the slave database corresponding to the client, wherein a read operation corresponding to the read request is executed against the slave database.

125 16. The system of claim 12, wherein the establishment module comprises a setup module configured for sending the public ID and the public passcode to the master database, and wherein the master database further comprises a second verification module configured for receiving the public ID and the public passcode, verifying the database server by use of the received public ID and public passcode, and if the database server is successfully verified, establishing the master
130 database connection with the database server.

17. The system of claim 12 further comprising a cache module configured for, after establishing the master database connection with the master database by use of the public ID and the public passcode, caching the master database connection with the master database.

1/9

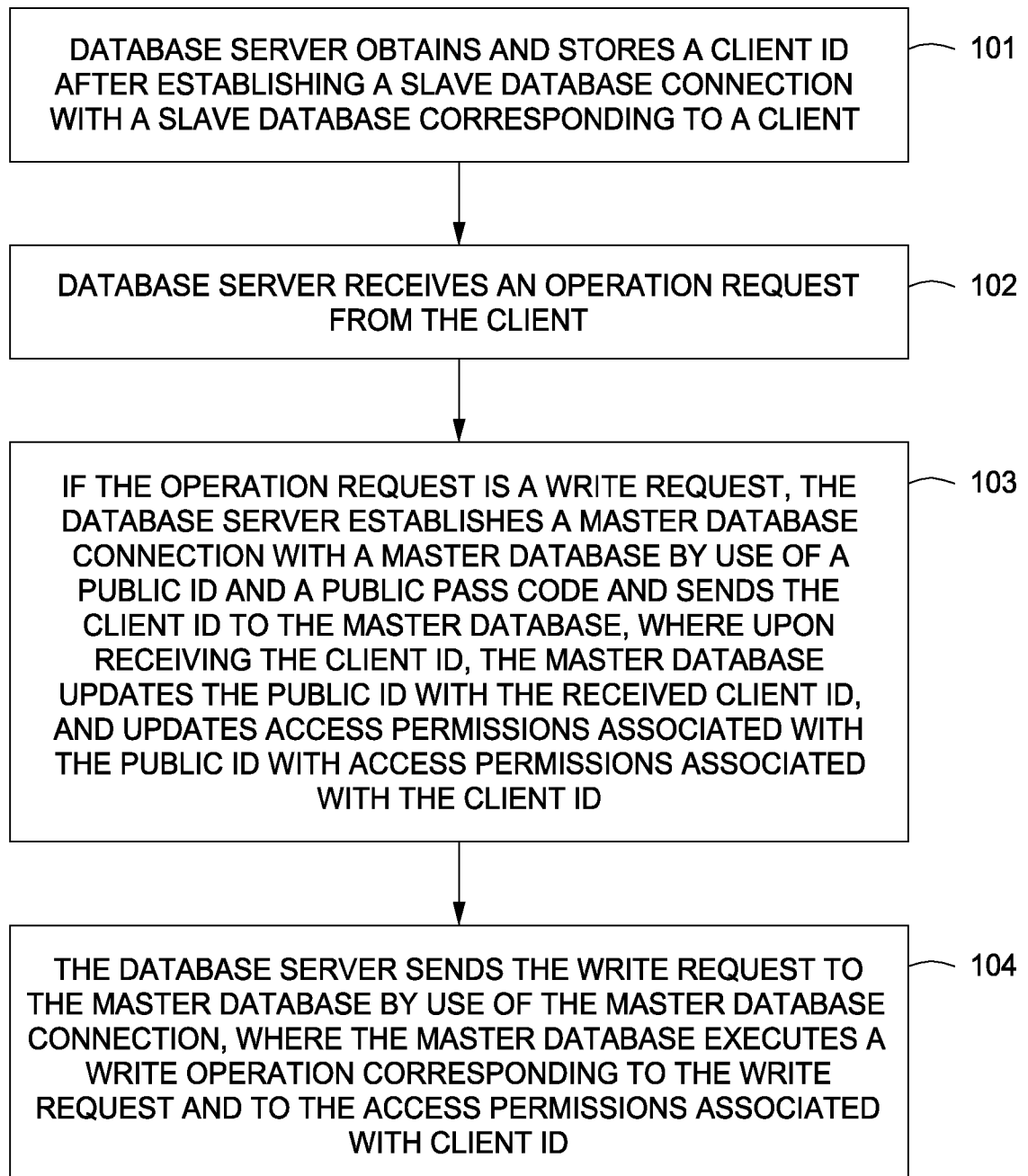
100

FIG. 1

2/9

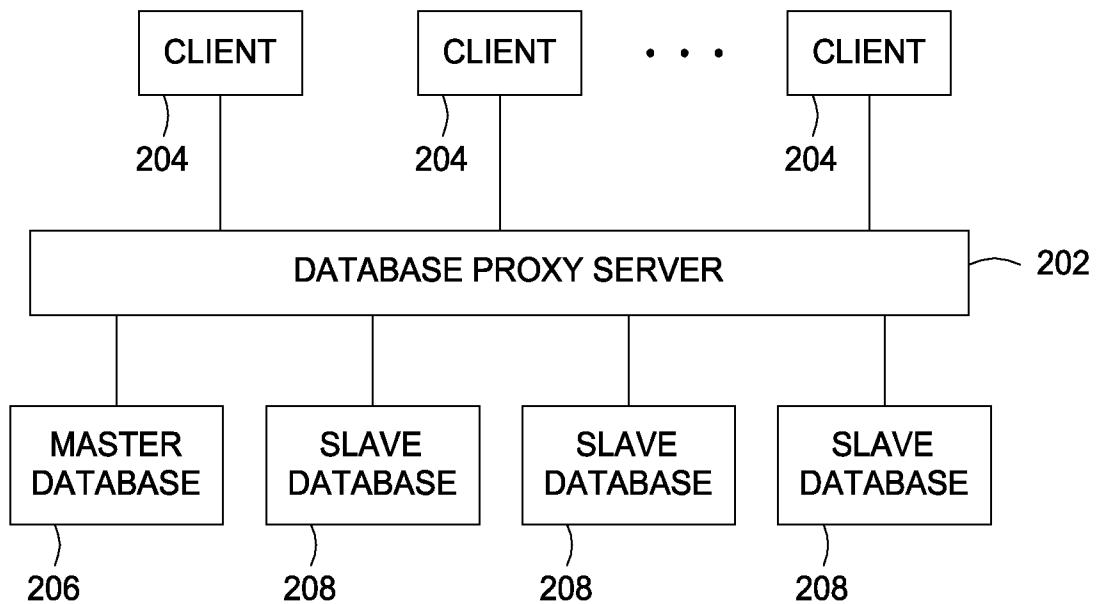


FIG. 2

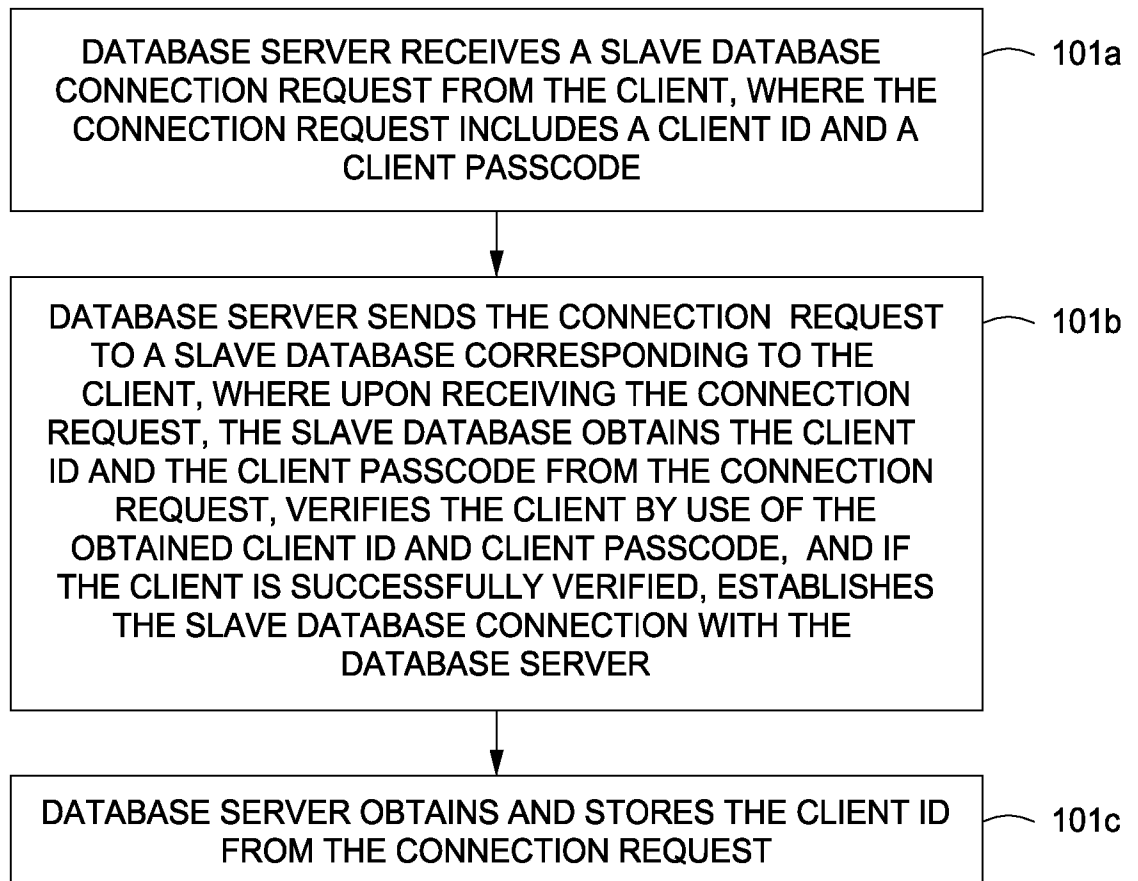
300

FIG. 3

3/9

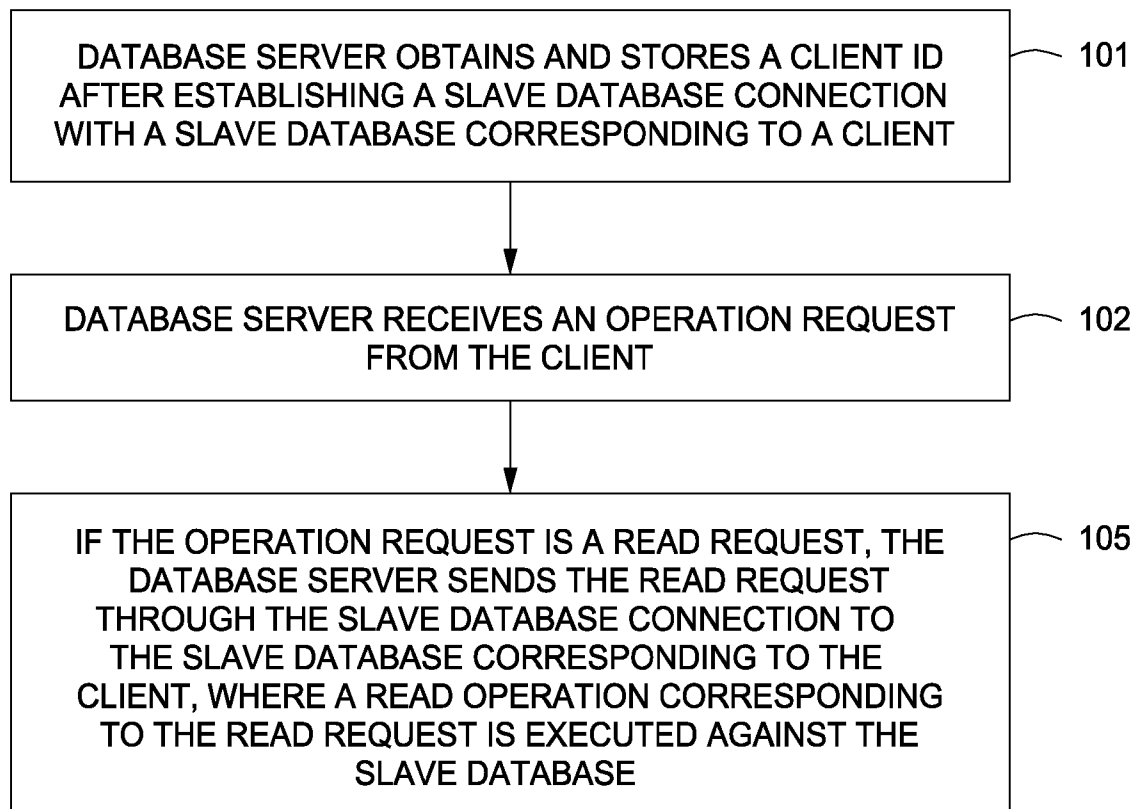
400

FIG. 4

4/9

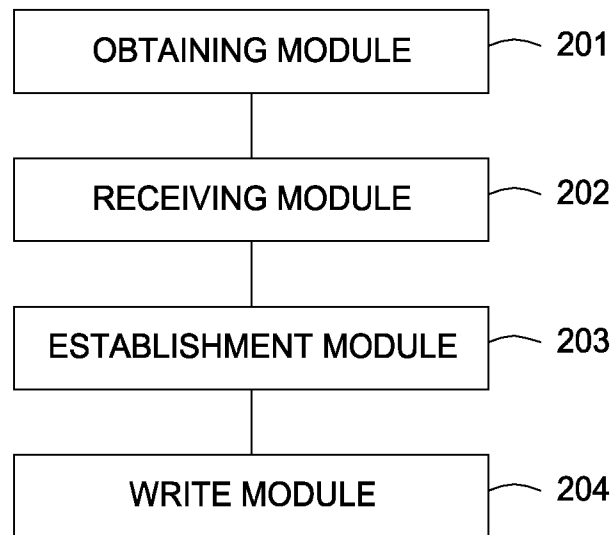
500

FIG. 5

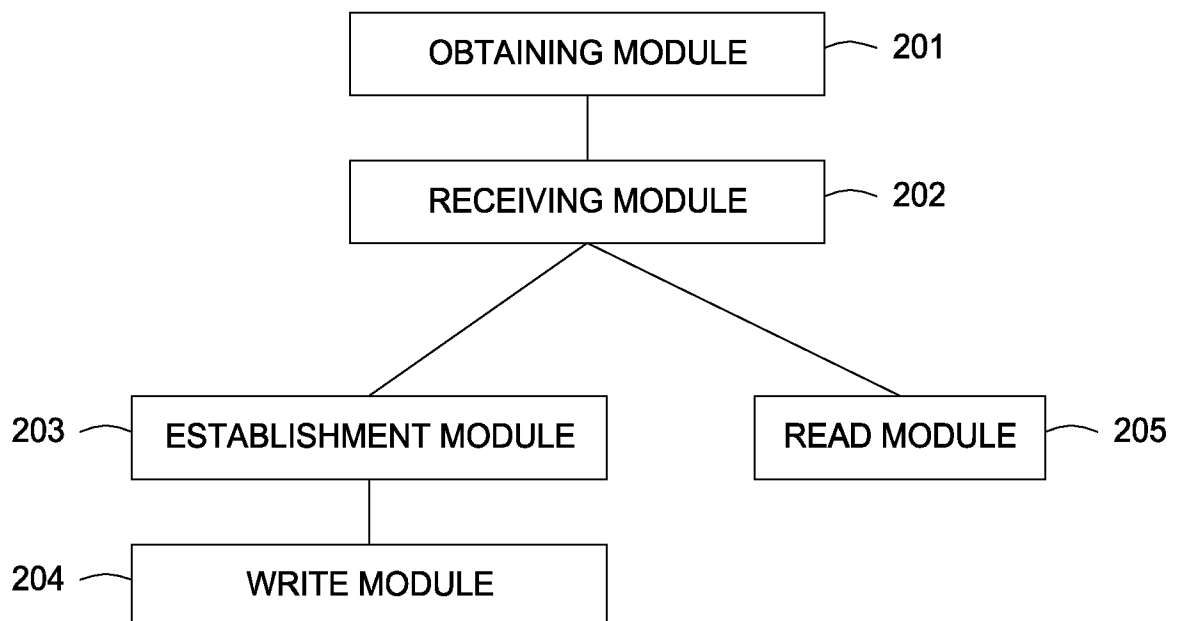
600

FIG. 6

5/9

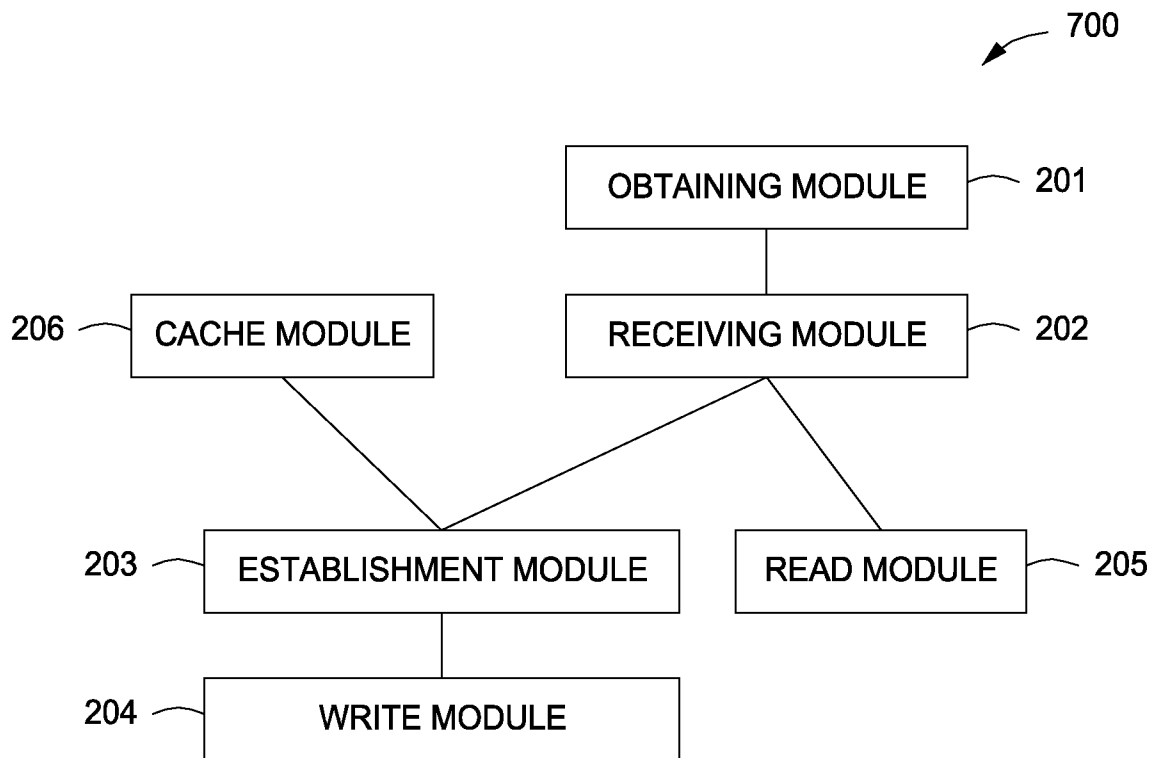


FIG. 7

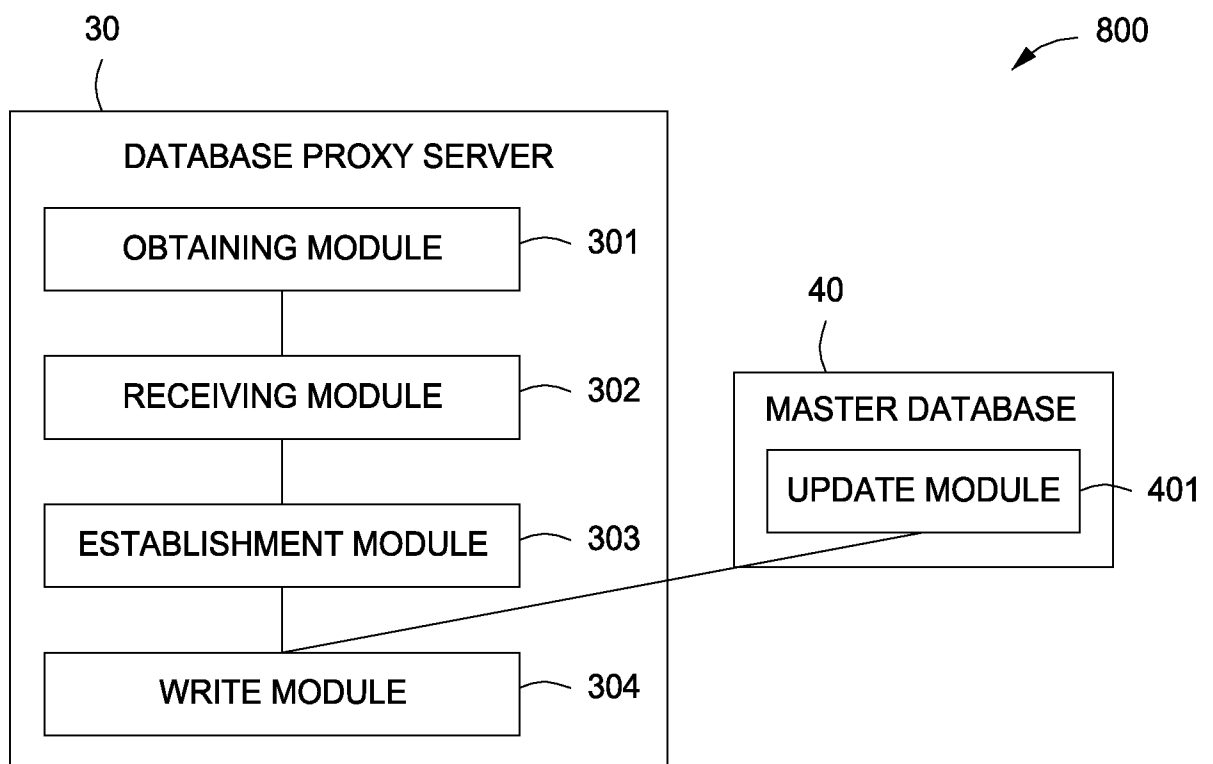


FIG. 8

6/9

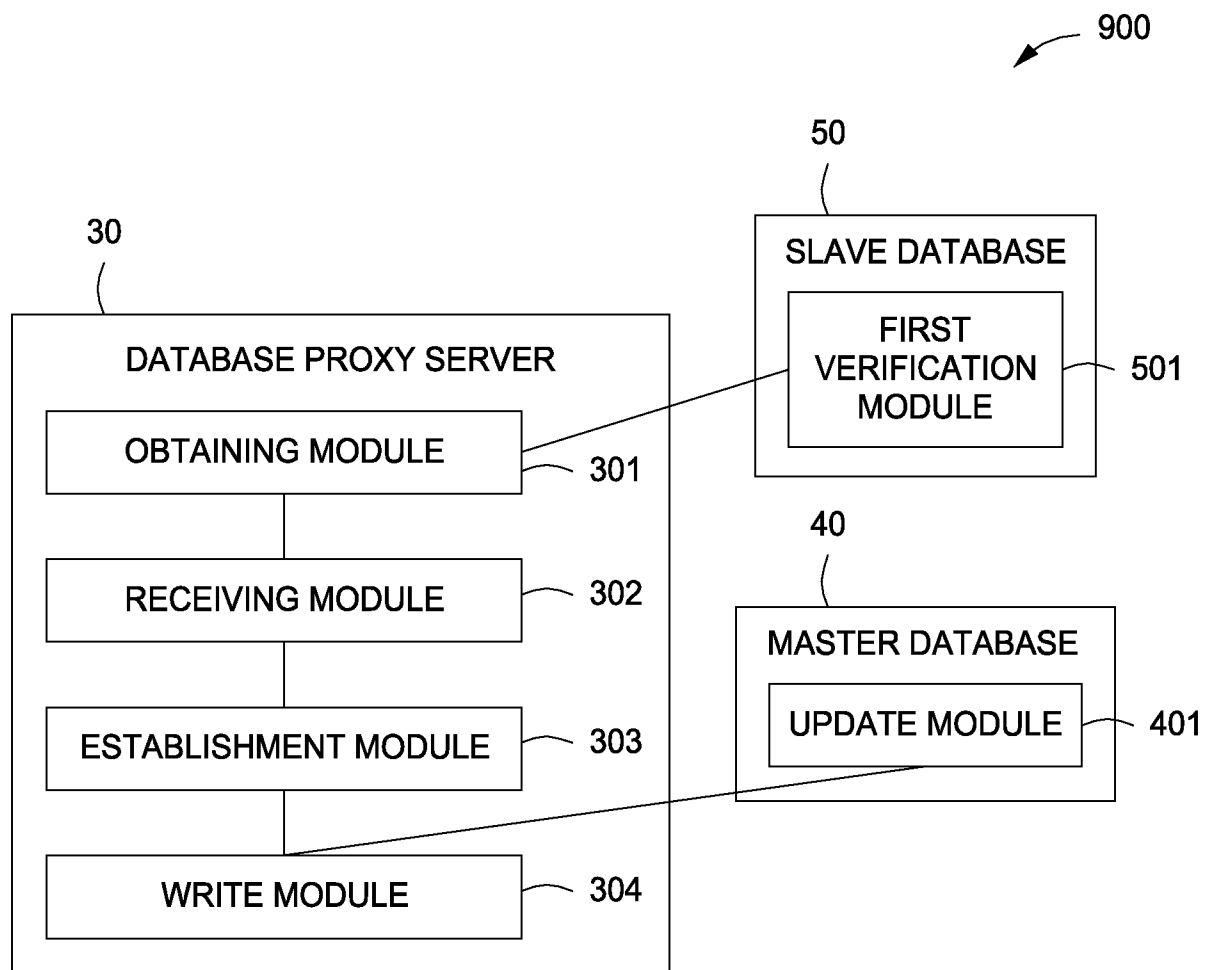


FIG. 9

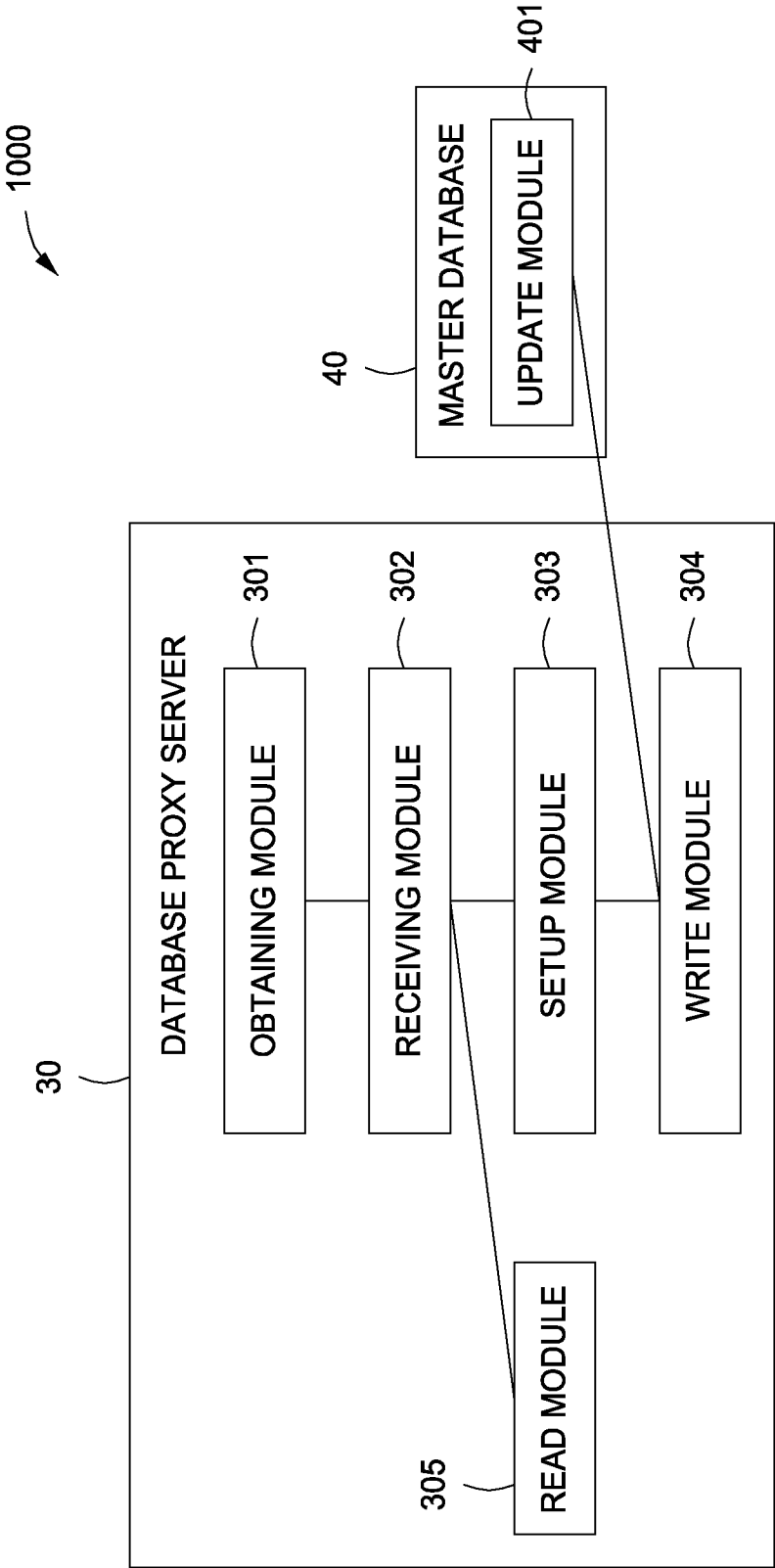


FIG. 10

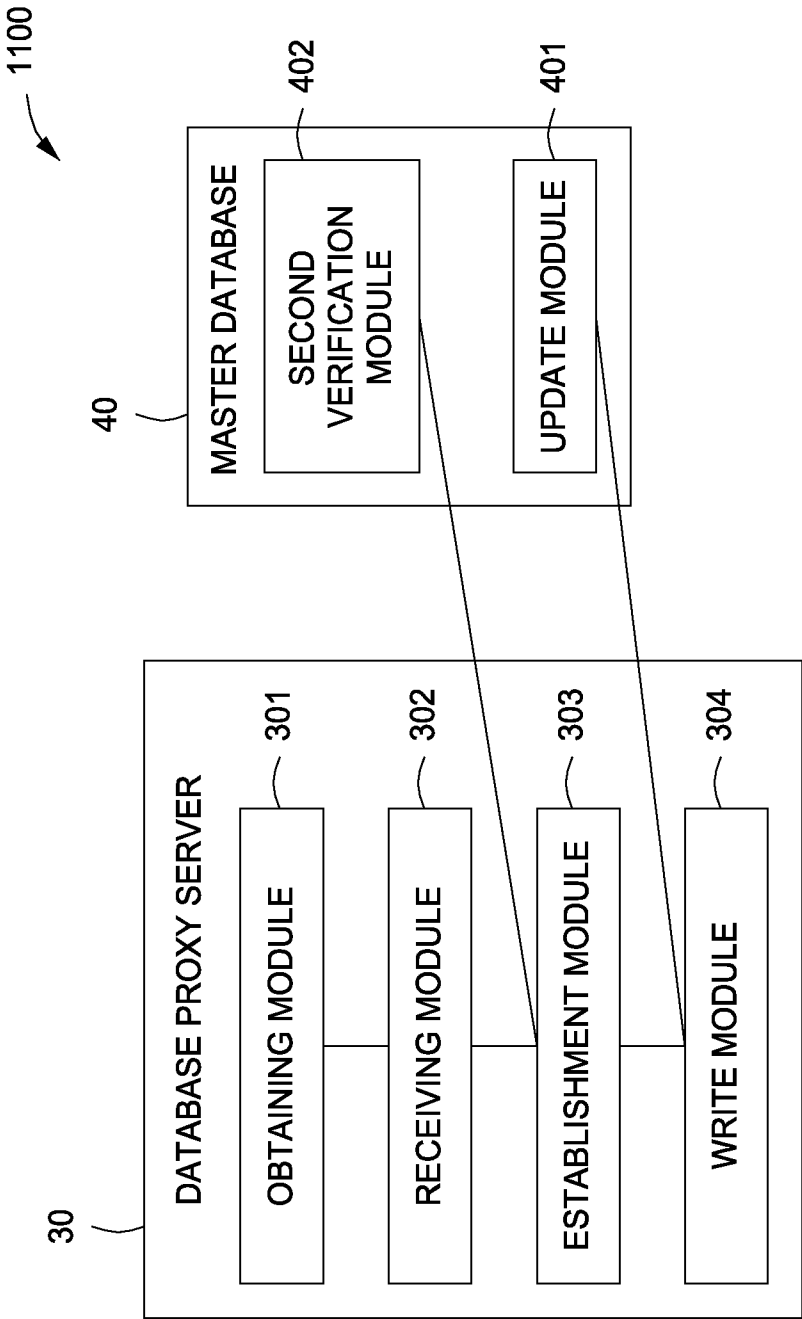


FIG. 11

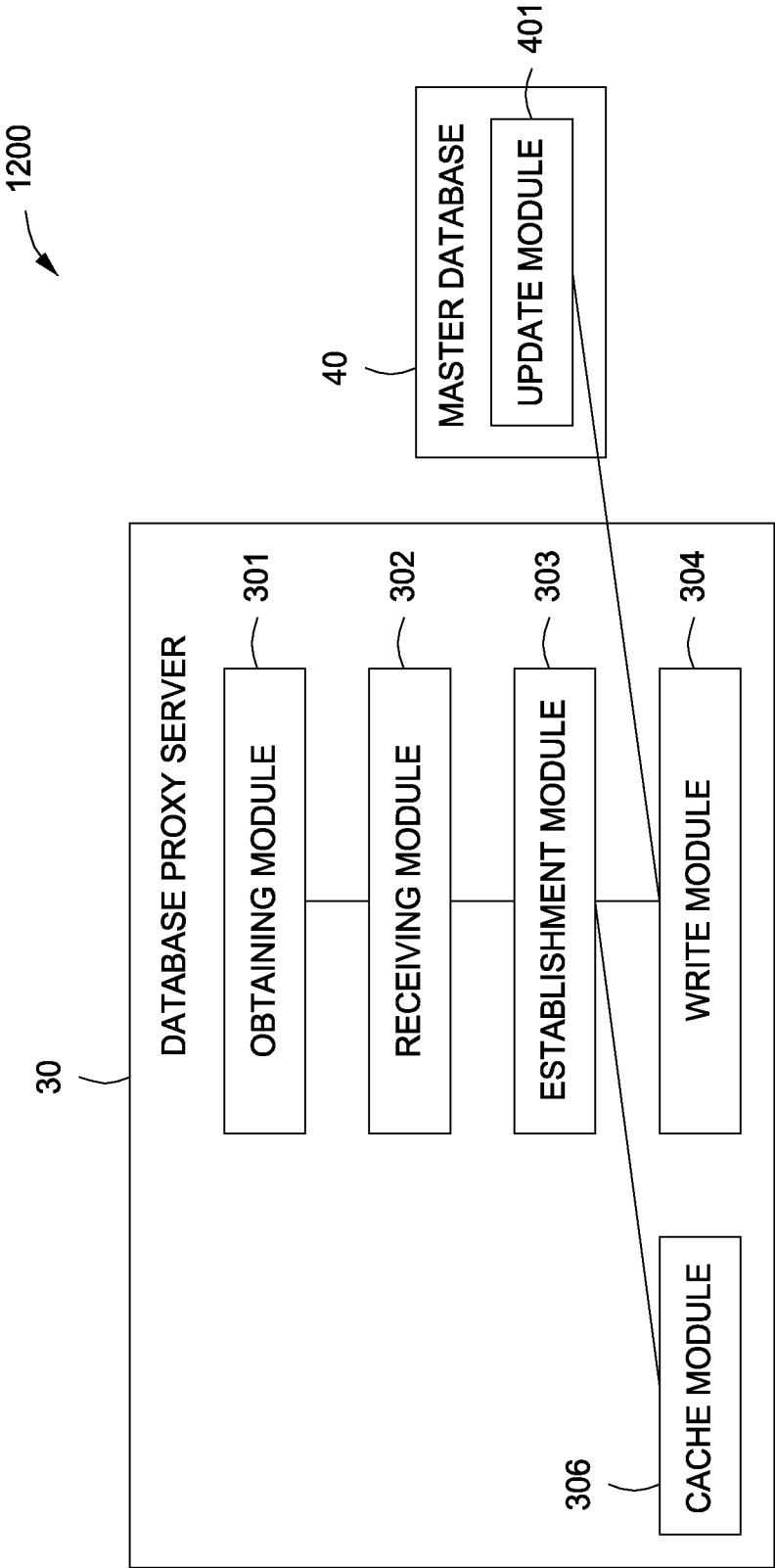


FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US16/16461

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 17/30; G06F 21/30; G06F 12/14 (2016.01)

CPC - G06F 17/30286, 17/30557, 17/30575

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)

IPC(8): G06F 17/30; G06F 21/30; G06F 12/14 (2016.01)

CPC: G06F 17/30286, 17/30557, 17/30575; H04L 63/083

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)

PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, Other Countries (INPADOC), RU, AT, CH, TH, BR, PH); Google Scholar, EBSCO, IEEE/IEEEExplore; Keywords: database master slave read write request client private public key ID identification access permission load balancing separation proxy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,523,032 B1 (SUNKARA, R et al.) 18 February 2003. Abstract; column 4, lines 24-34; column 4, lines 54-67; claims 1, 14.	1-17
A	US 6,240,512 B1 (FANG, Y et al.) 29 May 2001. Abstract; column 2, lines 51-54; column 10, lines 33-50; claim 16.	1-17
A	CN102129434A (MA, X) 20 July 2011. Abstract; paragraph [0036].	1-17
A	US 2004/0054779 A1 (TAKESHIMA, Y et al.) 18 March 2004. Entire Document.	1-17
A	US 2008/0295146 A1 (SRIRAM, T) 27 November 2008. Entire Document.	1-17
A	US 2012/0311003 A1 (KUZNETSOV, V et al.) 06 December 2012. Entire Document.	1-17

☐ 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

31 March 2016 (31.03.2016)

Date of mailing of the international search report

06 MAY 2016

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Shane Thomas

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774