



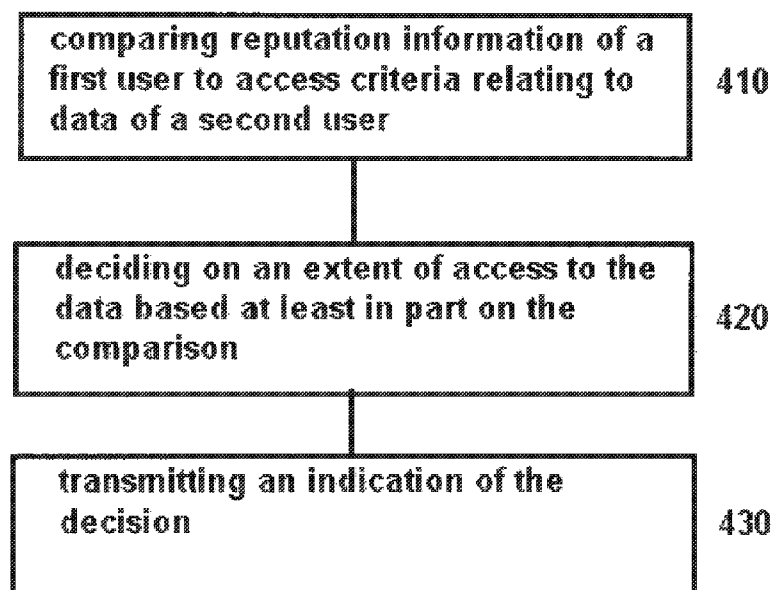
- (51) International Patent Classification:
H04L 29/06 (2006.01)
- (21) International Application Number:
PCT/FI2012/051014
- (22) International Filing Date:
23 October 2012 (23.10.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).
- (72) Inventors: **YAN, Zheng**; Jukolanahde 7 A 3, FI-02180 Espoo (FI). **JAATINEN, Jussi**; Albertinkatu 1 E 108, FI-00150 Helsinki (FI).
- (74) Agents: **NOKIA CORPORATION** et al.; IPR Department, Jussi Jaatinen, Keilalahdentie 4, FI-02150 Espoo (FI).

(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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

- (54) Title: METHOD AND APPARATUS FOR MANAGING ACCESS RIGHTS



(57) Abstract: In accordance with an example embodiment of the present invention, there is provided an apparatus, configured to compare reputation information of a first user to access criteria relating to data of a second user, and to decide on an extent of access to the data based at least in part on the comparison, and a transmitter configured to cause an indication of the decision to be transmitted. The apparatus may receive the reputation information from a reputation source.

FIGURE 4



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
ML, MR, NE, SN, TD, TG).

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

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

METHOD AND APPARATUS FOR MANAGING ACCESS RIGHTS

TECHNICAL FIELD

5 [0001] The present application relates generally to managing data and access rights to data.

BACKGROUND

 [0002] Users need to store their data, which may comprise confidential information such as at least one of financial, healthcare and legal documents, in secured ways. Users may
10 store documents in filing cabinets, safes, bank vaults, archives or company premises in paper or electronic format, for example. Different storage methods provide different usability and security features. For example, a document stored in a bank vault is reliably stored in the sense that it is very unlikely to be stolen, but accessing it requires visiting the bank to enter the vault in person. As another example, a document stored in a public internet site is
15 immediately accessible by anyone, rendering its contents public. As a yet further example, a document stored in a corporate data server may be accessible by persons who have been authorized to access data systems of the corporation. Such a data system may include processes followed by data owners and subscribed system users, and a data storage.

 [0003] Choosing a storage method may involve assessing which persons can be
20 trusted and thus allowed to access information stored in the storage. For example, corporate IT staff may undergo background checks to verify they can be trusted to maintain servers containing confidential information. A cloud storage service provider may assess the risks involved in allowing another party, such as for example another service provider or company, to access data, which may involve assessing whether the party is trustworthy enough and what
25 kind of risks are involved.

 [0004] In general electronically stored information at a third party may be conveniently accessible when needed, but controlling access to it may cause challenges with regard to security, privacy and trust, compared to controlling access to paper documents.

 [0005] Cloud-based storage services offer benefits including dependability, which
30 may be derived from redundancy in storage, and accessibility which may be derived from establishing the cloud-based system based on a public network, such as for example the Internet. Security may be provided by data encryption and/or authentication of users seeking access to the cloud-based storage system. Secure tunnels may be configured over public

networks to prevent unauthorized parties from intercepting communication between a cloud-based storage system and an authorized user accessing the system over the public network.

SUMMARY

5 [0006] Various aspects of examples of the invention are set out in the claims.

 [0007] According to a first aspect of the present invention, there is provided an apparatus, comprising at least one processing core configured to compare reputation information of a first user to access criteria relating to data of a second user, the at least one processing core being configured to decide on an extent of access to the data based at least in part on the comparison, and a transmitter configured to cause an indication of the decision to be transmitted.

 [0008] According to a second aspect of the present invention, there is provided a method, comprising comparing reputation information of a first user to access criteria relating to data of a second user, deciding on an extent of access to the data based at least in part on the comparison, and transmitting an indication of the decision.

 [0009] According to a third aspect of the present invention, there is provided an apparatus, comprising at least one processor, at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to at least receive from a reputation center an indication that a first user is to be given access to data of a second user, the data being stored in the apparatus, and provide the data to the first user.

 [0010] According to a fourth aspect of the present invention, there is provided a method, comprising receiving from a reputation center an indication that a first user is to be given access to data of a second user, the data being stored in an apparatus, and providing the data to the first user.

 [0011] Further aspects of the present invention comprise, for example, computer programs configured to cause methods according to the second and fourth aspects to be performed.

30 **BRIEF DESCRIPTION OF THE DRAWINGS**

 [0012] For a more complete understanding of example embodiments of the present invention, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0013] FIGURE 1 illustrates an example of a system capable of supporting at least some embodiments of the invention;

[0014] FIGURE 2 illustrates a block diagram of an apparatus such as, for example, a reputation center or a storage system, in accordance with at least one example embodiment of the invention;

[0015] FIGURE 3 is a signaling diagram illustrating signaling according to at least some example embodiments of the invention;

[0016] FIGURE 4 is a flowchart illustrating a first method in accordance with at least some embodiments of the invention; and

[0017] FIGURE 5 is a flowchart illustrating a second method in accordance with at least some embodiments of the invention

DETAILED DESCRIPTION OF THE DRAWINGS

[0018] An example embodiment of the present invention and its potential advantages are understood by referring to FIGURES 1 through 5 of the drawings.

[0019] FIGURE 1 illustrates an example of a system capable of supporting at least some embodiments of the invention. In FIG. 1 is illustrated a storage service system, such as for example a cloud storage system, 120. In the following this element will be referred to as storage system. User 140 represents a user, or his device, that is configured to access and interact with storage system 120. The connection between user 140 and storage system 120 is illustrated as connection 141. Connection 141 may take the form of a wire-line interface, such as for example a connection over a network of nodes, which are not illustrated. Connection 141 may comprise a secure tunnel over the network of nodes. In some embodiments, at least part of connection 141 comprises a radio interface, such as where user 140 comprises a wireless user equipment configured to access a network via a radio air interface, such as for example a cellular air interface. User 140 may update or store data in storage system 120 over connection 141, or data of user 140 may be stored in storage system 120 by other means. Reputation center 110 is configured to interface with storage system 120 via connection 111, which may be wire-line or at least in part wireless as discussed above in connection with connection 141. Alternatively, reputation center 110 may be comprised in storage system 120. User 130 may be configured to interface with storage system 120 via connection 131. Connection 131 may be wire-line or at least in part wireless as discussed above in connection with connection 141. User 130 may have data stored in storage system 120, or user 130 may be interested in obtaining from storage system 120 data of other users. User 140 may be

enabled to interface with reputation center 110 via connection 142, which like connection 141 may be at least in part wireless, completely wireless or entirely wire-line.

[0020] In some embodiments, user 130 has an interface to reputation center 110, this interface is illustrated in FIG. 1 as connection 132. In some embodiments, user 140 has an interface to reputation center 110, this interface is illustrated in FIG. 1 as connection 142. At least one of connection 142 and connection 132 may be wire-line or at least in part wireless as discussed above in connection with connection 141. In embodiments where at least one of connection 132 and connection 142 is absent, the users may interact with reputation center 110 indirectly via storage system 120.

[0021] Reputation center 110 may interface to reputation source 150 via connection 151 to retrieve or collect reputation information concerning a user. Reputation center may interface to further reputation source 160 via connection 161. Reputation center may interface to further reputation source 170 via connection 171. In some embodiments, at least one reputation source is comprised in reputation center 110. In some embodiments, where reputation center 110 is comprised in storage system 120, at least one reputation source may also be comprised in storage system 120.

[0022] User 140 desiring to store or have stored his data in storage system 120 may define data access criteria by specifying which users are allowed to access the data, or by describing characteristics, situations or conditions relating to users who are allowed to access the data. User 140 may be configured to provide the access criteria to storage system 120 via connection 141. In some embodiments, the data of user 140 is stored into storage system 120 by user 140, or an employer, bank or healthcare provider of user 140, for example, and user 140 separately sets or modifies access criteria relating to the data over connection 141. In some embodiments, user 140 provides the access criteria to reputation center 110, via connection 142, or by causing storage system 120 to provide the access criteria to reputation center via connection 111 interconnecting storage system 120 and reputation center 110.

[0023] In some embodiments, user 140 defines, or causes to be defined, in the access criteria what kind of users should be given access to the data. This user 140 may define access rights to be provided to a set of users that is not explicitly identified in the access criteria in the sense that identities of users or user groups would be included in the access criteria, but characteristics or conditions of which are described in the access criteria. In some cases, the access criteria may describe at least one situation, such that a user in that situation is to be given access. The characteristics may comprise reputation, such that user 140 issues access rights to be given to the data only to users satisfying at least one criterion relating to

reputation. The at least one criterion relating to reputation may comprise a threshold value of reputation defining a limit in reputation that separates users not to be given access from users that should be given access. For example, if reputation is expressed using a metric that extends in from zero to one, user 140 may define that only users with reputation exceeding

5 0.9 are to be given access. The at least one criterion relating to reputation may comprise an identity of at least one reputation class. For example, where users are classified into two classes, good reputation and bad reputation, user 140 may define in the access criteria that only users with good reputation are to be given access. As another example, where users are classified into three classes, good reputation, intermediate reputation and bad reputation, user

10 140 may define in the access criteria that only users with intermediate or good reputation are to be given access to the data.

[0024] Where reputation may be derived from more than one source, the at least one criterion relating to reputation may define a threshold level or class of reputation in combination with at least one reputation source. In such embodiments, user 140 may define in

15 access criteria that, for example, a reputation defined as at least 90% positive feedback from a certain, identified reputation source is needed for access to the data. In some embodiments, the access criteria may define more than one reputation source with separate criteria for each reputation source, wherein a user seeking access to the data must fulfill all criteria to be given access. In some embodiments, the access criteria define a specific reputation source and

20 corresponding threshold level or class, and also that in case the defined reputation source is unavailable, an auxiliary reputation source, also identified in the access criteria, is to be used. Threshold level or class information may also be provided, in the access criteria, concerning the auxiliary reputation source. Access criteria may also define a requested penalty for abuse.

[0025] Defining access criteria that comprise reputation aspects may allow user 140

25 to specify that only trustworthy persons can access his data. A reputation provided by a reliable reputation source can be utilized to prevent malicious access to the data of user 140. A reputation source may comprise a public reputation source. User 140's data may be stored in storage system 120 in an encrypted form to prevent operators of storage system 120 from accessing the data. Responsive to access being granted to a requesting user, the data may be

30 re-encrypted for the requesting user, for example using a public key of the requesting user. Re-encrypting may comprise transforming the original encryption of a symmetric key used for data encryption by performing a new encryption operation in order to make the encrypted symmetric key accessible by the authorized requesting user, subsequent to which it becomes possible for the requesting user to access the plain data.

[0026] User 130 may issue a request for data of user 140. User 130 may issue the request via connection 131 to storage system 120, responsive to which storage system 120 may be configured to request reputation center 110 to assess whether user 130 satisfies access criteria relating to the data. Storage system 120 may be configured to request reputation center 110 to do this via connection 111, for example. The request sent from storage system 120 to reputation center 110 may comprise an identity of requesting user 130 and an identifier of the data, and the access criteria if they are stored in storage system 120. Alternatively, user 130 may transmit the request via connection 132 to reputation center 110, which may store or have access, via connection 111 from storage system 120, to the access criteria relating to the requested data.

[0027] Responsive to being in possession of the access criteria relating to the requested data and an identity of the requesting user, reputation center 110 may be configured to assess whether the requesting user, in this example user 130, satisfies the access criteria. Assessing may comprise obtaining reputation information of the requesting user and comparing it to the access criteria. Obtaining reputation information may comprise requesting the reputation information from a reputation source, for example where the access criteria define that a user requesting access to the data must have a positive feedback rate exceeding 80% from reputation source 150, reputation center 110 may be configured to request a feedback rate from reputation source 150, using the identity of the requesting user, via connection 151. Alternatively where the access criteria don't define a reputation source, reputation center 110 may be configured to use a default reputation source. Where the access criteria don't define a threshold level or class, reputation center 110 may be configured to use a default one. For example, where the access criteria defines only that a requesting user must have a good reputation without specifying a threshold level or class, or reputation source, reputation center 110 may be configured to select a default reputation source, and apply a default threshold level or class. Examples of default reputation sources may include parties with interaction experiences with requesting user 130, the customers of requesting user 130 who may provide feedback on user 130, a performance monitor of requesting user 130, authorized parties, such as for example online auction sites, banks, police records and credit histories. An example of a threshold level for an online auction site derived reputation is 95% positive feedback from customers or interaction partners. An example of a threshold class for reputation derived from a bank is that the requesting individual has no recent history of default. An example of a threshold class for reputation derived from police records is that the requesting individual has no recent convictions for crimes. An example of a threshold class

for reputation derived from a credit history is that the requesting individual has a history of managing his loans successfully.

[0028] In some embodiments, reputation is generated based on at least one of reputation contributed by user feedback, reputation contributed by performance monitoring and/or reporting, and reputation contributed by authorized parties. Reputation contributed by user feedback may be based at least in part on voting results, votes being cast by interaction partners. In some embodiments, effects of votes are weighted by reputations of voting interaction partners. In some embodiments, effects of votes are decremented as time progresses, resulting in a larger weight being assigned to more recent votes. Reputation contributed by performance monitoring and/or reporting may be based at least in part on records of reliability, availability and/or a level of performance. Effects of such records may be decremented as time progresses, resulting in a larger weight being assigned to more recent records. The number of votes and performance monitoring reports may also be considered in reputation generation. The bigger the number of them, the more convincing the generated reputation.

[0029] When the comparison indicates the requesting user is to be denied access to the data, reputation center 110 may be configured to indicate this to the entity that transmitted the request to reputation center 110. Where reputation center 110 received the request from user 130, it may be configured to indicate to user 130 that access was denied, optionally also indicating the reason for denial. The reason for denial may comprise an identity of a reputation source or sources used in performing the assessment. Where reputation center 110 received the request from storage system 120, it may be configured to indicate to storage system 120 that access is denied, optionally also indicating the reason for denial.

[0030] When the comparison indicates the requesting user to be granted access to the data, reputation center 110 may be configured to indicate this to at least one of the requesting user and storage system 120. The indication may comprise an expression of extent of access, where access is granted to only part of the data. Access may be only partially granted if, for example, the access criteria comprise plural thresholds defining varying levels of reputation needed to access the data to varying extent. For example, the highest threshold in reputation may be required to be exceeded in order to be granted full access. Partial access may comprise that access is granted to a subset of the data or that a resolution of the data is decreased. Decreasing resolution may comprise that when the data is provided to the requesting user, an image or video file is re-sampled at lower resolution. Storage system 120 may alternatively store a higher-resolution and a lower-resolution version of the data.

[0031] When reputation center 110 indicates that access is to be granted, storage system 120 may responsively perform re-encryption and inform the requesting user that the data is available. The requesting user may then request the data to be transmitted, for example via connection 131, from storage system 120 to the requesting user. Re-encrypting may
5 comprise that storage system 120 obtains a key related to the requesting user from reputation center 110 and re-encrypting the data encryption key for the requesting user using the key related to the requesting user. Alternatively, the reputation center 110 may provide a key relating to the requesting user to storage system 120 for use in re-encrypting the data for the requesting user. In some embodiments, the requesting user is queried by reputation center 110
10 for a public key after it has been determined, that the requesting user is to be granted at least some access to the data. An advantage of querying for the key only after it has been determined that access is to be granted is that unnecessary signaling of keys is avoided in cases where access to the data is denied.

[0032] In some embodiments, storage system 120 is not fully trusted by the data
15 owner. Thus, the personal data saved in storage system 120 may be encrypted by the data owner. Other entities may be enabled to access the personal data in order to fulfill a service for the data owner or other parties. How to control personal data access at a semi-trusted or distrusted data center and how to greatly reduce the potential risks caused by distrustworthy access are practical issues.

[0033] In some embodiments, encryption of the stored data isn't used. In these
20 embodiments the data is stored in non-encrypted form, and a copy of the non-encrypted data is provided responsive to the the comparison indicating that the requesting user fulfills the access criteria and is to be granted access the information.

[0034] In some embodiments, reputation center 110 or storage system 120 is
25 configured to inform the requesting user of a penalty associated with abusing access to the requested data. Optionally, the requesting user is prompted to accept or reject the offered penalty before finalizing the granting of access to the data. The penalty may be informed in connection with the indication that access is to be granted. The penalty may be a default penalty of reputation center 110, or alternatively it may be derived from the access criteria
30 relating to the requested data. For example, the access criteria may specify that access is only to be granted to users with more than 80% positive feedback from a specific peer-to-peer site, that the feedback must comprise more than 300 entries, and that a penalty for disclosing the requested data to third parties is that the reputation score of the requesting user in the peer-to-peer site is wiped out. Where the requesting user is prompted to accept the offered penalty,

reputation center 110 may be configured to only finally indicate that access is to be granted responsive to the requesting user accepting the offered penalty.

[0035] In some embodiments, storage system 120 is configured to pay a fee, such as for example an annual fee, to reputation center 110 in exchange for the services of reputation center 110. In some embodiments, user 140 comprises another storage system 120, such as for example a cloud storage system. Services of reputation center 110 may comprise, for example, at least one of re-encryption of credential generation, reputation information handling and deciding on granting access to data.

[0036] In some embodiments, the penalty depends on the reputation of the requesting user, wherein a user with a higher reputation will suffer a lower penalty. Alternatively, a requesting user with a lower reputation, which is still enough to be given access, may suffer a higher penalty for misuse or disclosure of the information. In some embodiments, the penalty may escalate in that a user abusing trust for a second time suffers an increased penalty.

[0037] A default penalty specified by reputation center 110 may comprise that the reputation information of the requesting user in the reputation source used is decremented to reduce the reputation of the requesting user in the reputation source used. In other words, the penalty may comprise that the reputation of the requesting user is made worse. For example, where an interaction-based reputation comprises 100 positive votes and five negative votes, the penalty may comprise adding 50 negative votes.

[0038] In embodiments where a penalty is attached to abusively disclosing the requested data to third parties, processing in storage system 120 may comprise that the data is furnished with a digital watermark to help identify the party who discloses the data to third parties. Applying the digital watermark may comprise that the requested data is subtly modified in a way specific to the requesting user, wherein the requesting user is optionally not informed of the modification. For example, where the requested data comprises a digital X-ray image, the modification may comprise subtle changes to the image file that do not affect the usability and/or quality of the image for legitimate purposes. The modification specific to the requesting user may comprise, for example, that an identity of the requesting user is encoded in the requested data, or a timestamp is encoded in the requested data, such that storage system 120 keeps a record of which users were given copies of the data at which times. The data may also be furnished with a signature from user 140 to prevent modification of the data, for example removal of the digital watermark. The signature may comprise, for example, a hash or cryptographic hash applied to the requested data after addition of the

digital watermark. To determine which user has disclosed a copy of the data, an unmodified copy of the data may be compared to the disclosed copy, the difference between the copies corresponding to the modification specific to the user that has disclosed the data. Without access to the unmodified copy, it would be difficult for the requesting user to determine what the modification is. In some embodiments, digital watermarking is only done where storage system 120 is enabled to access an unencrypted version of the stored data. In some embodiments, storage system 120 is not enabled to access an unencrypted version of the stored data. In embodiments where storage system 120 is not enabled to access an unencrypted version of the stored data, storage system 120 may be configured to process the requested data by requesting an encrypted digital fingerprint from the data owner, and aggregating the encrypted digital fingerprint and encrypted requested data together before providing the aggregated data to the requesting user. An encrypted digital fingerprint may be signed by the data owner to achieve non- repudiation.

[0039] In general there is provided an apparatus, such as for example a server performing the role of reputation center 110. The apparatus may comprise at least one processing core configured to compare reputation information of a first user to access criteria relating to data of a second user, the at least one processing core being configured to decide on an extent of access to the data based at least in part on the comparison. The access criteria may be received in the apparatus from the second user or from a storage system, for example. The reputation information of the first user may be received in the apparatus from at least one reputation source, which may be identified in the access criteria. The comparing may be configured to occur responsive to a request, optionally identifying the first user, received in the apparatus, to access the data. In some embodiments, the request received from the first user comprises an identity of a reputation source capable of providing reputation information of the first user.

[0040] The apparatus may further comprise a transmitter configured to cause an indication of the decision to be transmitted, for example to at least one of the first user and a storage system.

[0041] In some embodiments, the indication comprises an indication as to an extent of access. An extent of access may be full access or partial access, for example. In some embodiments, the indication comprises cryptographic information to enable the first user to access, at least in part, the data. The cryptographic information may comprise, for example, an identity of a key used to encrypt the data for the first user or a hash value the first user may use to verify that the data the first user received is authentic.

[0042] In some embodiments, the indication comprises an instruction to encrypt the data for the first user. Such an instruction may comprise at least one of a public key of the first user, an identity of the first user, a credential related to the first user or an identity of a key of the first user. Responsive to the instruction, a storage system may be configured to
5 obtain a key of the first user and encrypt the data or a key for the first user. The storage system may obtain the key of the first user from the indication, or from a server storing public keys using an identity of the first user.

[0043] In some embodiments, the apparatus is configured to obtain the reputation information of the first user at least in part from the storage service system. Reputation
10 information from the storage service system may comprise information on whether the first user has used the storage service system correctly. In some embodiments, the apparatus is configured to obtain the reputation information of the first user at least in part from a multi-user service. A multi-user service may comprise, for example, at least one of an online auction site, an online peer-to-peer community and a multi-user web of trust service.
15 Reputation information obtained from a multi-user service may comprise reputation information based on feedback concerning the first user from other users of the multi-user service.

[0044] In some embodiments, the apparatus is configured to obtain the reputation information of the first user at least in part from at least one of an insurance company, a bank,
20 a police database, a governmental database and a no-fly list. A no-fly list may comprise a list of individuals, maintained by a government agency or an airline, wherein the individuals on the list are forbidden from boarding aircraft.

[0045] FIGURE 3 is a signaling diagram illustrating signaling according to some example embodiments of the invention. The vertical axes represent user 140, storage system
25 120, reputation center 110, requesting user 130 and reputation source 150, respectively.

[0046] In phase 310, user 140 provides access criteria relating to the user's data to storage system 120. Alternatively, the access criteria may be provided to reputation center 110. In phase 320, requesting user 130 requests to obtain the data from storage system 120. In phase 330, storage system 120 requests reputation center 110 to determine, if requesting user
30 130 is to be granted access to the requested data, optionally also to which extent. In embodiments where storage system 120 was provided the access criteria in phase 310, storage system 120 may furnish the access criteria to reputation center 110 in phase 330. Storage system 120 may inform reputation center 110 of an identity of requesting user 130 in phase 330.

[0047] In phase 340, reputation center 110 may request reputation information of requesting user 130 from a reputation source 150, and responsively, in phase 350, receive it. Reputation center 110 may select reputation source 150 based at least in part on information comprised in the access criteria or the requests of phases 320 and 330. In phase 360 reputation center 110 is configured to compare the reputation information of requesting user 130, obtained from reputation source 150 or elsewhere, to the access criteria. Based at least in part on the comparison, reputation center 110 is configured to decide whether requesting user 130 is to be granted access to the data. Reputation center 110 may be configured to decide to grant only partial access to the data.

[0048] In optional phase 370, reputation center 110 may be configured to inform requesting user 130 of the decision to grant access, wherein the message of phase 370 may comprise information concerning a penalty to be applied to the requesting user 130 should he disclose the requested information to third parties, or otherwise abuse it. A penalty applied to the requesting user may comprise a penalty applied by decreasing the reputation of the requesting user. Where the message of phase 370 comprises information concerning a penalty, it may comprise a request for requesting user 130 to accept the penalty. In this case, in optional phase 380, requesting user 130 may acknowledge and accept the penalty, which may cause a legal agreement to enter into force between user 140 and requesting user 130. In some embodiments, should requesting user fail to acknowledge and accept the penalty, processing stops and access is not granted to requesting user 130. Under the legal agreement, the users agree that should requesting user 130 at least one of abuse and disclose the data, the penalty is to be applied. In connection with the legal agreement, a tracking mechanism may be implemented. A tracking mechanism may comprise a watermarking process as described above. Alternatively, a tracking mechanism may comprise maintaining a record, for example in storage system 120 or in reputation center 110, of users who have been granted access to the data. If the data is disclosed in breach of the legal agreement and only one user has been granted access to it, it may be concluded that the sole user to have been granted access is the one responsible for the disclosure.

[0049] In phase 390, reputation center 110 may be configured to indicate to storage system 120 that access is to be granted to the requesting user to the requested data. The indicating may comprise an indication as to an extent of access to be granted, as discussed above. The indication may comprise an indication that a penalty has been agreed. In optional phase 3100, storage system 120 may be configured to request an encryption key from requesting user 130, and requesting user 130 may be configured to responsively provide the

requested encryption key in optional phase 3110. In phase 3120, storage system 120 may be configured to re-encrypt a data encryption key for requesting user 130. In some embodiments, storage system 120 is configured to, in phase 3120, re-encrypt a secret key to enable a requesting user to gain access to the data. In some embodiments, where the message of phase 390 comprises an indication that a penalty is agreed between the users, storage system 120 is configured to apply a digital watermark specific to requesting user 130, and optionally also a digital signature to the requested data before re-encrypting, to enable requesting user 130 to be identified as a responsible party in case the requested data is disclosed to third parties. In some embodiments the digital watermark and, optionally, the signature are applied every time, regardless of presence of an indication of a penalty in the message of phase 390. In some embodiments, storage system 120 is only configured to apply the digital watermark if storage system 120 is enabled to access an unencrypted version of the requested data. In some embodiments, storage system 120 cannot access an unencrypted version of the requested data. Storage system 120 may be configured to modify the requested data by requesting an encrypted digital fingerprint from the data owner and aggregating the encrypted digital fingerprint and encrypted requested data together before providing the aggregated data to the requesting user. The encrypted fingerprint may be signed by the data owner to achieve non-repudiation.

[0050] In phase 3130, storage system 120 may be configured to inform requesting user 130 that the requested data is ready for retrieval. In phase 3140, requesting user may request for the requested data to be transmitted to him. In phase 3150, storage system 120 may be configured to transmit the requested data, to requesting user 130. In some embodiments storage system 120 is configured to transmit the requested data in phase 3130, and phases 3140 and 3150 don't exist.

[0051] FIGURE 4 is a flowchart illustrating a first method in accordance with at least some embodiments of the invention. The illustrated method may be performed in reputation center 110, for example. In phase 410, reputation information of a first user is compared to access criteria relating to data of a second user. The access criteria may be access criteria received in reputation center 110, for example, from the second user. The access criteria may relate to all data of the second user stored in an apparatus performing the method of FIG. 4, or it may be specific to a certain subset of the data, or an individual data file.

[0052] In phase 420, the method comprises deciding on an extent of access to the data based at least in part on the comparison of phase 410. An extent of access may comprise no access, partial access or full access, for example. In phase 430, an indication of the

decision is transmitted, or caused to be transmitted. The indication may be transmitted, for example, to at least one of the first user and a storage service storing the data of the second user.

[0053] FIGURE 5 is a flowchart illustrating a second method in accordance with at least some embodiments of the invention. The illustrated method may be performed in storage system 120, for example. In phase 510, the method comprises receiving from a reputation center an indication that a first user is to be given access to data of a second user, the data being stored in an apparatus. The apparatus may comprise storage system 120, for example. The indication may comprise at least one of an indication of extent of access to be granted to the first user, an identity of the first user, and an indication that a penalty has been agreed between the first and second users.

[0054] In phase 520, the method may comprise that the data is modified in a way specific to the first user. As discussed above, such a modification may comprise, for example, modifying the data using at least one of an identity of the first user and a timestamp. The modification may be essentially unperceptible in a media file, which may comprise that it is essentially not visible to the naked eye in an image file or that it is essentially inaudible to a natural person in an audio file. The modification may be referred to as a digital watermark. In some embodiments, in addition to the modification, the data is furnished with a digital signature to allow any further modification of the data to be detectable. Phase 520 is optional.

In phase 530, the method may comprise providing the data to the first user. In some embodiments, the data is modified in a way specific to the first user only where storage system 120 is enabled to access an unencrypted version of the stored data. In some embodiments, storage system 120 is not enabled to access an unencrypted version of the stored data. Modifying the data in a way specific to the first user may comprise aggregating an encrypted digital fingerprint with the encrypted data. The digital fingerprint for aggregating may be requested from the data owner, for example responsive to a decision to grant access to the data to the first user. Such requesting may be done by storage system 120 responsive to storage system 120 being informed of the decision to grant access to the first user. Aggregating the encrypted digital fingerprint may comprise aggregating in accordance with homomorphic theory.

[0055] FIGURE 2 illustrates a block diagram of an apparatus 10 such as, for example, a reputation center 110 or storage system 120, in accordance with at least one example embodiment of the invention. While several features of the apparatus are illustrated and will be hereinafter described for purposes of example, other types of electronic devices,

such as mobile telephones, server computers, desktop computers, routers, gateways, and other types of electronic systems, may employ various embodiments of the invention.

[0056] As shown, the apparatus 10 may include at least one transmitter 14 and a receiver 16 configured to communicate information over a network, such as for example a wire-line or wireless communications network. The apparatus 10 may also include a processor 20 configured to provide signals to and receive signals from the transmitter and receiver, respectively, and to control the functioning of the apparatus. Processor 20 may be configured to control the functioning of the transmitter and receiver by effecting control signaling via electrical leads to the transmitter and receiver. Likewise processor 20 may be configured to control other elements of apparatus 10 by effecting control signaling via electrical leads connecting processor 20 to the other elements, such as for example an optional display or a memory. The processor 20 may, for example, be embodied as various means including circuitry, at least one processing core, one or more microprocessors with accompanying digital signal processor(s), one or more processor(s) without an accompanying digital signal processor, one or more coprocessors, one or more multi-core processors, one or more controllers, processing circuitry, one or more computers, various other processing elements including integrated circuits such as, for example, an application specific integrated circuit, ASIC, or field programmable gate array, FPGA, or some combination thereof. Accordingly, although illustrated in FIG. 2 as a single processor, in some embodiments the processor 20 comprises a plurality of processors or processing cores.

[0057] It is understood that the processor 20 may comprise circuitry for implementing audio/video and logic functions of apparatus 10. For example, the processor 20 may comprise a digital signal processor device, a microprocessor device, an analog-to-digital converter, a digital-to-analog converter, and/or the like. Control and signal processing functions of the apparatus may be allocated between these devices according to their respective capabilities. Further, the processor may comprise functionality to operate one or more software programs, which may be stored in memory. In general, processor 20 and stored software instructions may be configured to cause apparatus 10 to perform actions. For example, processor 20 may be capable of operating a program, such as a reputation center program. The program may allow the apparatus 10 to transmit and receive content, such as reputation information, according to a protocol, such as wireless application protocol, WAP, hypertext transfer protocol, HTTP, and/or the like

[0058] Apparatus 10 may also comprise a user interface including, for example, a display 28, a user input interface, and/or the like, which may be operationally coupled to the

processor 20. In this regard, the processor 20 may comprise user interface circuitry configured to control at least some functions of one or more elements of the user interface. The processor 20 and/or user interface circuitry comprising the processor 20 may be configured to control one or more functions of one or more elements of the user interface through computer program instructions, for example, software and/or firmware, stored on a memory accessible to the processor 20, for example, volatile memory 40, non-volatile memory 42, and/or the like. Although not shown, the apparatus may comprise a battery for powering various circuits related to the apparatus. The user input interface may comprise devices allowing the apparatus to receive data, such as a keypad 30.

[0059] The apparatus 10 may include volatile memory 40 and/or non-volatile memory 42. For example, volatile memory 40 may include Random Access Memory, RAM, including dynamic and/or static RAM, on-chip or off-chip cache memory, and/or the like. Non-volatile memory 42, which may be embedded and/or removable, may include, for example, read-only memory, flash memory, magnetic storage devices, for example, at least one data center, hard disks, at least one array of hard disks, floppy disk drives, magnetic tape, etc., optical disc drives and/or media, non-volatile random access memory, NVRAM, and/or the like. Like volatile memory 40 non-volatile memory 42 may include a cache area for temporary storage of data. At least part of the volatile and/or non-volatile memory may be embedded in processor 20. The memories may store one or more software programs, instructions, pieces of information, data, and/or the like which may be used by the apparatus for performing functions of the apparatus.

[0060] Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is that control of access to data may be provided in a controlled, automated and trustworthy manner. Another technical effect of one or more of the example embodiments disclosed herein is that data security is improved. Another technical effect of one or more of the example embodiments disclosed herein is that management of reputation information in reputation sources may be improved.

[0061] Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware and application logic. The software, application logic and/or hardware may reside on memory 40, the control apparatus 20 or electronic components, for example. In an example embodiment, the application logic, software or an instruction set is maintained on any one of various conventional computer-readable media. In the context of this document, a “computer-

readable medium” may be any media or means that can contain, store, communicate, propagate or transport the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer, with one example of a computer described and depicted in FIGURE 2. A computer-readable medium may comprise a
5 computer-readable non-transitory storage medium that may be any media or means that can contain or store the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer. The scope of the invention comprises computer programs configured to cause methods according to embodiments of the invention to be performed.

10 **[0062]** If desired, the different functions discussed herein may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the above-described functions may be optional or may be combined.

[0063] Although various aspects of the invention are set out in the independent claims, other aspects of the invention comprise other combinations of features from the
15 described embodiments and/or the dependent claims with the features of the independent claims, and not solely the combinations explicitly set out in the claims.

[0064] It is also noted herein that while the above describes example embodiments of the invention, these descriptions should not be viewed in a limiting sense. Rather, there are several variations and modifications which may be made without departing from the scope of
20 the present invention as defined in the appended claims.

WHAT IS CLAIMED IS

1. An apparatus, comprising:

at least one processing core configured to compare reputation
information of a first user to access criteria relating to data of a second user, the at
least one processing core being configured to decide on an extent of access to the data
based at least in part on the comparison, and
a transmitter configured to cause an indication of the decision to be
transmitted.

2. An apparatus according to claim 1, wherein the apparatus further comprises a
receiver configured to receive an access request relating to the data, and wherein the at
least one processing core is configured to decide on the extent of access to the data at
least in part responsive to the access request.

3. An apparatus according to any preceding claim, wherein the apparatus is
configured to receive the access criteria from the second user.

4. An apparatus according to any preceding claim, wherein the transmitter is
configured to transmit the indication to a storage service system.

5. An apparatus according to any preceding claim, wherein the indication
comprises an indication as to an extent of access.

6. An apparatus according to any preceding claim, wherein the indication
comprises cryptographic information to enable the first user to access, at least in part,
the data.

7. An apparatus according to any preceding claim, wherein the indication
comprises an instruction to encrypt the data for the first user.

8. An apparatus according to any of claims 4 - 7, wherein the apparatus is
configured to obtain the reputation information at least in part from the storage service
system.

9. An apparatus according to any of claims 1 - 7, wherein the apparatus is configured to obtain the reputation information at least in part from a multi-user service.

5

10. An apparatus according to claim 9, wherein the reputation information comprises feedback information concerning the first user.

10

11. An apparatus according to any of claims 1 - 7, wherein the apparatus is configured to obtain the reputation information at least in part from at least one of an insurance company, a bank, a police database, a governmental database and a no-fly list.

15

12. An apparatus according to any preceding claim, wherein the apparatus is configured to obtain the reputation information from more than one source.

13. An apparatus according to any preceding claim, wherein the apparatus is configured to inform the first user of a penalty for unauthorized disclosure of the data.

20

14. A method, comprising:

comparing reputation information of a first user to access criteria relating to data of a second user;

deciding on an extent of access to the data based at least in part on the comparison, and

25

transmitting an indication of the decision.

15. A method according to claim 14, further comprising receiving an access request relating to the data, and deciding on the extent of access to the data at least in part responsive to the access request.

30

16. A method according to any of claims 14 - 15, wherein the access criteria are received from the second user.

17. A method according to any of claims 14 - 16, wherein the transmitting comprises transmitting the indication to a storage service system.
- 5 18. A method according to any of claims 14 - 17, wherein the indication comprises an indication as to an extent of access.
19. A method according to any of claims 14 - 18, wherein the indication comprises cryptographic information to enable the first user to access, at least in part, the data.
- 10 20. A method according to any of claims 14 - 19, wherein the indication comprises an instruction to encrypt the data for the first user.
21. A method according to any of claims 17 - 20, further comprising obtaining the reputation information at least in part from the storage service system.
- 15 22. A method according to any of claims 14 - 20, further comprising obtaining the reputation information at least in part from a multi-user service.
23. A method according to claim 22, wherein the reputation information comprises feedback information concerning the first user.
- 20 24. A method according to any of claims 14 - 23, further comprising obtaining the reputation information at least in part from at least one of an insurance company, a bank, a police database, a governmental database and a no-fly list.
- 25 25. A method according to any of claims 14 - 24, wherein the method comprises obtaining the reputation information from more than one source.
26. A method according to any of claims 14 - 25, further comprising informing the first user of a penalty for unauthorized disclosure of the data.
- 30 27. An apparatus, comprising:
at least one processor;
at least one memory including computer program code,

the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform at least the following:

receive from a reputation center an indication that a first user is to be given access to data of a second user, the data being stored in the apparatus, and provide the data to the first user.

28. An apparatus according to claim 27, further comprising that the apparatus is caused to receive from the second user access criteria concerning data of the second user stored in the apparatus;

29. An apparatus according to any of claims 27 – 28, wherein the apparatus is caused to modify the data in a way specific to at least one of the first user and a time instant.

30. An apparatus according to claim 29, wherein the modifying comprises modifying based on at least one of a timestamp and an identity of the first user.

31. An apparatus according to any of claims 29 – 30, wherein the apparatus is configured to modify the data in a way specific to at least one of the first user and a time instant only in case the apparatus is enabled to access an unencrypted version of the data.

32. An apparatus according to any of claims 27 – 31, wherein the indication comprises an indication that a penalty has been agreed between the first and second users or between the reputation center and the first user.

33. An apparatus according to claim 32, wherein the apparatus is caused to perform the modifying responsive to the indication that a penalty has been agreed.

34. An apparatus according to any of claims 27 – 30, wherein the apparatus is not enabled to access an unencrypted version of the data and wherein the apparatus is configured to modify the data by aggregating the encrypted data and a digital fingerprint of the second user together before providing the first user access to the data.

35. A method, comprising:

receiving from a reputation center an indication that a first user is
to be given access to data of a second user, the data being stored in an apparatus, and
providing the data to the first user.

36. A computer program product comprising a computer-readable medium bearing
computer program code embodied therein for use with a computer, the computer
program code comprising:

code for comparing reputation information of a first user to access
criteria relating to data of a second user;
code for deciding on an extent of access to the data based at least in
part on the comparison, and
code for a transmitter configured to cause an indication of the
decision to be transmitted.

37. A computer program configured to cause a method according to at least one of
claims 14 – 26 or 35 to be performed.

38. An apparatus comprising:

means for comparing reputation information of a first user to access
criteria relating to data of a second user;
means for deciding on an extent of access to the data based at least
in part on the comparison, and
means for transmitting an indication of the decision.

39. An apparatus, comprising:

means for receiving from a reputation center an indication that a
first user is to be given access to data of a second user, the data being stored in an
apparatus, and
means for providing the data to the first user

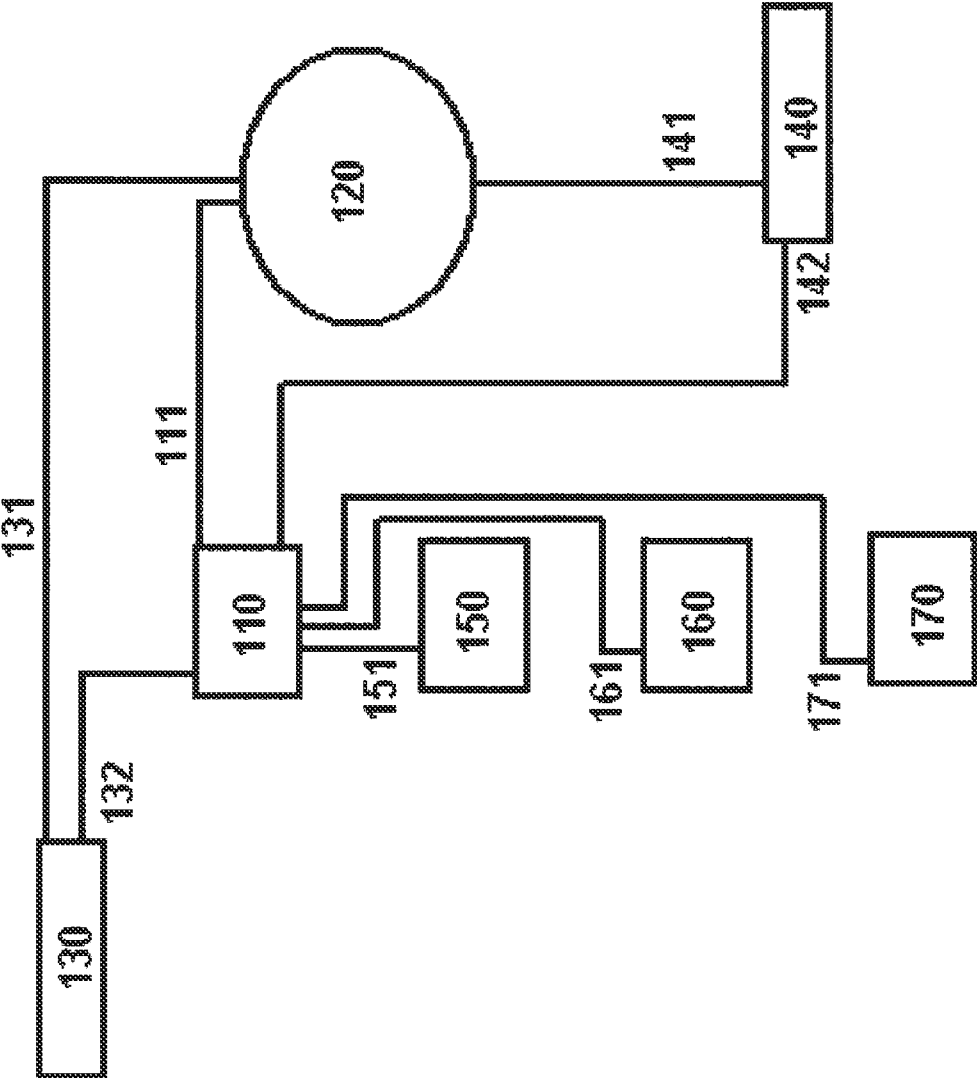


FIGURE 1

10

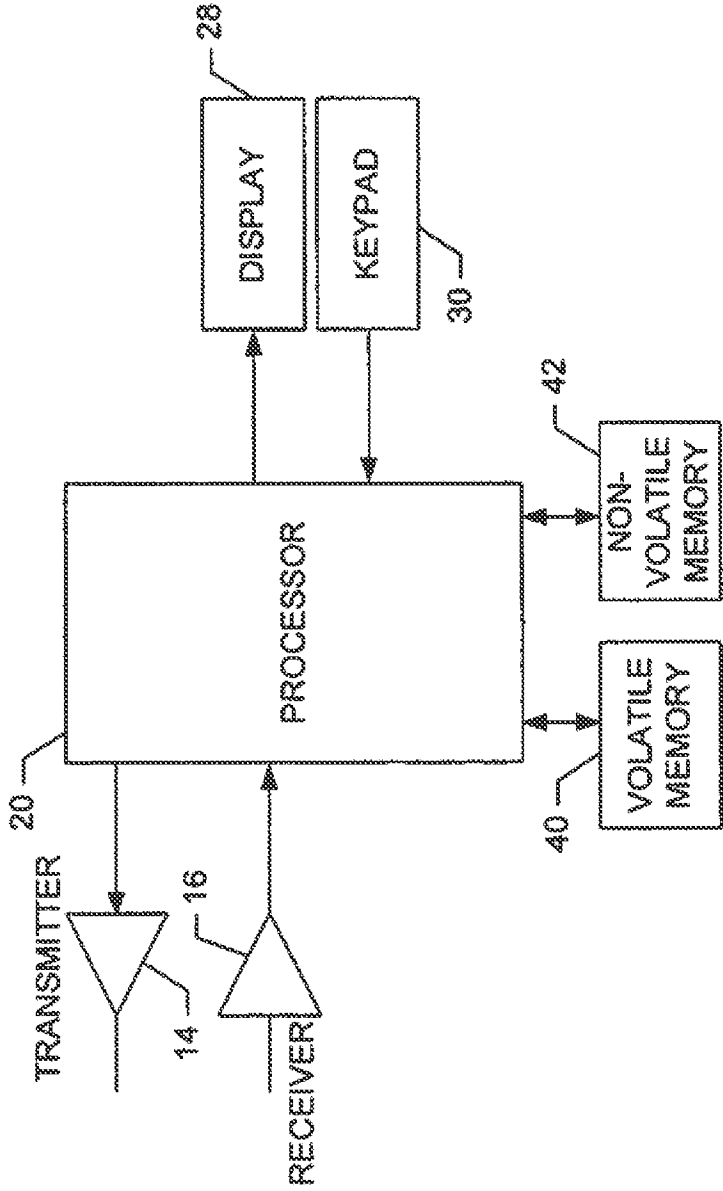


FIGURE 2

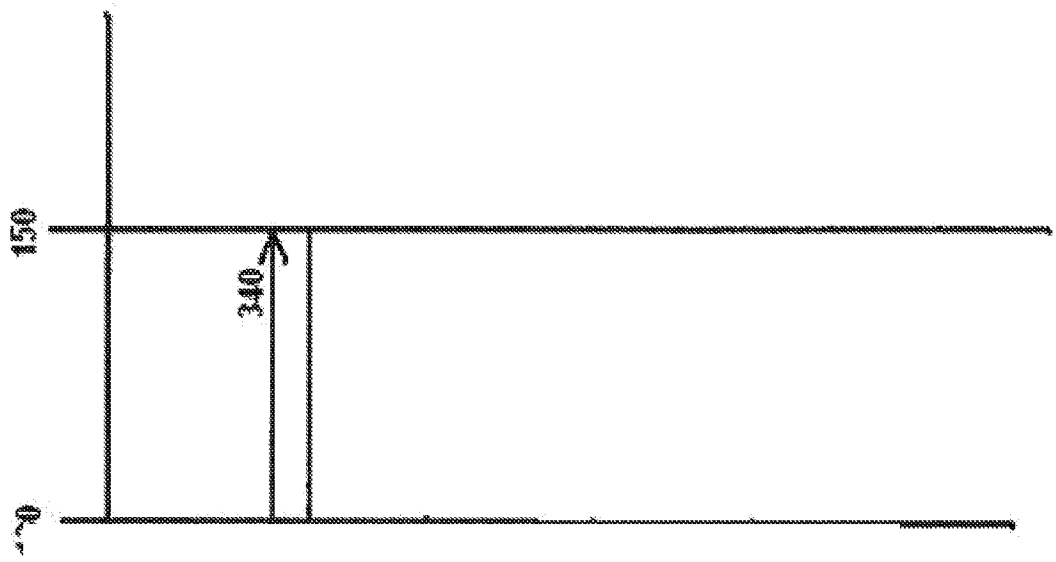
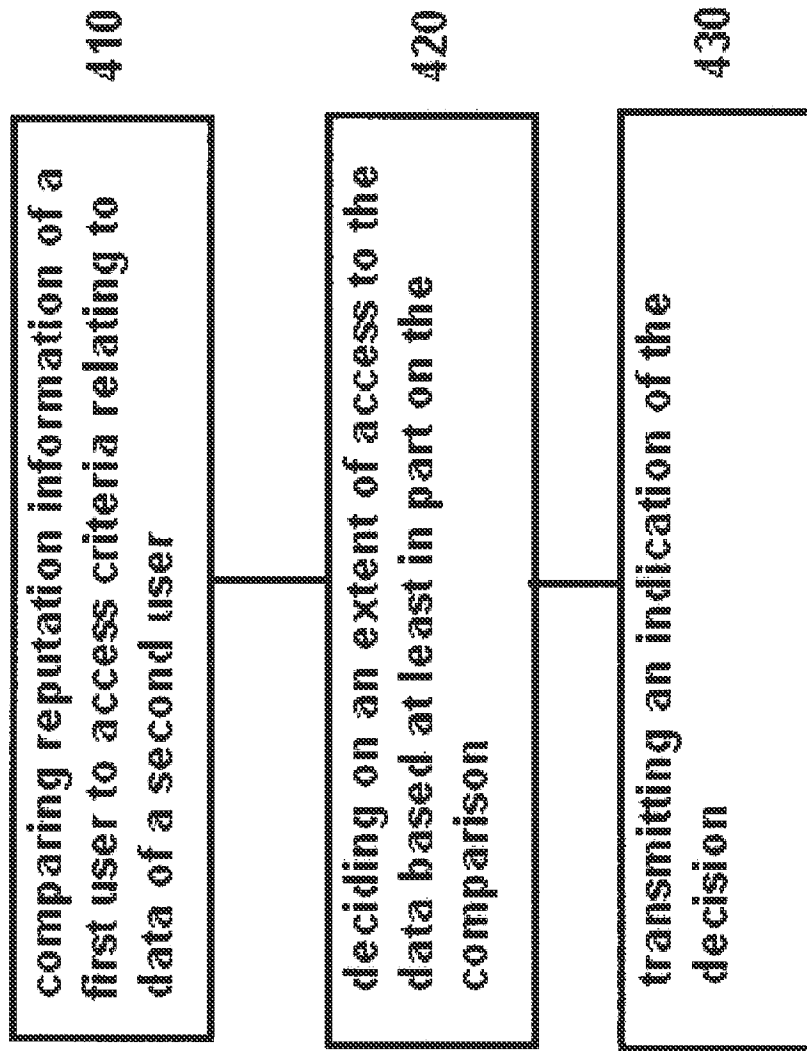
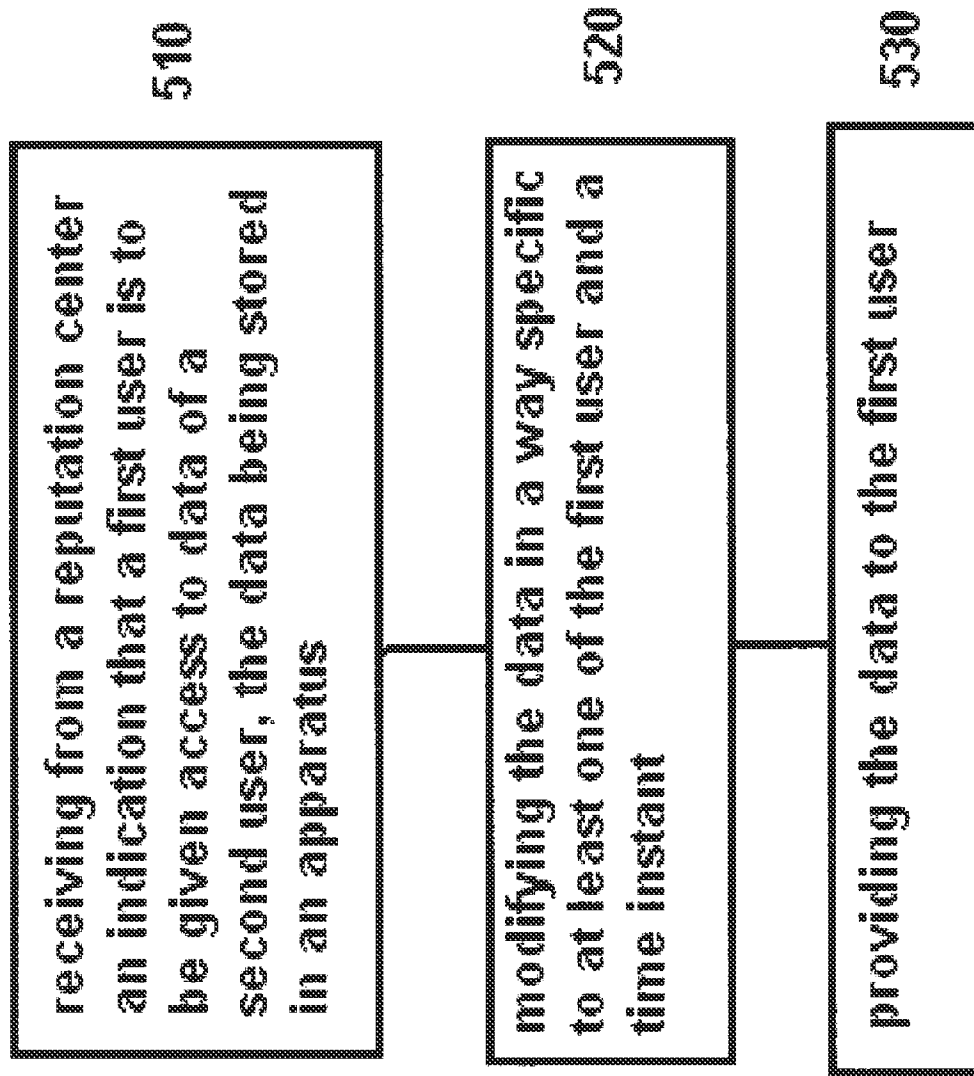


FIGURE 3

**FIGURE 4**

**FIGURE 5**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2012/051014

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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: H04L, H04W, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
FI, SE, NO, DKElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 8266284 B2 (IVERSON KRIS [US]) 11 September 2012 (11.09.2012) pars. [0015],[0016], [0039],[0041], [0071], fig. 6	1-28, 35-39 29-34
A	US 2007214506 A1 (RAO ANUP V [US] et al.) 13 September 2007 (13.09.2007)	1-39
A	US 2008082662 A1 (DANDLIKER RICHARD [US] et al.) 03 April 2008 (03.04.2008)	1-39
A	US 2011296187 A1 (BISSO ROBERT [US] et al.) 01 December 2011 (01.12.2011)	1-39



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

12 June 2013 (12.06.2013)

Date of mailing of the international search report

17 June 2013 (17.06.2013)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland

Facsimile No. +358 9 6939 5328

Authorized officer

Jorma Ristola

Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2012/051014

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.

H04L 29/06 (2006.01)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2012/051014

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 8266284 B2	11/09/2012	CN 102100032 A US 2009287819 A1 WO 2009139950 A1	15/06/2011 19/11/2009 19/11/2009
.....			
US 2007214506 A1	13/09/2007	US 7802304 B2	21/09/2010
.....			
US 2008082662 A1	03/04/2008	EP 2033108 A2 WO 2007136665 A2	11/03/2009 29/11/2007
.....			
US 2011296187 A1	01/12/2011	CN 102918533 A EP 2577523 A2 WO 2011152987 A2	06/02/2013 10/04/2013 08/12/2011
.....			