(19) DANMARK

(10) **DK/EP 2946288 T3**

Patent- og Varemærkestyrelsen

(12) Oversættelse af europæisk patentskrift

(51) Int.Cl.: ***G 06 F 21/62 (2013.01)***

(45) Oversættelsen bekendtgjort den: **2020-08-31**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2020-08-05**

(86) Europæisk ansøgning nr.: **13871735.0**

(86) Europæisk indleveringsdag: **2013-12-26**

(87) Den europæiske ansøgnings publiceringsdag: **2015-11-25**

(86) International ansøgning nr.: **IN2013000804**

(87) Internationalt publikationsnr.: **WO2014111952**

(30) Prioritet: **2013-01-17 IN 157MU2013**

(84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **Tata Consultancy Services Limited, Nirmal Building 9th Floor , Nariman Point, Mumbai 400 021, Indien**

(72) Opfinder: **UKIL, Arijit, Tata Consultancy Services Limited, Bengal Intelligent Park, Building - D Plot No. - A2 M2&N2 Block - EP, Salt Lake Electronics Complex, Sector - V, Kolkata 700091, West Bengal, Indien**
JOSEPH, Joel, Tata Consultancy Services Limited, Tata ResearchDevelopment 6 Design Centre, 54/B Hadapsar Industrial Estate, Hadapsar, Pune 411013, Maharashtra, Indien
BANAHATTI, Vijayanand, Tata Consultancy Services Limited, Tata Research Development 6 Design Centre, 54/B Hadapsar Industrial Estate, Hadapsar, Pune 411013, Maharashtra, Indien
LODHA, Sachin, Tata Consultancy Services Limited, Tata Research Development 6 Design Centre, 54/B Hadapsar Industrial Estate, Hadapsar, Pune 411013, Maharashtra, Indien

(54) Benævnelse: **FESTE FOR ET PANEL SYSTEM OG METODE TIL AT LEVERE ADGANGSKONTROL TIL FØLSOM INFORMATION**

(56) Fremdragne publikationer:
US-A- 5 918 222
US-A1- 2004 181 665
US-A1- 2004 221 062
US-A1- 2005 232 423
US-A1- 2009 031 426
US-A1- 2011 178 943
US-A1- 2011 179 477
US-A1- 2012 260 345
Michele Bezzi: "An information theoretic approach for pri- vacy metrics", TRANSACTIONS ON DATA PRIVACY, 1 January 2010 (2010-01-01), pages 199-215, XP055285913, Retrieved from the Internet: URL:https://www.semanticscholar.org/paper/ An-information-theoretic-approach-for-priv acy-Bezzi/145933fb98872af4c50db185d0f0fb98 08e89c1e/pdf

Fortsættes ...

DESCRIPTION

FIELD OF THE INVENTION

[0001] The invention generally relates to method for controlling access to information and more particularly to method and system for controlling information access by utilizing a trusted computing platform while sharing sensitive information.

BACKGROUND OF THE INVENTION

[0002] With the advent of communicating networks and other related devices handling, processing and transmitting of highly sensitive information has raised concern for the information owners engaged in electronic commerce, health insurance service provides and other such secure transactions. Efforts have been made in past to maintain integrity, validity and confidentiality of these communication channels, but conceited. One major gap existing in prior art solutions is their consideration of trust and privacy as two different aspects of ubiquitous computing applications. It shall be acknowledged that with the evolution of smart applications, trust and privacy cannot be considered as non-intersecting aspects.

[0003] Prior art mostly deals with finding ways of hiding the private data in case of data mining without explicitly providing the methodology for quantifying privacy breach probability of a secret data when shared. None of the prior arts mention provision of a trusted computing platform that can provide the required platform for the users or applications to assess the cost in terms of privacy leak when they plan to be part of such kind of smart activities, and without estimating the cost of privacy breach, private data sharing may yield severe consequences. For example, in participating sensing, crowd sourcing and other volunteering kind of applications, when data is shared for global or community purpose, privacy preserving capability of shared data needs to be known a priori. If not known citizens may not participate in such kind of activities as the private information can be potentially leaked when confirmed trust relationship between different entities involved does not exist. The success of such applications where users voluntarily share their private data for global benefit, therefore, lies in building confidence of privacy preservation among the users and providing a negotiation based framework to decide on sharing private data. Thus, it is challenging to provide for private sharing of information a secure transactional environment without a robust trust management mechanism. Additionally, since sharing of highly confidential information makes it prerogative for the information owner to decide, negotiate and permit the use of sensitive information being shared, required is a negotiation enabling trusted platform for sharing the information in a most secure and trusted way.

[0004] US 2005/232423 (D1) discloses methods for using abstractions of people, including dynamic and static groups of people, to enhance the efficiency of the specification and

automation of policies for sharing information between users with a "need-to-know." It can also provide these users information based on a "time-to-know." By providing access to information based on group affiliation and properties of the content of the information, optimal information privacy is maintained while minimizing encumbrances to sharing data with appropriate users and even at appropriate times.

[0005] "An information theoretic approach for pri-vacy metrics", by Michele Bazzi TRANSACTIONS ON DATA PRIVACY, (20100101), pages 199-215 (D2) discloses anonymizing of data and to assess the quality of the process proposes various privacy metrics, such as k-anonymity,-diversity, and t-closeness. These metrics are able to capture different aspects of the disclosure risk, imposing minimal requirements on the association of an individual with the sensitive attributes.

SUMMARY

[0006] In one aspect of the invention there is provided a processor-implemented information access control method based on trustworthiness computing mechanism, comprising: providing to an information owner an information structure including at least in partition a set of quasi identifiers available from a plurality of auxiliary sources, and in at least other partition a sensitive information; receiving at the information owner, request from one or more consumers to share the sensitive information; computing a trust score for each of the request from one or more consumers based on a probability score indicative of the sensitive information privacy breach to obtain trustworthiness for the one or more consumers, wherein said probability score is evaluated from an exploitation factor derived from availability of quasi identifiers to the corresponding consumer and potency of each of the consumer to deduce the sensitive information from the available quasi identifiers, and wherein the quasi identifiers are information pointers to one or more secret attributes of the sensitive information and has a potential to identify secret information; and enabling the information owner to negotiate upon degree of the sensitive information to be shared therewith and restrictively shared with the one or more consumers based on the trust score.

[0007] The invention also provided a processor-implemented information access control system enabling an information owner of restrictive information sharing with one or more consumer based on trustworthiness computing mechanism, the system comprising: an information module configured to define an information structure including at least in partition a set of quasi identifiers available from a plurality of auxiliary sources, and in at least other partition a sensitive information; a trust management module configured to compute a trust score for each of the request from one or more consumers based on a probability score indicative of the sensitive information privacy breach, to obtain trustworthiness for the one or more consumers, wherein said probability score is evaluated from an exploitation factor derived from availability of quasi identifiers to the corresponding consumer and potency of each of the consumer to deduce the sensitive information from the available quasi identifiers and wherein the quasi identifiers are information pointers to one or more secret attributes of

the sensitive information and has a potential to identify secret information; and a negotiation module stored in memory and executable by a processor to negotiate upon degree of the sensitive information to be shared with the one or more consumers based on the trust score.

[0008] Embodiments of the invention may have the advantage of providing a negotiation based trusted computing network enabling information access control to the information owner.

[0009] Embodiments of the invention may have the advantage of enabling a trusted platform to identify the trusted end user based on a trust score for sharing therewith the sensitive information.

[0010] Embodiments of the invention may have the advantage of vesting the information owner with an authority to decide upon the extent of sensitive information to be shared.

[0011] Embodiments of the invention may have the advantage of minimising risk of privacy breach during transmittance of sensitive information between the information owner and the intended end users.

[0012] Embodiments of the invention may have the advantage of assisting the information owner to computer and choose the end user with a highest trusted score for sharing the highly sensitive information.

[0013] Additional features and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention. These and other features of the present invention will become more fully apparent from the following description, or may be learned by the practice of the invention as set forth hereinafter. The invention is as defined in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The foregoing summary, as well as the following detailed description of preferred embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there is shown in the drawings example constructions of the invention; however, the invention is not limited to the specific system and method disclosed in the drawings:

Figure 1 shows an exemplary architecture in which the invention---the information access control method based on trustworthiness computing platform-is implemented according to an embodiment of the invention.

Figure 2 is a flowchart illustrating the steps of an exemplary information access control method according to this invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015] Some embodiments of this invention, illustrating all its features, will now be discussed in detail. The words "comprising," "having," "containing," and "including," and other forms thereof, are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items.

[0016] It must also be noted that as used herein and in the appended claims, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise. Although any systems and methods similar or equivalent to those described herein can be used in the practice or testing of embodiments of the present invention, the preferred, systems and methods are now described.

[0017] Reference in the specification to "one embodiment", "an embodiment" or "another embodiment" of the present invention means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrase "in one embodiment" or "in an embodiment", appearing in various places throughout the specification, are not necessarily all referring to the same embodiment.

[0018] Embodiments of the present invention are directed to a system and a method for enabling an entity possessing the sensitive information to share in a most secure and trusted way. The system computes trust score of the consumer or end user with whom the information is to be shared, and thereon uses the trust score value to evaluate if the consumer can be trusted for sharing the most sensitive information. Once the consumer is evaluated, the system empowers the information owner to decide on sharing/not sharing and partial sharing aspect of the information.

[0019] In one embodiment, the information owner is capacitated to decide on sharing its private data with respect to a parameter so that the decision is less subjective. In another alternate embodiment, the system and method of present disclosure allows minimum leakage of private information and makes information owner aware of the risk of privacy breach when private information is shared. The information owner can then utilize corrective measures like perturbing sensitive information when sharing, in case trust score of the consumer is low.

[0020] In a preferred embodiment, the information owner being made aware of the trust scores of the end consumers, can negotiate and thereupon decide upon sharing the extent of sensitive information therewith or choose amongst them the best fit end user with whom the entire sensitive information can be securely shared, thus providing maximization of sensitive data privacy protection. Moreover, the information owner is enabled to make cost benefit analysis of information sharing.

[0021] In accordance with one embodiment, a user or application--vis a vis--the information owner requires sharing its sensitive information, for say, location data with other application or to a server or an end user. Since the location data is private in nature and the user wants to share it cautiously. Here the user intends to get two sets of information- one about the privacy breaching probability of sharing location data to the end user and the other of trustworthiness of the end user with respect to that sensitive data (or attribute = location).

[0022] Privacy breach probability of the secret data is computed by the end user or a trusted third party having access to the corresponding end users and communicated to the owner before publishing or at the time of information capture. Trust score of the end user is computed by the (trusted) end user itself and shared with the sources with periodic or request-based publication or by trusted third party. Since the Information owner is enabled with these two pieces of information (privacy breach likelihood of the source for the end user and trust score of the end user) to decide on the sharing, it provides him with the capability of its privacy preservation and risk estimation. It also enables information owner to negotiate with the consumer when sharing private data.

[0023] In another embodiment, an information owner intends to select the health insurance provider and may decide on the quality vis-à-vis privacy respecting health care provider. When sensitive data like one's location or health data needs to be shared, the owner is enabled with the capability to estimate the likelihood of privacy breaching. In case of multiple end users available, owner may like to know about trust scores of each end user; based on which he can judiciary share the sensitive information with the end user having highest trust score value. For this reason, finding privacy breaching probability of a sensitive data to be shared needs to be evaluated.

[0024] Figure 1 shows a system 100 that enables the information owner 102 to share his highly sensitive information, which illustrates one embodiment of the systems and methods described herein. Within the secure and trusted 100, the information owner 102 possessing the sensitive information set S (sl, s2, s3.....sn) over a personal computer or workstation (computer) which is equipped with a computer disk and a memory disk. The computer is linked to other computers of the end users 104 over a trusted network. The information module 100 (i) of the system 100 is configured to define the complete information structure for the information owner 102. The information structure is divided partly in the sensitive information that the owner 102 is required to share with the end users 104 and the quasi identifier information that is available from plurality of auxiliary sources, described in later sections of the disclosure. In other alternate embodiment, the system 100 of the present invention is deployed at the site of the information owner.

[0025] The system of Figure 1 establishes a scenario, according to one exemplary embodiment of the invention, where user or application is the information owner 102 and server(s) 104 is end user for applications 102 and users 102; whereas, applications 104 are end users for user 102. Privacy breach likelihood of the secret data is computed by the system

100 and communicated to the owner 102 before sharing. Trust score value can be periodically published or request-based.

[0026] Considering where a particular user or application 102 holds an information structure, so defined by the information module 101 (i) and consisting of partly a sensitive data set S [s1, s2, s3...sn] and partly a quasi-identifier set [Q]. S and Q can be scalar or vector. Quasi-identifiers are like information pointers to secret attributes of sensitive information and have the potential to explicitly identify the secret (private) information when compared with other external or background information. Sensitive data may be user's identity, location information, salary, disease information, and medical sensor data. On the contrary, Quasi-identifier, for example, can be zip code, age, marital status, educational qualification, vehicle type, medical practitioner's identity etc.

[0027] The consumer 104 can be a remote server, social networking site, other utility service provider or company, organizations etc, which asks information owner 102 to share its private data. The consumer 104 has the capability to avail quasi-identifier data Q from various other sources 106 E1, E2, E3, which are called auxiliary sources. Quasi-identifiers Q are available to the consumer 104 from auxiliary sources 106. Set Q may be different at different auxiliary sources 106 and one set of Q is available to the consumer 104.

[0028] Referring generally to Figure 1 and 2, and particularly to Figure 2, whenever the user 102 is requested to send his/her private value [S], as shown in step 201, the trust score of auxiliary source 106 from Q (= {Q1, Q2, Q3, QX}) is computed by the trust management module 100(ii) of the system 100, shown in step 202. Based on the trust score value Tx of consumer 104, the user 102 can decide to share the sensitive information [S] or not, as shown in step 203 and 204. Accordingly, the privacy breach probability of sensitive information will decrease with intelligent use of computed trust score.

[0029] In the event of multiple consumers (104) X={X1, X2, ...}, the information owner 102 can choose X based on the trust score. More the value of trust score more is the probability of privacy preserving of sensitive data. Based on the trust score value, the user 102 negotiates with the consumer for the extent of sensitive information sharing using the negotiation module 100(iii), also shown in step 203 (of Figure 2), and accordingly take the following, though not limited to, below given actions (indicated in step 204):

1. a) Decide to share with the consumer 104 its sensitive information [S] completely;
2. b) Negotiate with the consumer 104, via a negotiation module, upon the degree of information he considers suitable for sharing like:
    1. 1) With multiple consumers present, selecting the consumer having the highest rated trust score; or
    2. 2) With a consumer rated low for his trust score, the user can perturb some sets of sensitive information using any of the known perturbation algorithm like k-anonymity.

[0030] The other aspect of the present invention describes the process of computation of trust score by the trust management module 100(ii) based upon which the entire decision making of the user 102 rests. It shall be well understood that the consumer 104 acquire the capability of privacy breaching of information owner/user 102 when it avails quasi-identifiers Q from different auxiliary sources 106. Alternately the consumer may maintain his own database for information seeking.

[0031] In an illustrating embodiment, an imaginary health record is considered, the information structure (contained in the information module) of which is depicted in the Table 1 below:

Table 1

Patient name	Age	Sex	Doctor assigned	Blood sugar	Uric acid	Zip	Disease
Jim	22	M	Scooby	110	15.7	309342 0	Kidney failure
Kelly	40	F	Tim	190	6.9	450943 2	AIDS
Tom	75	M	Allan	80	12.2	118095 91	Hepatitis
Harry	52	M	Dino	290	7.1	540912 3	Bone fracture
Jena	43	F	Marga	343	6.1	864500 1	Diabetes

[0032] Here, say Jim is the information owner 102 and the sensitive information that he owns represents a set [S] = {blood sugar, uric acid, disease}. Let the consumer or end user 104 is a medical researcher and asks 102 to send a set of his sensitive information represented by [S'] = {blood sugar, uric acid}. Let Quasi identifier set Q = {age, doctor assigned, zip} for the information structure.

[0033] Now, as understood the trust score and privacy preserving probability of the consumer 104 is its availability to Q. More the consumer gets Q, more is the probability that he can know about the complete sensitive information [S] from a section of said information [S'].

[0034] Trust score of a consumer 104 is computed by the trust management module 100(ii) based on his knowledge gain against the private data [S] and available quasi identifiers Q. Considering that information owner 102 partially reveals his/her sensitive data, while consumer 104 being malicious is capable of deducing the complete sensitive data. In the above case, let the data owner 102 sends his/her blood test report only to a third party/ consumer 104 while keeping his/her disease undisclosed. The set [S] is the complete sensitive data set, while [S'] is the partially revealed set shared with the consumer 104. While the user 102 wants that the unshared information [S ∩ S']' should not get revealed, consumer may like to get intentionally or unintentionally as much knowledge as possible from S' to derive S. Consumer 104 can get the knowledge gain from quasi-identifiers available from different sources 106. It is obvious to

understand that knowledge gain is inversely proportional to trust score i.e. in order to register oneself as a trusted consumer he has to minimize the knowledge gain from auxiliary sources.
Next, in order to compute trust score of consumer 104, the trust management module 100(ii) does the following computation:
Firstly, the exploitation factor of the request information is calculated from two major information sets:

1. a) Availability of quasi identifier information (a) from different sources; and
2. b) Potency of the quasi identifier to expose privacy (p) of the sensitive information

[0035] The exploitation factor of the requested data is thus dependent on the following.

1. 1. Number of quasi identifiers in the requested set
2. 2. Potency of each quasi-identifier to reveal the data owner's identity
3. 3. Availability of the quasi identifiers

[0036] The Exploitation factor of the requested data is expressed as:
Exploitation factor = func (availability of quasi-identifier(a), potency of the quasi-identifier to expose privacy (p))

[0037] For a quasi-identifier, the likelihood to exploit the sensitive information of an information owner 102 is a product of its potency to reveal identity (p) and its availability (a).

[0038] Next, the trust score is computed by the following expression:

Trust score (Tx) = 1 – Exploitation factor of the requested data,

(Or) Tx = 1 – a.p .....(1)

[0039] The following given section will discuss in detail the two aspects of computing trust scorelikelihood to exploit the sensitive information of an information owner 102 is a product of its potency to reveal identity (p) and its availability (a).

1) Potency to reveal identity (p)

[0040] Potency of a quasi-identifier is its ability to uniquely identify the information owner within a population of the available set of quasi-identifiers (Q).

p = info_gain (Q);

and

info_gain (Q) = priv_gain (q)

$$\text{priv_gain}(q) = \left(\sum_{i=1}^{|q|} q_i \cdot log_2 \frac{1}{q_i}\right)$$

$$\text{info_gain}\ (Q) = \left(\sum_{n=1}^{|Q|} priv_gain(q_n)\right)$$

$$\textbf{so, p=} \left(\sum_{n=1}^{|Q|} \left(\sum_{i=1}^{|Q|} q_i . log_2 \frac{1}{q_i}\right)_n\right)$$

2) Availability (a)

[0041] Availability of a quasi-identifier is determined by the number of auxiliary sources 106 supplementing the quasi-identifier are present and the degree of accessibility of such auxiliary sources 106 for that data consumer 104. For example the information on Wikipedia is more accessible than a National Defense employee's database. So availability may vary for every data consumer.

[0042] Some governing principles of availability are:

- More the number of auxiliary sources providing the requested information more is the availability;
- More public or accessible the auxiliary sources are, more is the availability

[0043] One other exemplary embodiment considers a database containing a patient information table bearing the columns: Name, Date of Birth, Gender, Zip and Disease. Let the information related to Date of Birth, Gender, Zip combination forms a set of quasi-identifier information denoted as: q_1 = {Date of Birth, Gender, Zip}.

[0044] Let the information consumer 104 is a pharmaceutical company which requires the patient information as part of their medicinal research. The information owner 102 does not want his or her identity to be revealed and therefore mask the name column value while providing the other details to the consumer 104. But since the shared information has a quasi-identifier i.e. q_1, there is a possibility of revealing the patient's identity. In this case, from (1), the

Likelihood of exploitation for $q_1 = p_1 * a_1$.

Empirically it has been observed that 87% of the people in the U.S. can be uniquely identified by the combination of Gender, Date of Birth and Zip. Therefore (Gender, Date of Birth, Zip) forms a 0.87 quasi-identifier for the U.S. population.

[0045] Therefore let's consider the potency of q1 to be 0.87 and its availability for the data consumer as 0.85. Hence the likelihood of exploitation for q1 = 0.7395.

Hence Tx for consumer = 1 - 0.7395 = 0.2605.

[0046] Likewise, let the requested data have 'n' number of quasi identifiers.

Quasi-identifier	Potency	Availability	L(Qi)
Q_1	0.87	0.8	0.696
Q_2	0.7	0.3	0.21
Q_3	0.5	0.5	0.25

[0047] The combined likelihood of exploitation for all three quasi-identifier is given by,

$L_{Ex3} = L(Q_1 \cup Q_2 \cup Q_3)$

[0048] Here the inclusion exclusion principle of probability theory is applied to determine the value of L_{Ex3}. In this case, if the likelihood of exploitation for all the quasi-identifiers is assumed to be independent of each other then,

$L_{Ex3} = L(Q_1) + L(Q_2) + L(Q_3) - L(Q_1 \cap Q_2) - L(Q_1 \cap Q_3) - L(Q_3 \cap Q_2) + L(Q_1 \cap Q_2 \cap Q_3)$

[0049] Therefore, L_{Ex3}=0.81988 and Tx = 1 - L_{Ex3} = 0.18012.

Thus, Exploitation factor of requested data can be expressed as,

$L_{Exn} = L(\cup_{i=1}^{n} Qi)$

where 'n' is the number of quasi-identifiers in the requested data.

[0050] Now understanding that from the trust management module 100(ii) that if the trust score of the consumer 104 is low, the negotiation module 100 (iii) assists the information owner 102 to negotiate upon the degree of information to be shared and finally communicates the consumer regarding the owner decision of not sharing the sensitive details such as Gender, Date of Birth and Zip as it is. It has to protect the information owner's identity. This is how the information owner and data consumer negotiates via the negotiation module. For the pharmaceutical company, gender is important factor in medicinal research. Hence the consumer may want the gender value to be as it is. The owner 102 can anonymize the zip and DOB before sharing the information with the data consumer, as will be suggested by the negotiation module. This will reduce the potency of the quasi-identifier of revealing the owner identity which in turn reduces the likelihood of exploitation.

Name	Date of Birth	Gender	Zip	Disease
Adam	27-Jan-1983	Male	422009	Flu
Luther	3-Jun-1978	Male	411023	Migraine

[0051] In other alternate embodiment, when quasi-identifiers are dependent, Bayesian inference is required for computing availability "a". Consider, Pr (q_1) = probability of occurrence of quasi-identifier q_1, Pr (s_1| q_1) = probability of knowing the sensitive attribute s_1 from q_1, Pr (q_2| q_1) = probability of knowing another quasi-identifier q_2 from q_1. Availability "a" is the probability of knowing sensitive attribute s_1 from the quasi-identifiers, where,

$$a = P_r(s1|q1) = \frac{P_r(q1).P_r(s1|q1)}{P_r(q1).P_r(q2|q1) + P_r(q1).P_r(s1|q1)}$$

[0052] Broadly, the system 100 is understood to comprise of an information module 100(i) configured to define an information structure; a trust management module 100(ii) to compute trustworthiness of each of the consumer from a probability score derived from an exploitation factor that is further defined as a product of availability of quasi identifier information to the corresponding consumer and potency of each of the consumer to deduce the sensitive information from the available quasi identifier; a negotiation module 100(iii) stored in memory and executable by a processor to negotiate upon degree of the sensitive information to be shared with the consumers upon communicating with the trust management module 100(ii) and accordingly shares the information completely/partially with perturbation of the private data.

[0053] Program instructions may be used to cause a general-purpose or special-purpose processing system that is programmed with the instructions to perform the methods described herein. Alternatively, the methods may be performed by specific hardware components that contain hardwired logic for performing the methods, or by any combination of programmed computer components and custom hardware components. The methods described herein may be provided as machine readable medium having stored thereon instructions that may be used to program a processing system or other electronic device to perform the methods.

[0054] The term "machine readable medium" or "processor implemented method" used herein shall include any medium that is capable of storing or encoding a sequence of instructions for execution by the processor and that causes the processor to perform any one of the methods described herein: Furthermore, it is common in the art to speak of software, in one form or another (e.g., program, procedure, process, application, module, logic, and so on) as taking an action or causing a result. Such expressions are merely a shorthand way of stating the execution of the software by a processing system to cause the processor to perform an action or produce a result.

[0055] Accordingly, although the invention has been described in detail with reference to particular preferred embodiments, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the scope of the claims that follow and their equivalents.

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US2005232423A [0004]

Non-patent literature cited in the description

- **MICHELE BAZZI**An information theoretic approach for pri-vacy metricsTRANSACTIONS ON DATA PRIVACY, 2010, 199-215 [0005]

Påstande

1. En processor-udført information-adgangskontrolmetode, baseret på pålidelig databehandlingsmekanisme, der består af:

at levere en informationsstruktur til en informationsejer, inklusive mindst i adskillelse et sæt kvasi-identifikationsgenkendere, der er tilgængelige fra en flerhed af hjælpekilder, og i mindst anden adskillelse en følsom information, der er forbundet med informationsejeren, hvori kvasi-identifikationsgenkenderne er informationsvisere, der er forbundet med informationsejeren og viser til én eller flere hemmelige kendetegn for den følsomme information og har potentialet til at identificere hemmelig information, og hjælpekilder er andre kilder end informationsejeren;

at modtage hos informationsejeren anmodning fra en eller flere forbrugere om at dele den følsomme information; databehandle en tillidsscore for hver af anmodning fra én eller flere forbrugere, baseret på en sandsynlighedsscore, der indikerer brud på den følsomme personoplysning for at opnå tillid til en eller flere forbrugere, hvori nævnte sandsynlighedsscore evalueres fra en udnyttelsesfaktor, hvor udnyttelsesfaktoren er et produkt af tilgængeligheden af kvasi-identifikationsgenkendere til den tilsvarende forbruger og styrken af hver af kvasi-identifikationsgenkenderne til at røbe personoplysninger fra den følsomme information, hvori tilgængeligheden af en kvasi-identifikationsgenkender afgøres ved et antal hjælpekilder, der er til stede, og graden af adgang for antallet af hjælpekilder for den ene eller flere forbrugere, og hvori styrken fra en kvasi-identifikationsgenkender er en evne for kvasi-identifikationsgenkenderen til udelukkende at identificere informationsejeren indenfor en mængde af de tilgængelige sæt kvasi-identifikationsgenkendere, og sætte informationsejeren i stand til at handle på graden af den følsomme information, der dermed skal deles og restriktivt delt med den ene eller flere forbrugere, baseret på tillidsscoren.

2. Metoden i påstand 1, hvori den i det mindste ene forbruger er en fjernserver, socialt netværksvært, offentlige værker leverandør eller selskab, organisation, en forsker eller en kombination deraf.

3. Metoden i påstand 1, hvori tillidsscoren er databehandlet ved modtagelse af anmodningen fra den ene eller flere forbrugere.

4. Metoden i påstand 1, hvori informationsejeren handler for at begrænse adgang til følsom information til en upålidelig part, delvist eller helt, baseret på tillidsscoren.

5. Metoden i påstand 1, hvori informationsejeren begrænser delingen af følsom information ved anvendelse af forstyrrelsesalgoritme som k-anonymity.

6. En processor-indsat information-adgangskontrolsystem, der gør en informationsejer af restriktiv information i stand til at dele med en eller flere forbrugere, baseret på tillidsdatabehandlingsmekanisme, hvor systemet består af:

et informationsmodul, der er konfigureret til at definere en informationsstruktur, inklusive mindst i adskillelse et sæt kvasi-identifikationsgenkendere, der er tilgængelige fra en flerhed af hjælpekilder, og i det mindste anden adskillelse en følsom information, der er forbundet med informationsejeren, hvori kvasi-identifikationsgenkenderne er informationsvisere, der er forbundet med informationsejeren, og viser til en eller flere hemmelige kendetegn for den følsomme information og har potentiale til at identificere hemmelig information, og hjælpekilder er andre kilder end informationsejeren;

et tillidsstyringsmodul, der er konfigureret til at databehandle en tillidsscore for hver anmodning fra en eller flere forbrugere, baseret på en sandsynlighedsscore, der indikerer brud på den følsomme personoplysning, for at opnå tillid til en eller flere forbrugere, hvori nævnte sandsynlighedsscore evalueres fra en udnyttelsesfaktor, hvor udnyttelsesfaktoren er produktet af tilgængeligheden af kvasi-identifikationsgenkendere til den tilsvarende forbruger og styrken af hver af kvasi-identifikationsgenkendere til at afsløre personoplysninger om den følsomme information, hvori tilgængeligheden af en kvasi-identifikationsgenkender afgøres ved antallet af hjælpekilder, der er tilstede og graden af adgang for antallet af hjælpekilder for den ene eller flere forbrugere, og hvori styrken af en kvasi-identifikationsgenkender er en kvasi-identifikationsgenkenders evne til udelukkende at identificere informationsejeren indenfor en mængde af tilgængelige sæt kvasi-identifikationsgenkendere; og

et forhandlingsmodul, der er opbevaret i hukommelse og udførlig ved en processor til at forhandle på en grad af den følsomme information, der skal deles med en eller flere forbrugere, baseret op tillidsscoren.

7. Information-adgangskontrolsystemet i påstand 6, hvori den i det mindste ene forbruger kan være en fjernserver, social netværksvært, offentlige værker leverandør eller selskab,

organisationer, en forsker eller en kombination deraf.

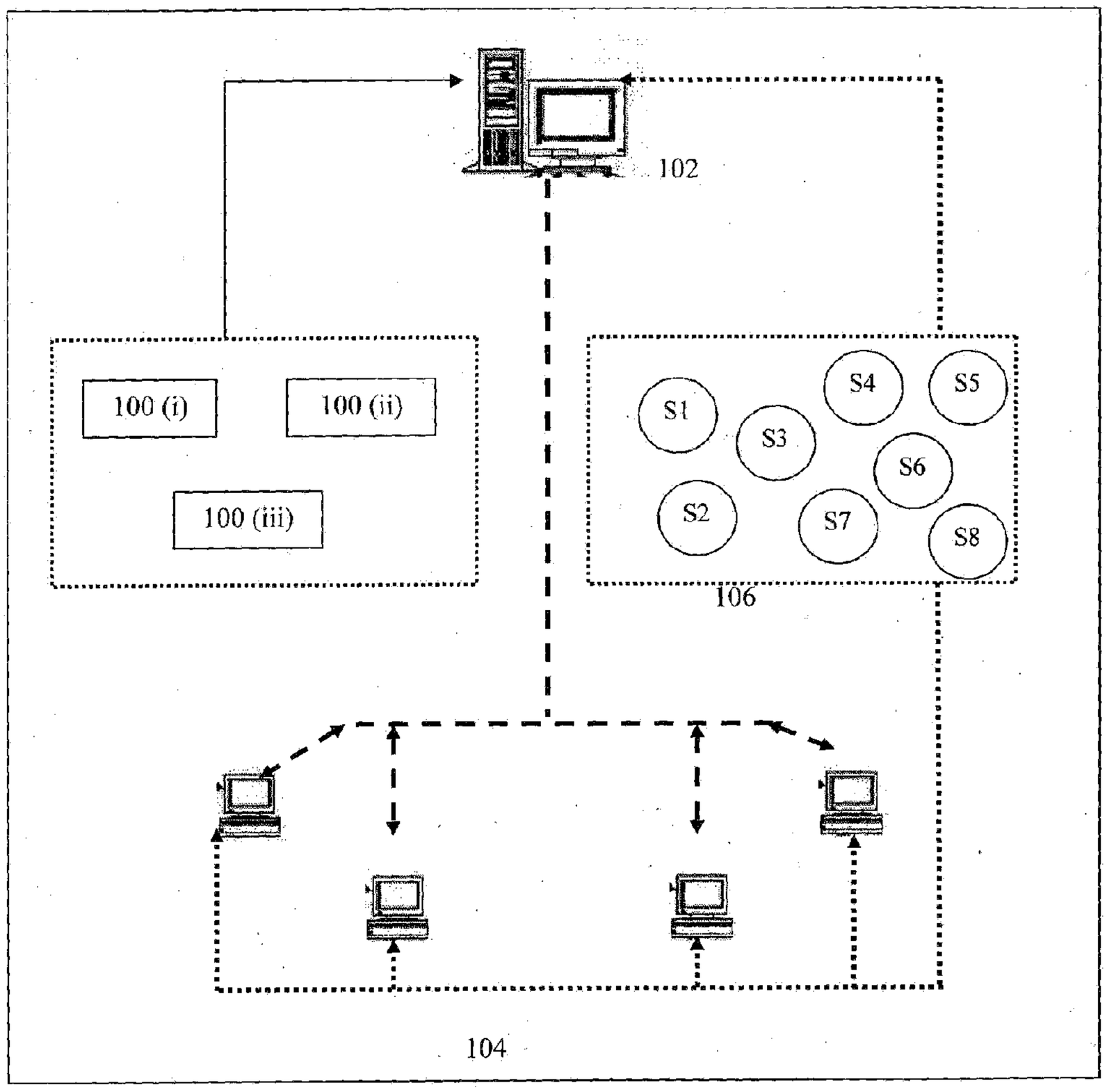
8. Information-adgangskontrolsystemet i påstand 6, hvori tillidsstyringsmodulet kommunikerer med informationsejeren til at databehandle tillidsscoren, når som helst forbrugeren anmoder om det.

9. Information-adgangskontrolsystemet i påstand 6, hvori tillidsstyringsmodulet databehandler udnyttelsesfaktoren som et produkt af tilgængeligheden til kvasi-identifikationsgenkender og forbrugerens styrke til at udlede den følsomme information.

10. Information-adgangskontrolsystemet i påstand 6, hvori forhandlermodulet begrænser adgang til følsom information til en upålidelig part, delvist eller helt, i respons til tillidsscore, der er databehandlet af tillidsstyringsmodulet.

11. Information-adgangskontrolsystemet i påstand 6, hvori forhandlingsmodulet begrænser delingen af følsom information ved anvendelse af forstyrrelsesalgoritme som k-anonymity.

DRAWINGS



Quasi-identifier information gathering from auxiliary sources ·····►

Negotiation and permission ◄- - - -►

FIGURE 1

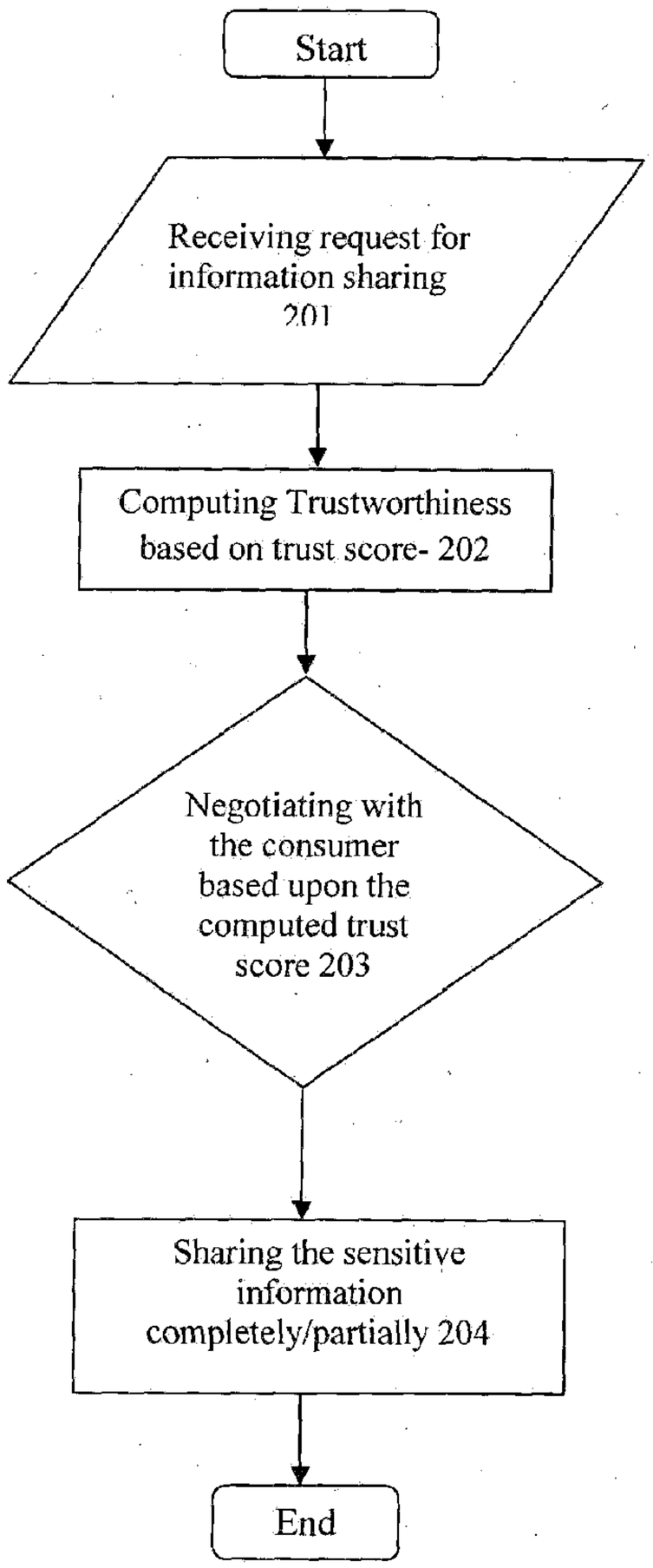

Start
Receiving request for information sharing 201
Computing Trustworthiness based on trust score- 202
Negotiating with the consumer based upon the computed trust score 203
Sharing the sensitive information completely/partially 204
End

FIGURE 2