US 20070179956A1

(19) **United States**

(12) **Patent Application Publication**

Whitmyer, JR.

(10) **Pub. No.: US 2007/0179956 A1**

(43) **Pub. Date: Aug. 2, 2007**

(54) **RECORD PROTECTION SYSTEM FOR NETWORKED DATABASES**

(76) Inventor: **Wesley W. Whitmyer JR.**, Stamford, CT (US)

Correspondence Address:
ST. ONGE STEWARD JOHNSTON & REENS, LLC
986 BEDFORD STREET
STAMFORD, CT 06905-5619 (US)

(21) Appl. No.: **11/334,246**

(22) Filed: **Jan. 18, 2006**

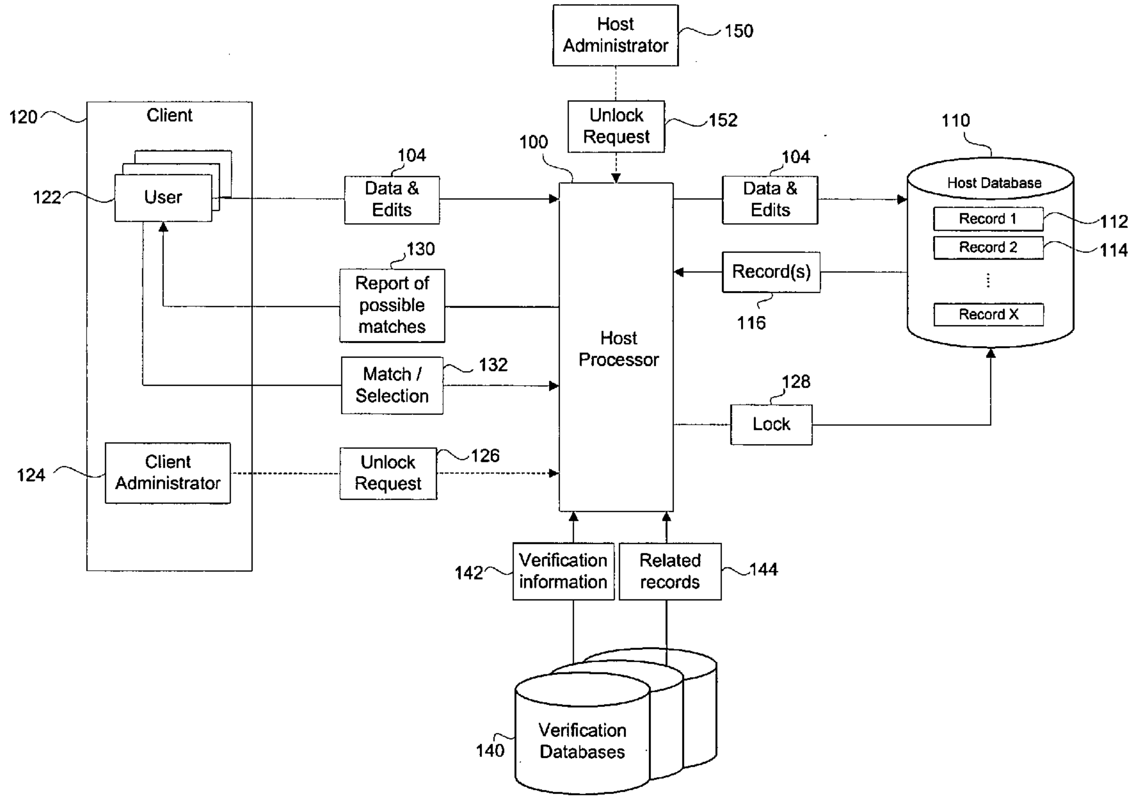
Publication Classification

(51) **Int. Cl.**
G06F 17/30 (2006.01)

(52) **U.S. Cl.** **707/10**

(57) **ABSTRACT**

A record protection system for a networked database is provided. The system includes a client, a host processor accessible by the client via a telecommunications network, a database accessible by the host processor and containing at least one data record, software executing on the host processor for receiving data from the client for one or more fields of the data record, software executing on the processor for receiving data from a source, software executing on the host processor for comparing the data received from the client to the data received from the source, and software executing on the host processor to prevent editing of the data record by the client if the at least a portion of the data received from the client matches the data received from the source.



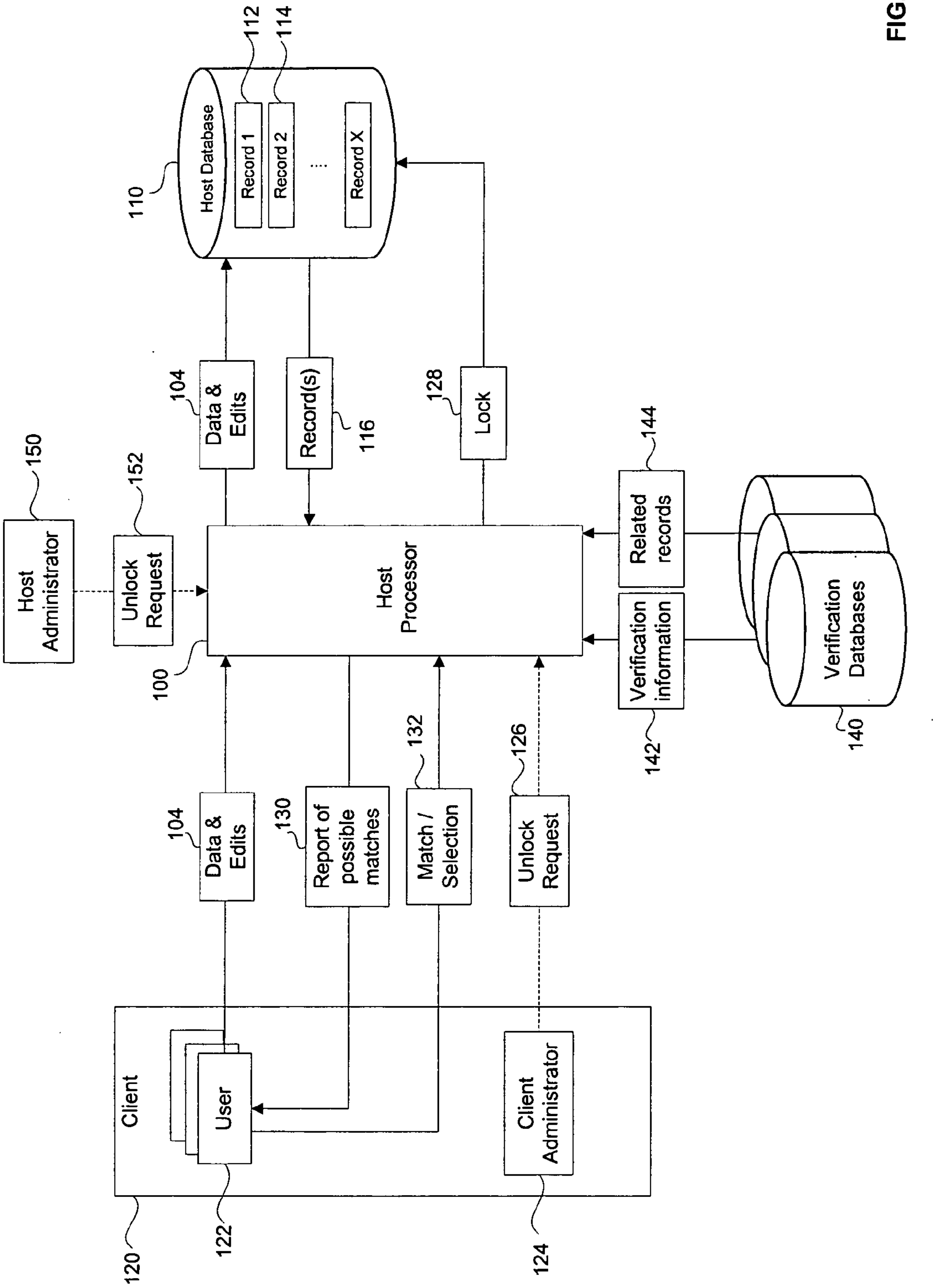

Host Database
Record 1
Record 2
....
Record X
110
112
114
Host Administrator
150
Unlock Request
152
Data & Edits
104
Record(s)
116
Lock
128
Related records
144
Host Processor
100
Verification information
142
Verification Databases
140
Data & Edits
104
Report of possible matches
130
Match / Selection
132
Unlock Request
126
Client
User
Client Administrator
120
122
124

FIG. 1

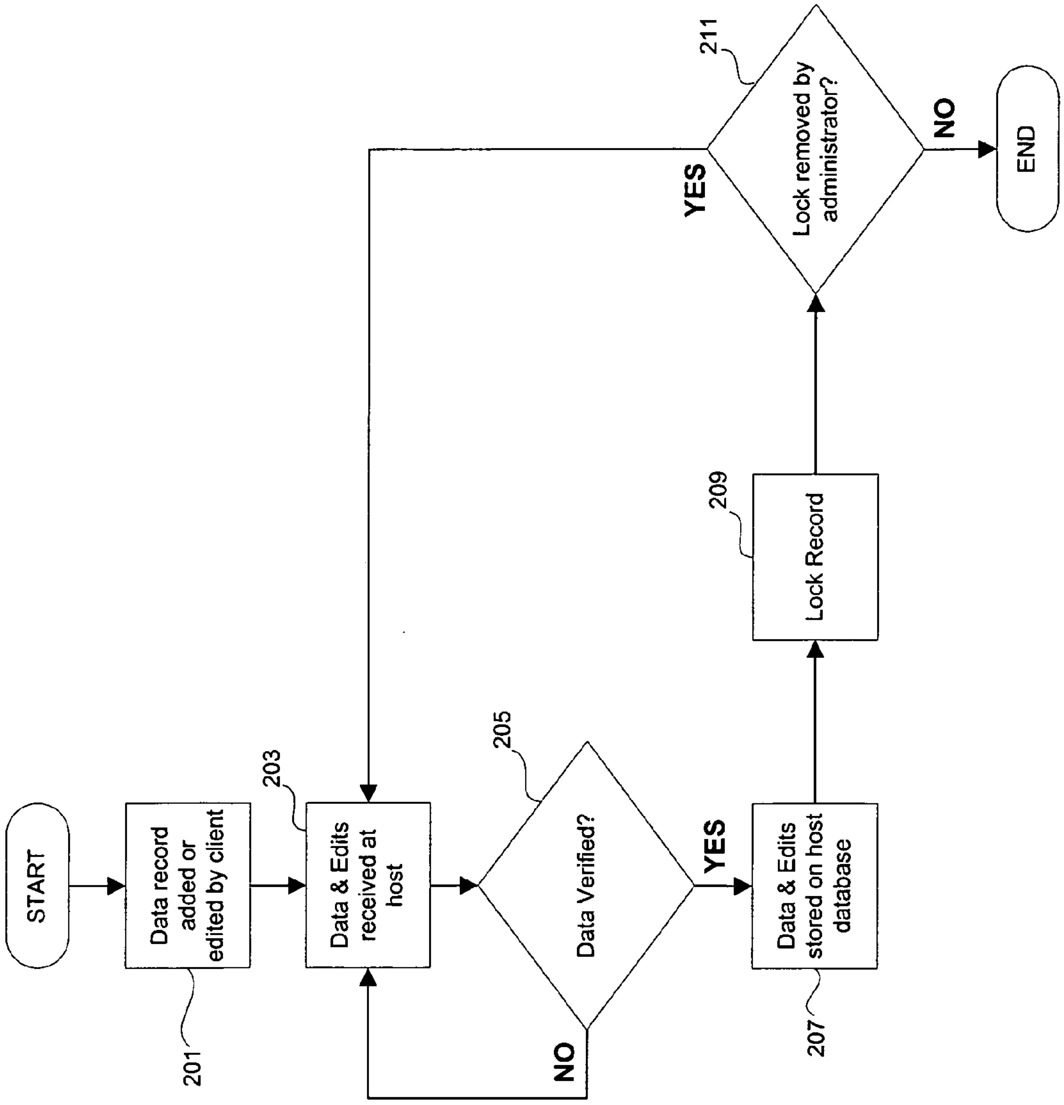

START
201
Data record added or edited by client
203
Data & Edits received at host
205
Data Verified?
NO
YES
207
Data & Edits stored on host database
209
Lock Record
211
Lock removed by administrator?
YES
NO
END

FIG. 2

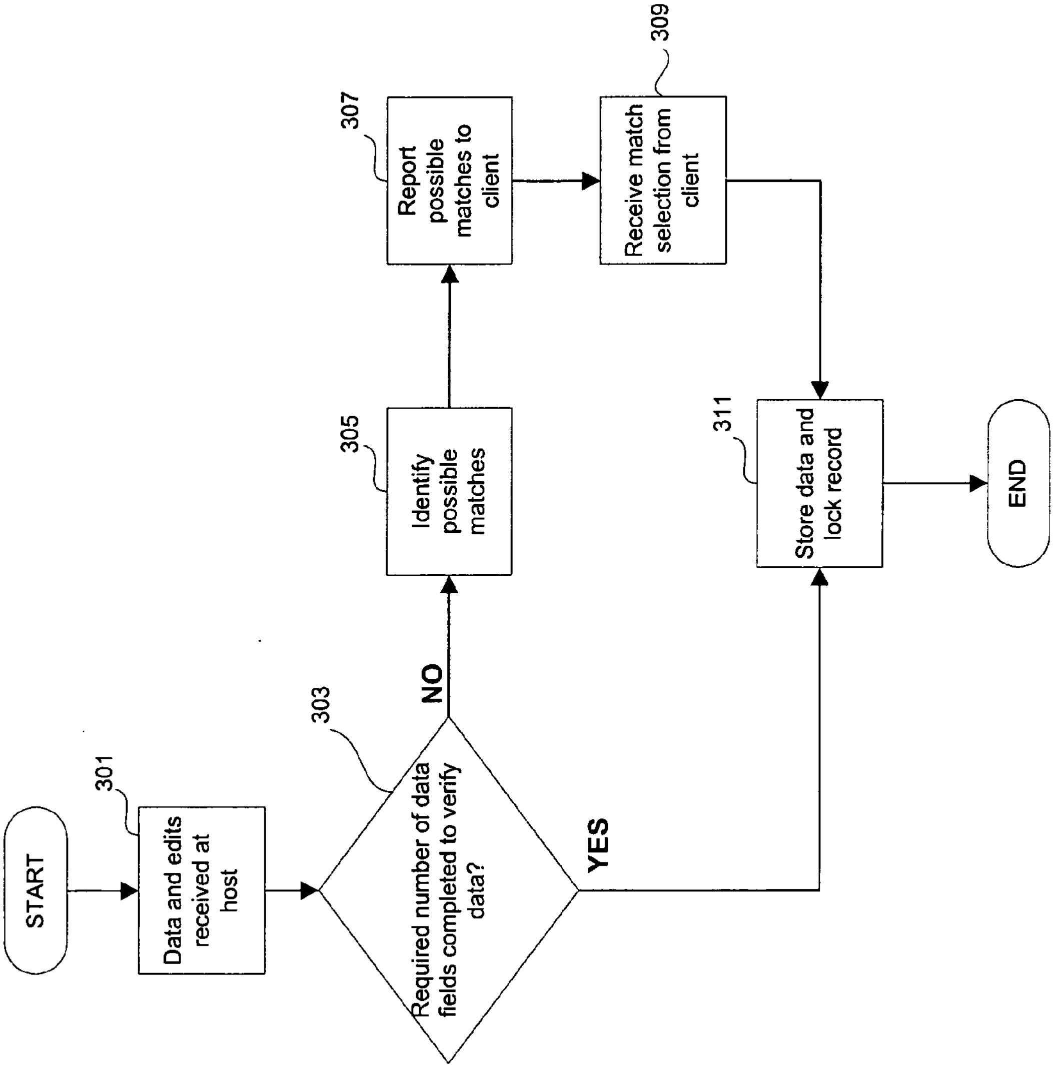

START
Data and edits received at host
301
Required number of data fields completed to verify data?
303
NO
YES
Identify possible matches
305
Report possible matches to client
307
Receive match selection from client
309
Store data and lock record
311
END

FIG. 3

RECORD PROTECTION SYSTEM FOR NETWORKED DATABASES

FIELD OF THE INVENTION

[0001] The invention relates to network-based data processing and storage, and more particularly to a system and method for protecting data records in Internet-based databases.

BACKGROUND OF THE INVENTION

[0002] Internet-based application service providers, so-called "ASPs" are known and provide the advantage that hardware and software maintenance and upgrades are centrally managed by a third party. The ASP model has been further extended to include web-hosted databases. For example, an ASP may provide a client with a backup database for duplicate storage of client data records. Further, an ASP or any other host may maintain a client's active database, and/or sensitive data therein, and allow the client to remotely store and edit data records to the database via the Internet. Thus, a client/user may log in to his web-hosted database via a web browser on his LAN/computer and create or manipulate data records in real time.

[0003] However, one difficulty faced when one or more users of a particular client are accessing a web-hosted database is preventing errors in the creation of new data records and in edits to existing data records. The problem is further complicated when the completion of a particular field of a data record triggers the storage and/or edit of related data in the data record. For example, a user may have automatic permissions to enter and edit data in the web-hosted database. Upon completing a particular field of a data record, additional fields of the data record may be automatically populated based on the entered data. There is then a risk that the user or another user having edit permissions may accidentally or erroneously edit the particular field and/or the automatically generated data.

[0004] What is desired, therefore, is a system and method for locking data records in networked or web-hosted databases. Further desired is a system and method for locking a data record upon the occurrence of specified trigger.

SUMMARY OF THE INVENTION

[0005] According, it is an object of the present invention to provide a system and method for automatically locking a data record in a networked database upon the completion of a verification step.

[0006] It is a further object of the present invention to provide the system and method wherein the lock may be reversed or modified by a host or client administrator.

[0007] These and other objectives are achieved by providing a record protection system for a networked database, including a client, a host processor accessible by said client via the Internet, a database accessible by said host processor and containing at least one data record, software executing on said host processor for receiving data from said client for one or more fields of the data record, software executing on said processor for receiving data from a source, software executing on said host processor for comparing the data received from said client to the data received from the source, and software executing on said host processor to prevent editing of the data record by said client if at least a portion of the data received from said client matches the data received from the source.

[0008] Further provided is a method for protecting data records in a networked database, including the steps of receiving data from a client via a telecommunications network for one or more fields of a data record, determining whether at least a portion of the data matches data received from a source, storing matched data in the data record, and locking the data record to prevent future editing by the client.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. **1** is a schematic diagram of a record protection system for a networked database according to the present invention.

[0010] FIG. **2** is a method of protecting data records in a networked database employable by the system shown in FIG. **1**.

[0011] FIG. **3** is a method of protecting data records in a networked database employable by the system shown in FIG. **1**.

DETAILED DESCRIPTION OF THE DRAWINGS

[0012] FIG. **1** shows a schematic diagram of a record protection system according the present invention. The system includes a host processor **100**. The host processor **100** may be any processor, controller or server for executing one or more software applications. The host processor **100** may be in communication with any number of databases, such as the database **110**. The database **110** includes a plurality of data records, e.g., data record **112** and data record **114**.

[0013] The host processor **100** further includes software for receiving data and edits **104** for storage in the database **110**. The data **104** may be received from a client **120**, or any number of users **122** associated with the client **120**, via a communications network (not shown). The communications network may be any network, such as the Internet or an Intranet. In a preferred embodiment, a user **122** remotely accesses the database **110** via a web interface on a client computer.

[0014] As shown, the host processor **100** receives data **104** from the client **120** and/or any user **122**. The data **104** may be data for initiating the creation of a new data record or proposed edits to an existing data record (e.g., **112**). In one embodiment, the host (i.e., host processor **100** and host database **110**) may be a provider of a service for maintaining U.S. patents (e.g., paying patent maintenance fees) for any number of clients **120**. Therefore, the host processor **100** may receive data related to new patents for which maintenance is desired (e.g., identified by verification information **142** or data records in a verification database **140**) or updates and/or edits to an existing patent data record stored in the host database **110**. As one of ordinary skill in the art will understand, the host has an interest in the client **120** being able to input its own data to save the time and labor required to populate the database **110**. However, the host must ensure that the correct patent is identified and further that no user **122** of the client **120** erroneously enters data identifying an incorrect patent. Failure to ensure the accuracy of entered data may lead to the host failing to pay a maintenance fee or paying a maintenance fee on the wrong patent.

[0015] The system further includes any number of verification databases **140** (e.g., or sources). The verification databases **140** may include verification information **142** and/or data records to verify the data and edits **104** provided by the client **120**. In some embodiments, the verification databases **140** include information related to any number of potential data records to be created in the host database **110**. For example, if the database **110** includes data records of patents owned by one or more clients, one of the verification databases **140** may include information related to substantially all U.S. and/or foreign patents and patent applications. For example, the verification databases **140** may include the United States Patent and Trademark database, the European Patent Office database, etc. Therefore, when a client **120** attempts to create a new data record regarding a patent, the host processor **100** may query the verification databases **140** and attempt to verify and/or match at least a portion of the received data and edits **104** with verification information **142** retrieved from the verification databases **140** prior to creating or storing the new data record.

[0016] Upon receipt of data and edits **104**, the host processor **100** may initiate the creation of a new data record in the host database **110**. The host processor **100** may then query the verification databases **140** (discussed below) to determine possible matches to the received data **104**. For example, in the practice of maintaining of patent data records, the client **120** may provide a patent number, a filing date, and/or issue data of a U.S. patent. The host processor **100** may then identify one or more data records (e.g., relating to patents) in the verification databases **140** corresponding to this received data. In some embodiments, the host processor **100** may also identify and/or access any number of existing data records **116** in the host database **110** identified by the data and edits **104**. For example, if a client **120** enters data corresponding to an existing data record, the system may prompt the client **120** (e.g., via a web interface) to determine whether the client **120** is either attempting to edit the existing data record **116** or erroneously attempting to create a duplicate data record.

[0017] As shown in FIG. **1**, the system includes a software means **128** for locking one or more data records. For example, the host processor **100** may lock a particular data record to prevent any further edits to the data record, e.g., following a verification step or matching of data. In some embodiments, the verification step or verification may require that a user **122** first complete a particular field and/or a set number of fields of data. For example, the user **122** may complete data fields for a particular data record via the web interface. The host processor **100** may require at least three separate identifying pieces of data to be entered prior to updating or creating the data record. Once each of the particular number of required data fields are verified and/or matched to a single data record and/or set of verification information **142** in the verification databases **140**, the data is stored in the host database **110** and the corresponding data record(s) locked. In some embodiments, the system may allow the user **122** to continue to complete any number of data fields until at least a predetermined number of the data fields match or identify the same verification information **142**. The predetermined amount may be based on a data sensitivity factor, a fixed number of data fields, and/or a host or client preference.

[0018] In some embodiments, data entered by a user **122** via a web interface may be stored in temporary storage of the system prior to the data is being verified. For example, a user **122** may enter data and edits **104** with the appearance of the data being stored or added to a particular data record (e.g., **112**). However, the system may store the data (and lock the record) only after the entered data is verified.

[0019] In a preferred embodiment, a locked data record may only be edited if unlocked by an administrator, e.g., via the transmission of an unlock request **126**/**152**. The administrator may be a client administrator **124** or host administrator **150**, shown in FIG. **1**. If a data record is unlocked, additional data and edits may be received. Otherwise, the data record may remain locked.

[0020] If the data and edits **104** provided by the user **122** are identifiable to more than one set of verification information **142** or existing data record, the host processor **100** may provide the client **120** (or user **122**) with a report of possible matches **130** (e.g., prompt, display, email, etc). For example, the user **122** may enter a correct patent filing date but an incorrect patent number. Based on the data entered and stored client data/preferences, the system may query any number of databases (e.g., verification databases **140** and/or host database **110**) to determine potential sets of verification information **142** (e.g., patents) or existing data records to which the user **122** is referring. For example, knowing the filing date and assignee (e.g., the client), the host processor **100** may be able to determine one or two potential patents filed on that day matching some of the entered data. The host processor **100** may then prompt the user **122** via the web interface to select the intended information or record from a list of possible matches. Upon the user **122**'s selection **132**, the data record may be locked.

[0021] The verification databases **140** shown in FIG. **1** may further include information to supplement the data and edits **104** of a newly created or existing data record. Upon a user **122** providing a minimum amount of data to verify the data and identify a particular U.S. (or foreign) patent, the host processor **100** may query the verification databases **140** and retrieve the remaining data necessary to create the new data record and/or related records **144** to supplement the data **104** provided by the user **122**. For example, should the user **122** provide a patent number and filing date identifying a particular patent, the host processor **100** may lock the data record and access the verification databases **140** to determine an issue date and/or schedule of maintenance fee due dates. Further, the host processor **100** may identify all related patents (e.g., parent applications, continuations, divisionals, foreign filings, etc). The host processor **100** may then prompt or generate a report **130** to ask the user **122** if they wish to create data records for the related patents. The system may further link the related data records.

[0022] FIG. **2** shows a schematic diagram of a method for protecting a data record in a networked database according to the present invention. The method is described with respect to the system show in FIG. **1**. However, one of ordinary skill in the art will understand that the method may be implemented in other systems and devices. The method includes a first step **201** of providing data to add (or edit) a data record by a client and/or user. For example, a user **122** may provide data **104** to input fields via a web interface to create a new data record. As discussed above, in some embodiments the user **122** may be given the appearance of creating or editing a data record via the web interface, however the data record may not be edited until the verification step is completed. Data and edits **104** provided by the user/client are next received by the host processor (step **203**).

[**0023**] Following (or during) the receipt of data from the user, the host processor **100** attempts to verify or match the data (step **205**). In some embodiments, the host processor **100** may require that a predetermined number of data fields be completed by the user. The host processor **100** may then query verification databases **140** (and/or database **110**) to verify the data in the data fields. If the data is verified (e.g., matched to a particular set of verification information **142** or record), the data and edits may be stored in the host database (step **207**). The data record is then locked to prevent further edits (step **209**). As discussed above, the host processor **100** may then automatically populate additional data fields of the data record based on the verified data or create additional related data records.

[**0024**] FIG. **3** shows a method of creating or editing a data record in a networked database employable by the system shown in FIG. **1**. In a first step, data and/or edits are received by the host (e.g., from a client and/or client computer). The client may, for example, enter data to several data fields via a web interface. It is contemplated that some of the data may be incorrect and/or in an improper form. Therefore, the system may require that a predetermined number of data fields be filled out prior to identifying the single data record to which it pertains. If the data entered in the data fields is sufficient to match the data to a single set of verification information (or data record) from a source or database (step **303**), the data may be stored and the record locked (step **311**). If the data provided by the client is insufficient to identify a single record, the system may identify possible matches and report the possible matches to the client (step **305**-**307**). The client may then select the one record to which it was referring (step **309**) and the data may be stored in the appropriate data record.

[**0025**] Advantages of the present invention include the provision of a system and method to maintain sensitive data records for a client while minimizing the risk of an employee of the client accidentally modifying the data. The present invention allows a client to perform their own data entry while ensuring that the data is accurate. The present invention is particularly useful for an entity providing the service of paying patent maintenance fees on behalf of a plurality of clients.

[**0026**] Although the invention has been described with reference to a particular arrangement of parts, features, and the like, these are not intended to exhaust all possible arrangements or features, and indeed many modifications and variations will be ascertainable to those of skill in the art.

What is claimed is:

1. A record protection system for a networked database, comprising:

a client;

a host processor accessible by said client via a telecommunications network;

a database accessible by said host processor and containing at least one data record;

software executing on said host processor for receiving data from said client for one or more fields of the data record;

software executing on said processor for receiving data from a source;

software executing on said host processor for comparing the data received from said client to the data received from the source; and

software executing on said host processor to prevent editing of the data record by said client if at least a portion of the data received from said client matches the data received from the source.

2. The system according to claim 1, wherein said software to prevent editing further for permitting editing of the data record if the data received from said client does not match the data received from the source.

3. The system according to claim 1, wherein data received from said client matches if it corresponds to a single data record received from the source.

4. The system according to claim 1, wherein data received from said client matches if it corresponds to a particular number of data fields of a single data record received from the source.

5. The system according to claim 1, further comprising:

software executing on the host processor for storing the matched data in one or more fields of the data record.

6. The system according to claim 1, further comprising:

software executing on said host processor for automatically retrieving supplemental data corresponding to the matched data and storing the supplemental data in said database.

7. The system according to claim 6, wherein at least some of the supplemental data is retrieved from the source.

8. The system according to claim 1, wherein at least one of the data received from said client and the data received from the source is intellectual property data.

9. The system according to claim 8, wherein the source is a patent office database.

10. The system according to claim 1, further comprising:

a web interface for receiving the data from said client, said web interface including a plurality of input fields.

11. The system according to claim 10, wherein each of the input fields correspond to one of fields of the data record.

12. The system according to claim 10, wherein said software for comparing the data compares the data after the completion of a set number of the input fields.

13. The system according to claim 10, wherein said software for comparing the data compares the data in real time as the data is entered into the input fields by said client.

14. The system according to claim 1, further comprising:

software executing on the host processor for generating a report.

15. The system according to claim 14, wherein the report includes an inquiry generated if the data does not match.

16. The system according to claim 14, wherein the report includes one or more potential matches for client selection.

17. The system according to claim 16, wherein said software to prevent editing prevents editing to the data record upon receipt of a match selection from said client.

18. The system according to claim 14, wherein the report includes one or more suggested additions to matched data.

19. The system according to claim 14, said software for generating a report further transmitting the report to said client.

20. The system according to claim 1, further comprising:

software executing on the host processor for receiving an unlock command indicative of permitting editing of the data record.

21. The system according to claim 20, wherein the unlock command is received from one of a host administrator or a client administrator.

22. The system according to claim 1, wherein the data record is a new data record.

23. The system according to claim 1, wherein the data received from said client includes at least one edit to stored data in the data record.

24. A method for protecting data records in a networked database, comprising the steps of:

receiving data from a client via a telecommunications network for one or more fields of a data record;

determining whether at least a portion of the data matches data received from a source;

storing matched data in the data record; and

locking the data record to prevent future editing by the client.

25. The method according to claim 24, further comprising the steps of:

generating a report; and

transmitting the report to the client.

26. The method according to claim 25, wherein the report includes a one or more possible matches to the data received from the client.

27. The method according to claim 25, wherein the report includes a suggested addition to the data record.

28. The method according to claim 24, further comprising the steps of:

retrieving supplemental data corresponding to the data received from the client; and

storing the supplemental data in at least one other field of the data record.

29. The method according to claim 24, further comprising the step of:

unlocking the data record upon receipt of an unlock command.

* * * * *