(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 July 2017 (06.07.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/116311 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/SG2016/050627

(22) International Filing Date:
30 December 2016 (30.12.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201510786Y 30 December 2015 (30.12.2015) SG

(71) Applicant: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis, Singapore 138632 (SG).

(72) Inventors: **WESTERSKI, Adam Maciej;** c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632 (SG). **KANAGASABAI, Rajaraman;** c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632 (SG). **SIM, Sian Hui Kelvin;** c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP;** P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD OF DETECTING FRAUD IN PROCUREMENT AND SYSTEM THEREOF

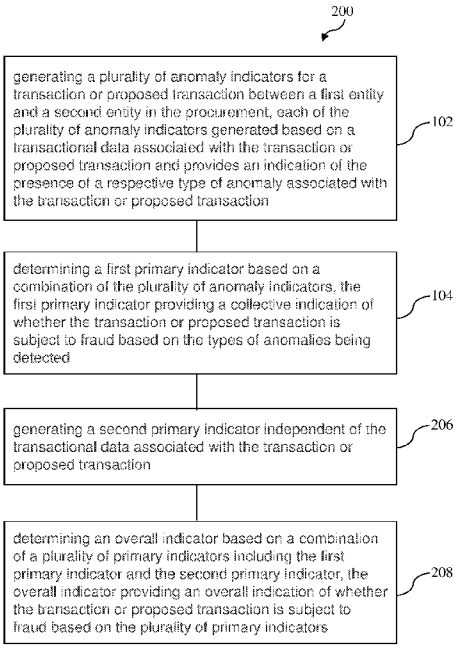

FIG. 2

(57) Abstract: There is provided a computer-implemented method of detecting fraud in procurement. The method includes generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity based on an associated transactional data. A first primary indicator is then determined based on a combination of the plurality of anomaly indicators, providing a collective indication of fraud. The primary indicator can next be further combined with a second primary indicator which can be based on transaction history involving the first and/or the second entity, thus generating an overall indicator to provide an indication of fraud.

WO 2017/116311 A1

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

METHOD OF DETECTING FRAUD IN PROCUREMENT AND SYSTEM THEREOF

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of priority of Singapore Patent Application No. 10201510786Y, filed 30 December 2015, the contents of which being hereby incorporated by reference in its entirety for all purposes.

TECHNICAL FIELD

[0002] The present invention generally relates to a method of detecting fraud in procurement and a system thereof.

BACKGROUND

[0003] Procurement is fast emerging as an area of economic importance. It has been reported that the average procurement department of an organization manages about 60% of total enterprise spend, and many of the organization's larger and longer-term opportunities may depend on how well procurement identifies and drives innovation within the organization. A sharp rise in procurement fraud has also been observed, such as reported in a 2014 PwC Global economic crime survey. The survey reported that 29% of the companies are affected by at least one form/type of procurement fraud, making it the second most common economic crime.

[0004] Conventionally, "eyeball" sampling may be used for compliance checking and fraud detection in procurement, but such an approach is a tedious and error-prone. The increasing adoption of procurement software has given rise to the availability of transactional data or usage logs that lend themselves amenable for data analysis. Consequently, business intelligence software has begun to be employed to assist in fraud detection in procurement. In addition, tools that perform descriptive statistics have also been used for computing quantities such as mean and dispersion. Both these methods have been found to be useful for macro-level insights, such as identifying departments or divisions of a company with maximum procurement spending, computing average expenditures and other statistical parameters such as quantiles or variances. They can also

help in data visualization such as trend graphs, and data pre-processing tasks such as data validation. However, major procurement frauds such as bid rigging, collusion between suppliers, and fraudulent payments via shell companies can be so subtle that they are difficult to detect by standard macro-level analysis.

[0005] Therefore, besides exploiting well established analysis methods, other solutions/approaches to the above problems have been examined by the academic research community in a broader context of fraud detection. The majority of proposed approaches revolve around employing data mining methods, which leverage statistical models and probabilistic approaches to create advanced machine learning algorithms. As the fraud detection problem can relate to many domains, such proposed solutions may vary in terms of scope, required input data, and challenges to solve. Within the machine learning area, the vast majority of existing approaches are based on supervised learning algorithms, i.e., assume existence of well annotated set of past fraud cases that are used for teaching the algorithm to detect future fraud cases. For example, popular techniques may include the use of neural networks and Bayesian networks or less frequently case-based reasoning or decision trees.

[0006] Regardless of the conventional approach taken, according to a published survey, conventional approaches are mostly explored specifically in context of financial fraud and credit card fraud. Nevertheless, there are also related researches that aim to solve similar fraud problems in other areas such as telecommunications, insurance or procurement.

[0007] In the area of procurement fraud, there exist published research works focusing on solving selected aspects of fraud detection, proposing a language to describe a fraud rule, assessing fraud risk rather than detecting fraud cases, and focusing on requester-vendor similarity detection to find collusions. While in the specific narrow application areas and under set conditions, such conventional approaches may provide satisfactory results, they do not focus on delivering a solution to cover the complexity of real world organization models/issues where many different types of fraud may occur concurrently.

[0008] A need therefore exists to provide a method of detecting fraud in procurement and/or a system thereof that seek to overcome, or at least ameliorate, one or more of the

deficiencies of conventional techniques/approaches such as those as mentioned above. It is against this background that the present invention has been developed.

SUMMARY

[0009] According to a first aspect of the present invention, there is provided a method (computer-implemented method) of detecting fraud in procurement, the method comprising:

generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction; and

determining a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected.

[0010] In various embodiments, the first primary indicator is determined based on a weighted sum of the plurality of anomaly indicators.

[0011] In various embodiments, the sum of the weights respectively assigned to the plurality of anomaly indicators is equal to 1.

[0012] In various embodiments, the plurality of anomaly indicators comprises one or more of an order split indicator, a cut-off rate indicator, and a price deviation indicator, wherein:

the order split indicator provides an indication of the presence of a type of anomaly relating to a purchase order being a result of a purchase order splitting,

the cut-off rate indicator provides an indication of the presence of a type of anomaly relating to a purchase order having a value higher than but close to a minimal predetermined value requiring a purchase order to be subjected to a tender process, and

the price deviation indicator provides an indication of the presence of a type of anomaly relating to a purchase order for one or more items having a value deviating from an expected or average value for the one or more items included in the purchase order.

[0013] In various embodiments, the transactional data is a purchase order data, the purchase order data comprising a first information for identifying the first entity, a second information for identifying the second entity, a third information for providing a description of the transaction or proposed transaction, and a fourth information indicative of at least one value associated with the transaction or proposed transaction.

[0014] In various embodiments, the method further comprises:

generating a second primary indicator independent of the transactional data associated with the transaction or proposed transaction; and

determining an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator, the overall indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on the plurality of primary indicators.

[0015] In various embodiments, the overall indicator is determined based on a weighted sum of the plurality of primary indicators.

[0016] In various embodiments, the second primary indicator is generated based on at least one of a first entity indicator and a second entity indicator, the first entity indicator provides an indication of a reliability of the first entity and the second entity indicator provides an indication of a reliability of the second entity.

[0017] In various embodiments, the first entity indicator is generated based on a history of at least one past transaction involving the first entity, and/or the second entity indicator is generated based on a history of at least one past transaction involving the second entity.

[0018] In various embodiments, the history of at least one past transaction involving the first entity relates to at least the overall indicator of the at least one past transaction involving the first entity, and/or the history of at least one past transaction involving the

second entity relates to at least the overall indicator of the at least one past transaction involving the second entity.

[0019] In various embodiments, the second primary indicator is generated based on a weighted sum of the first entity indicator and the second entity indicator.

[0020] In various embodiments, the collective indication and/or the overall indication of whether the transaction or proposed transaction is subject to fraud is expressed as a single numerical value representing a probability that the transaction or proposed transaction is subject to fraud.

[0021] In various embodiments, the method further comprises storing the overall indicator determined for the transaction or proposed transaction between the first entity and second entity in a database, wherein the overall indicator stored is associated with the first entity and the second entity involved in the transaction or proposed transaction.

[0022] In various embodiments, the first entity is a requester or buyer associated with the transaction or proposed transaction, and the second entity is the vendor or supplier associated with the transaction or proposed transaction.

[0023] According to a second aspect of the present invention, there is provided a system for detecting fraud in procurement, the system comprising:

an anomaly indicator generator module configured to generate a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction; and

a first primary indicator determining module configured to determine a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected.

[0024] In various embodiments, the first primary indicator is generated based on a weighted sum of the plurality of anomaly indicators.

[0025] In various embodiments, the system further comprises:

a second primary indicator generator module configured to generate a second primary indicator independent of the transactional data associated with the transaction or proposed transaction; and

an overall indicator determining module configured to determine an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator, the overall indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on the plurality of primary indicators.

[0026] In various embodiments, the second primary indicator is generated based on at least one of a first entity indicator and a second entity indicator, the first entity indicator provides an indication of a reliability of the first entity and the second entity indicator provides an indication of a reliability of the second entity.

[0027] In various embodiments, the system further comprises a computer-readable storage medium having stored therein the overall indicator determined for the transaction or proposed transaction between the first entity and second entity in a database, wherein the overall indicator stored is associated with the first entity and the second entity involved in the transaction or proposed transaction.

[0028] According to a third aspect of the present invention, there is provided a computer program product, embodied in one or more computer-readable storage mediums, comprising instructions executable by one or more computer processors to perform a method of detecting fraud in procurement, the method comprising:

generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction; and

determining a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] Embodiments of the present invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

FIG. 1 depicts a method of detecting fraud in procurement according to various embodiments of the present invention;

FIG. 2 depicts another method of detecting fraud in procurement according to various embodiments of the present invention;

FIG. 3 depicts a schematic drawing of a system for detecting fraud in procurement according to various embodiments of the present invention;

FIG. 4 depicts a schematic drawing of another system for detecting fraud in procurement according to various embodiments of the present invention;

FIG. 5 depicts a schematic drawing of an exemplary computer system;

FIG. 6 depicts a framework architecture based on which a method of detecting fraud in procurement may be implemented according to an example embodiment of the present invention;

FIG. 7 depicts an exemplary implementation of a method of detecting fraud in procurement based on the framework architecture of FIG. 6 according to an example embodiment of the present invention;

FIG. 8 depicts a schematic drawing illustrating an exemplary system implementation for detecting fraud in procurement according to an example embodiment of the present invention; and

FIGs. 9 to 11 depict various screen captures of an exemplary display interfaces that may be generated in a method of detecting fraud in procurement according to various example embodiments of the present invention.

DETAILED DESCRIPTION

[0030] Procurement in organizations or companies generally refers to acquisition of items of goods and/or services from external sources, such as suppliers/vendors. As the

procurement process involves financial operations between different entities/parties (e.g., requester/buyer of an organization and vendor/supplier of the items of goods and/or services), procurement may be prone to fraud where at least one of the entities/parties in transaction benefits at the cost of the organization or company. Similar to other areas of finance, detection of procurement fraud may be supported by computer systems. Conventional solutions in fraud detection or assessment deliver a variety of different approaches, which may rely either on statistical methods or machine learning algorithms. However, such conventional approaches may not deliver a solution capable of covering the complexity of real world organization models/issues, where multiple different types of fraud may occur concurrently. Accordingly, embodiments of the present invention provide a method (computer-implemented method) of detecting fraud in procurement and/or a system thereof that seek to overcome, or at least ameliorate, one or more of the deficiencies of conventional techniques/approaches such as the techniques as mentioned in the background.

[0031] Various embodiments of the present invention provide a technique/method or a framework for combining results of different algorithms, each algorithm configured to detect the presence (e.g., risk or probability) of a respective/corresponding type of anomaly associated with the transaction or proposed transaction in the procurement, into a single output or an overall indicator that summarizes the overall findings on whether the transaction or proposed transaction is subject to fraud. In various embodiments, the overall indicator is expressed as a single numerical value representing a probability that the transaction or proposed transaction is subject to fraud.

[0032] In the context of various embodiments, the term "transaction" may refer to a purchase order or log that has been executed, and the term "proposed transaction" may refer to a purchase order or log that has not yet been executed and/or has not yet been approved, such as by the organization.

[0033] Various embodiments of the present invention provides a technique/method or a framework for procurement data analytics that is capable of detecting procurement patterns at both macro-level and micro-level, and enables easier identification of fraudulent behaviour. Furthermore, besides fraud detection, various embodiments of the

present invention may also be applied to support compliance checking and gleaning insights into improving existing procurement processes.

[0034] FIG. 1 depicts a flow diagram illustrating a method 100 of detecting fraud in procurement according to various embodiments of the present invention. The method 100 comprises a step 102 of generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement. In this regard, each of the plurality of anomaly indicators is generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective/corresponding type of anomaly associated with the transaction or proposed transaction. The method 100 further comprises a step 104 of determining a first primary indicator based on a combination of the plurality of anomaly indicators. In this regard, the first primary indicator provides a collective indication of whether (e.g., probability or risk) the transaction or proposed transaction is subject to fraud based on (e.g., from the point of view of) the types of anomalies being detected.

[0035] In various embodiments, each anomaly indicator may be generated based on a respective/corresponding algorithm or technique configured to provide an indication of the presence of a respective/corresponding type of anomaly associated with the transaction or proposed transaction based on (e.g., analysing or processing) the transactional data associated with the transaction or proposed transaction. For example and without limitation, each anomaly indicator may be expressed as a numerical value representing a probability that the transaction or proposed transaction is subject to the corresponding type of anomaly. In a preferred embodiment, the numerical value may be a single numerical value, and preferably, may be expressed in or normalized to a range from 0 to 1 (or equivalent, such as 0% to 100%), where "0" may indicate that the probability that the transaction or proposed transaction is subject to that corresponding type of anomaly is non-existent or most unlikely (lowest probability), and "1" may indicate that the probability that the transaction or proposed transaction is subject to that corresponding type of anomaly is most likely (highest probability) or holds full confidence.

[0036] In various embodiments, the plurality of anomaly indicators may comprise one or more of an order split indicator, a cut-off rate indicator, and a price deviation

indicator. The order split indicator may provide an indication of the presence of a type of anomaly relating to a purchase order being a result of a purchase order splitting. The cut-off rate indicator may provide an indication of the presence of a type of anomaly relating to a purchase order having a value higher than but close to (e.g., only slight higher than) a predetermined minimum value requiring a purchase order to be subjected to a tender process. It can be understood that the predetermined minimum value may be set by an organization as appropriate based on various factors (e.g., compliance rules) and circumstances. For example and without limitation, a value higher than but close to a predetermined minimum value may be between about 100% to 120%, 100% to 110%, 100% to 105%, 100% to 102%, or 100% to 101% of the predetermined minimum value. It can also be understood that the difference margin considered to be sufficiently close to the predetermined minimum value is not limited to the above-mentioned ranges and may be set as appropriate or as desired based on various factors or circumstances without going beyond the scope of the present invention. The price deviation indicator may provide an indication of the presence of a type of anomaly relating to a purchase order for one or more items having a value deviating from an expected or average value for one or more items included in the purchase order, such as deviating by an amount considered to be suspicious or improper. Similarly, such a deviating amount may be expressed as a percentage of the expected or average value and may set by an organization as appropriate based on various factors and circumstances. The above-mentioned three types of anomaly indicators will be described in further detail later below according to various example embodiments of the present invention. It can be understood that the present invention is not limited to the above-mentioned three types of anomaly indicators which are provided merely by way of examples only, and alternative or additional anomaly indicators generated based on other algorithms or techniques, each configured to provide an indication of the presence of a respective/corresponding type of anomaly associated with the transaction or proposed transaction, may be included as appropriate or desired based on various factors or circumstances without going beyond the scope of the present invention.

[0037] In various embodiments, the first primary indicator is determined based on a weighted sum of the plurality of anomaly indicators. As a result, the first primary

indicator may be a single indicator providing a collective indication of whether (e.g., probability or risk) the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected, such as a numerical value in the range of 0 to 1 representing a probability that the transaction or proposed transaction is subject to fraud. Accordingly, in various embodiments, the sum of the weights respectively assigned to the plurality of anomaly indicators may be equal to 1.

[0038] In various embodiments, the transactional data may be a purchase order data. The purchase order data may comprise a first information/data for identifying the first entity, a second information for identifying the second entity, a third information for providing a description of the transaction or proposed transaction, and a fourth information indicative of at least one value associated with the transaction or proposed transaction. For example, the first entity may be a requester or a buyer associated with the transaction or proposed transaction and the first information may be, for example, the first entity's name and/or identification (ID). The second entity may be the vendor or supplier associated with the transaction or proposed transaction and the second information may be, for example, the second entity's name and/or identification. The third information may provide a description of the transaction or proposed transaction, such item description (e.g., summary of the items involved) and/or identification of the transaction or proposed transaction. It can be understood that the present invention is not limited to the above-mentioned types of information included in the transactional data, and for example, additional information such as the status of the transaction may be included as appropriate or desired based on various factors or circumstances without going beyond the scope of the present invention.

[0039] In various embodiments, the method of detecting fraud in procurement further comprises a step 206 of generating a second primary indicator independent of (i.e., not based on) the transactional data associated with the transaction or proposed transaction, and a step 208 determining an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator, the overall indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on (e.g., from the point of view of) the

plurality of primary indicators. The method with the above additional steps is denoted by reference numeral 200 as shown in the flow diagram of FIG. 2.

[0040] In various embodiments, the second primary indicator is generated based on at least one of a first entity indicator and a second entity indicator. In this regard, the first entity indicator provides an indication of a reliability (e.g., credibility or trustworthiness) of the first entity and the second entity indicator provides an indication of a reliability (e.g., credibility or trustworthiness) of the second entity. In various embodiments, the first entity indicator is generated based on (e.g., by analysing) a history of at least one past transaction involving the first entity, and the second entity indicator is generated based on (e.g., by analysing) a history of at least one past transaction involving the second entity. In various embodiments, the history of at least one past transaction involving the first entity relates to at least the overall indicator of the at least one past transaction involving the first entity, and the history of at least one past transaction involving the second entity relates to at least the overall indicator of the at least one past transaction involving the second entity. That is, in such embodiments, the first entity indicator is generated based on the overall indicator of the at least one past transaction involving the first entity, and the second entity indicator is generated based on the overall indicator of the at least one past transaction involving the second entity. The second primary indicator, along with the first and second entity indicators, will be described in further detail later below according to various example embodiments of the present invention.

[0041] In various embodiments, the second primary indicator may be generated based on a weighted sum of the first entity indicator and the second entity indicator. As a result, the second primary indicator may be a single indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on (e.g., from the point of view of) the first and second entity indicators. In various other embodiments, each of the first and second entity indicators may be expressed or normalized as a numerical value in the range of 0 to 1 (or equivalent, such as 0% to 100%), and the second primary indicator may simply comprise the first and second entity indicators. In various other embodiments, the first entity indicator may be referred to as the second

primary indicator, and the second entity indicator may be referred to as a third primary indicator.

[0042] Furthermore, in various embodiments, the overall indicator may be determined based on a weighted sum of the plurality of primary indicators, such as including the first and second primary indicators, or including the first to third primary indicators as described hereinbefore. As a result, the overall indicator may be a single indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on the plurality of primary indicators, such as a single numerical value in the range of 0 to 1 (or equivalent, such as 0% to 100%) representing a probability that the transaction or proposed transaction is subject to fraud. For example, "0" may indicate that the probability that the transaction or proposed transaction is subject to fraud is non-existent or most unlikely (lowest probability), and "1" may indicate that the probability that the transaction or proposed transaction is subject to fraud is most likely (highest probability) or holds full confidence. In various embodiments, the sum of the weights respectively assigned to the plurality of primary indicators may be equal to 1.

[0043] In various embodiments, the weights assigned to various elements, such as the weight assigned to each anomaly indicator for generating the first primary indicator and the weight assigned to each primary indicator for determining the overall indicator may be selected or determined as appropriate based on various factors or circumstances. For example, a weight may be used to denote or assign a level of importance to an indicator, e.g., a larger weight may be assigned to an indicator that is considered to more important and a smaller weight may be assigned to an indicator that is considered to be less important such that the indicator that is considered to be more important would have a greater effect on (or make a larger contribution to) the resultant indicator obtained. In various embodiments, the weights may be predetermined or may be determined by a user and applied accordingly, such as based on various feedbacks.

[0044] In various embodiments, the overall indicator determined for the transaction or proposed transaction between the first entity and second entity is stored in a database, such as for future reference (e.g.. to enable the history of the past transaction(s) involving the first and second entities to be analysed). In this regard, the overall indicator stored is

associated (e.g., linked/referenced in a data structure) with first entity and the second entity involved in the transaction or proposed transaction. For example, the overall indicator and an identifier (e.g., name or identification) of the associated first and second entities may be stored together in a dataset.

[0045] Accordingly, various embodiments of the present invention provide a data analytics framework, which operates on top of an input dataset composed of transactional data (e.g., purchase order data). In the framework, a single purchase order or log may be a set of information, which describes transaction details between a particular buyer/requester (first entity) and a particular seller/vendor (second entity). A purchase order may relate to a transaction that has already taken place (e.g., has been executed) or may relate to a formal log, which documents a desire to acquire certain goods and/or services (e.g. pending a formal approval within an organization). Therefore, purchase orders may be characterised by a variety of information that identify the buyer/requester (first information), the seller/vendor (second information), the subject/description of transaction (third information), value(s) of the purchase order (fourth information), the status of transaction, and so on. From the perspective of the described framework, the amount or structure/configuration of various features/elements is not constrained or limited in any way. As mentioned hereinbefore, it can be understood that the present invention is not limited to the types of information included in the transactional data, and for example, additional information may be included as appropriate or desired based on various factors or circumstances without going beyond the scope of the present invention.

[0046] Accordingly, various embodiments of the present invention may analyse a dataset of transactional data (e.g., purchase order data) and provide an assessment of those purchase orders with regard to fraud detection. Advantageously, the method of detecting fraud according to various embodiments is based on multiple different points of view/reference such as the assessment or evaluation of the transactional data determined by independent or separate (and possibly concurrently executed) algorithms/technique (e.g., each algorithm/technique for detecting a corresponding type of anomaly associated with the transactional data). The assessment may be performed individually for each purchase order and by each algorithm separately. Depending on the algorithm used, the assessment of fraud suspicion/risk may or may not rely on previous computations of

earlier processed purchased orders. Further points of view may be taken into account in the method such as the assessment or evaluation of the reliability of the buyer/requester and seller/vendor. The above assessments may thus result in an overall indicator, which may also be referred to as a procurement fraud indicator (PFI) or order suspicion indicator (OSI).

[0047] As described hereinbefore, the overall indicator or PFI/OSI may be a quantified measure of fraud suspicion/risk, and may take a value in the range of 0 to 1. Therefore, the overall indicator may be interpreted as a probability measure which denotes the probability of whether a given purchase order (transaction or proposed transaction) is subject to fraud or not. The value of overall indicator may equal to 0 when the fraud probability is non-existent, while may equal to 1 when the algoritrini/technique holds full confidence that a given purchase order is subject to fraud.

[0048] Accordingly, the method of detecting fraud according to various embodiments of the present invention advantageously combines/integrates the results of various different, independent fraud detection algorithms/techniques into a single, final measure of fraud suspicion/risk. In various embodiments, this may be achieved by combining/integrating the results/indicators determined based on various fraud detection algorithms/techniques on multiple tiers of processing, such as the anomaly indicators (which may also interchangeably be referred to as fragmentary indicators) and the primary indicators.

[0049] FIG. 3 depicts a schematic drawing of a system 300 for detecting fraud in procurement according to various embodiments of the present invention. The system 300 comprises an anomaly indicator generator module or circuit 302 configured to generate a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement. Each of the plurality of anomaly indicators is generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction. The system 300 further comprises a first primary indicator determining module or circuit 304 configured to determine a first primary indicator based on a combination of the plurality of anomaly indicators. The first primary indicator provides a collective indication of whether the transaction or proposed

transaction is subject to fraud based on (e.g., from the point of view of) the types of anomalies being detected. The system 300 further comprises a computer processor 306 capable of executing computer executable instructions (e.g., the anomaly indicator generator module 302 and the first primary indicator determining module 304) to perform one or more functions or methods (e.g., to generate an indication of the presence of a corresponding type of anomaly associated with the transaction or proposed transaction), and a computer-readable storage medium 308 communicatively coupled to the processor 306 having stored therein one or more sets of computer executable instructions (e.g., the anomaly indicator generator module 302 and the first primary indicator determining module 304).

[0050] In various embodiments, the system for detecting fraud in procurement may further comprise a second primary indicator generator module or circuit 406 configured to generate a second primary indicator independent of (i.e., not based on) the transactional data associated with the transaction or proposed transaction, and an overall indicator determining module or circuit 408 configured to determine an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator. In particular, the overall indicator provides an overall indication of whether the transaction or proposed transaction is subject to fraud based on (e.g., from the point of view of) the plurality of primary indicators. The system with the above additional modules is denoted by reference numeral 400 in the schematic drawing as shown in FIG. 4.

[0051] In various embodiments, the overall indicator determined for the transaction or proposed transaction between the first entity and second entity is stored in a database in the computer-readable storage medium 308, such as for future reference (e.g., to enable the history of the past transaction(s) involving the first and second entities to be analysed).

[0052] A computing system or a controller or a microcontroller or any other system providing a processing capability can be presented according to various embodiments in the present disclosure. Such a system can be taken to include a processor. For example, as mentioned above, the system 300, 400 described herein each includes a processor (or controller) and a computer-readable storage medium (or memory) which are for example

used in various processing carried out therein as described herein. A memory or computer-readable storage medium used in various embodiments may be a volatile memory, for example a DRAM (Dynamic Random Access Memory) or a non-volatile memory, for example a PROM (Programmable Read Only Memory), an EPROM (Erasable PROM), EEPROM (Electrically Erasable PROM), or a flash memory, e.g., a floating gate memory, a charge trapping memory, an MRAM (Magnetoresistive Random Access Memory) or a PCRAM (Phase Change Random Access Memory).

[0053] In various embodiments, a "circuit" may be understood as any kind of a logic implementing entity, which may be special purpose circuitry or a processor executing software stored in a memory, firmware, or any combination thereof. Thus, in an embodiment, a "circuit" may be a hard-wired logic circuit or a programmable logic circuit such as a programmable processor, e.g. a microprocessor (e.g. a Complex Instruction Set Computer (CISC) processor or a Reduced Instruction Set Computer (RISC) processor). A "circuit" may also be a processor executing software, e.g. any kind of computer program, e.g. a computer program using a virtual machine code such as e.g. Java. Any other kind of implementation of the respective functions which will be described in more detail below may also be understood as a "circuit" in accordance with various alternative embodiments. Similarly, a "module" may be a portion of a system according to various embodiments in the present invention and may encompass a "circuit" as above, or may be understood to be any kind of a logic-implementing entity therefrom.

[0054] Some portions of the present disclosure are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0055] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as "computing", "encrypting", "decrypting", "determining", "replacing", "generating", "initializing", "outputting", or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0056] The present specification also discloses a system or an apparatus for performing the operations/functions of the methods described herein. Such a system or apparatus may be specially constructed for the required purposes, or may comprise a general purpose computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms presented herein are not inherently related to any particular computer or other apparatus. Various general purpose machines may be used with computer programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate.

[0057] In addition, the present specification also at least implicitly discloses a computer program or software/functional module, in that it would be apparent to the person skilled in the art that the individual steps of the methods described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention. It will be appreciated to a person skilled in the art that various modules described herein (e.g., the anomaly indicator generator module 302 and/or the first primary indicator determining module 304) may be software module(s) realized by computer program(s) or set(s) of instructions executable by a computer processor to perform the required functions, or may be hardware module(s) being

functional hardware unit(s) designed to perform the required functions. It will also be appreciated that a combination of hardware and software modules may be implemented.

[0058] Furthermore, one or more of the steps of the computer program/module or method may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a general purpose computer. The computer program when loaded and executed on such a general-purpose computer effectively results in an apparatus that implements the steps of the methods described herein.

[0059] In various embodiments, there is provided a computer program product, embodied in one or more computer-readable storage mediums (non-transitory computer-readable storage medium), comprising instructions (e.g., the anomaly indicator generator module 302 and/or the first primary indicator determining module 304) executable by one or more computer processors to perform a method 100 of detecting fraud in procurement as described hereinbefore with reference to FIG. 1 or other method(s) described herein. Accordingly, various computer programs or modules described herein may be stored in a computer program product receivable by a computer system or electronic device (e.g., system 300 or 400) therein for execution by a processor of the computer system or electronic device to perform the respective functions.

[0060] The software or functional modules described herein may also be implemented as hardware modules. More particularly, in the hardware sense, a module is a functional hardware unit designed for use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an Application Specific Integrated Circuit (ASIC). Numerous other possibilities exist. Those skilled in the art will appreciate that the software or functional module(s) described herein can also be implemented as a combination of hardware and software modules.

[0061] The methods or functional modules of the various example embodiments as described hereinbefore may be implemented on a computer system, such as a computer system 500 as schematically shown in FIG. 5 as an example only. In other words, it can be appreciated that the system 300, 400 may be realized by a computer

system. The method or functional module may be implemented as software, such as a computer program being executed within the computer system 500, and instructing the computer system 500 to conduct the method of various example embodiments. The computer system 500 may comprise a computer module 502, input modules such as a keyboard 504 and mouse 506 and a plurality of output devices such as a display 508, and a printer 510. The computer module 502 may be connected to a computer network 512 via a suitable transceiver device 514, to enable access to e.g. the Internet or other network systems such as Local Area Network (LAN) or Wide Area Network (WAN). The computer module 502 in the example may include a processor 518 for executing various instructions, a Random Access Memory (RAM) 520 and a Read Only Memory (ROM) 522. The computer module 502 may also include a number of Input/Output (I/O) interfaces, for example I/O interface 524 to the display 508, and I/O interface 526 to the keyboard 504. The components of the computer module 502 typically communicate via an interconnected bus 528 and in a manner known to the person skilled in the relevant art.

[0062] It will be appreciated to a person skilled in the art that the terminology used herein is for the purpose of describing various embodiments only and is not intended to be limiting of the present invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0063] In order that the present invention may be readily understood and put into practical effect, various example embodiments of the present invention will be described hereinafter by way of examples only and not limitations. It will be appreciated by a person skilled in the art that the present invention may, however, be embodied in various different forms or configurations and should not be construed as limited to the example embodiments set forth hereinafter. Rather, these example embodiments are provided so

that this disclosure will be thorough and complete, and will fully convey the scope of the present invention to those skilled in the art.

[0064] FIG. 6 depicts a framework architecture based on which a method of detecting fraud in procurement may be implemented according to an example embodiment of the present invention, and will now be described below.

Framework Architecture Components

Primary Indicators

[0065] Primary indicators may present an aggregated fraud suspicion/risk overview for a purchase order. For example, the framework architecture may define three scopes/types of such an upper-level or top-level overview (e.g., Tiers 2 to 4 shown in FIG. 6). In the example embodiment, the three types of primary indicators may include:

- overview of all aspects of a purchase order (Order Suspicion Indicator (OSI));
- overview of other orders (e.g., previous orders) related to purchase order being analysed (Order History Indicators (OHI)); and
- overview of the purchase order data (e.g., metadata) being analysed (Order Suspicion Indicator Base (OSIB)).

[0066] In various embodiments, all primary indicators may operate on information/results that were produced during earlier stages of framework operation rather than raw purchase order data (i.e., data of the purchased order being analysed for fraud detection), for example, results derived from underlying fragmentary/anomaly indicators or previously computed primary indicators or OSI. In the context of various embodiments, for clarity and ease of reference, the final indicator (e.g., OSI) such as in Tier 4 shown in FIG. 6 may be referred to as an overall indicator instead of a primary indicator so as to differentiate from the primary indicators in lower tiers such as in Tiers 2 and 3 shown in FIG. 6.

Fragmentary Indicators (or Anomaly Indicators)

[0067] A fragmentary indicator may represent analysis of a purchase order focusing on a particular aspect of fraud or a specific fraud pattern. For example, such an indicator may not deliver exhaustive information but provides an analysis of a specific

fragment/aspect of information related to purchase order (e.g., order split indicator, cut-off rate indicator, and price deviation indicator). In various embodiments, fragmentary indicators are introduced in the framework architecture to advantageously decompose the approach/solution to fraud detection into sub-problems/factors, which may be resolved independently and concurrently.

[0068] It will be appreciated that the framework architecture is not limited to any number of fragmentary indicators, and may incorporate additional indicators) (e.g., configured or customised for analysing the purchase order data to detect a particular type of anomaly). Such additional fragmentary indicators) will be captured in one of the primary indicators (e.g., the first primary indicator as described hereinbefore) that is determined based on a combination of the plurality of fragmentary indicators (e.g., the first primary indicator may aggregate information from the plurality of fragmentary indicators).

Analytics

[0069] An analytics component may be provided in the framework architecture for implementing a feedback loop and provides the framework architecture with additional input(s) for computing the primary and/or fragmentary indicators. For example, the feedback may originate from the user of the framework architecture (e.g. a procurement officer) or be automated algorithmic solution reactive to the Order Suspicion Indicator values and invisible for (unnoticeable by) the end user. For example, as described hereinbefore, the OSI generated may be stored in the procurement database, and an algorithm for computing an entity indicator may be reactive to such an OSI generated in providing an indication of the reliability of the entity.

[0070] In various embodiments, the feedback information (e.g., OSI determined) may also be utilised to adjust/configure the weights of various aggregation functions (e.g., when determining the first primary indicator or when determining the overall indicator (e.g., OSI being determined)) and other possible parameters in the primary and fragmentary indicator computations as appropriate.. Accordingly, rather than being static, the framework architecture may advantageously have a continuously self-learning ability.

Procurement Database

[0071] The bottom layer of framework architecture provides access to raw data of procurement purchase orders captured, for example, as already exist or being stored in a variety of procurement management systems. It will be appreciated that the framework architecture does not put any requirements or constraints regarding compatible procurement systems. However, data access component may be needed in order to perform indicator computations, which base their processing on raw data (purchase order data captured).

[0072] In various embodiments, the framework architecture includes a computer-readable storage medium (e.g., **308** as shown in FIGs. **3** and 4) and the procurement database may be stored in the computer-readable storage medium. Furthermore, various procurement fraud indicators determined/generated as described herein may be stored in the computer-readable storage medium for future reference. For example, the Order History Indicator for an entity may then to determined based on the Order Suspicion Indicators stored for previous purchase orders for the entity.

Exemplary Framework Operation Flow and Indicator Calculation/Computation

[0073] In various embodiments, the procurement fraud indicators may be calculated in a processing flow comprising four tiers as shown in FIG. **6,** with data processing starting at Tier **1** and ending at Tier 4:

Tier **1** (Fragmentary Indicators / Anomaly Indicators)

[0074] The lowest tier (Tier **1)** may involve the execution of all algorithms included in the framework for computing all of the fragmentary indicators. The computations performed at this stage is based on the purchase order data (transactional data or metadata) being analysed. The computations of exemplary fragmentary indicators will be described later below by way of examples only for illustration purpose. For example, the computations may involve a comparison of various element(s) of the purchase order data being analysed with certain reference information (e.g., the remaining purchase orders from the dataset or certain reference indicators).

Tier 2 (Order Suspicion Indicator Base)

[0075] Tier 2, an intermediate tier, may rely on the results from Tier 1 in order to combine the results of the fragmentary indicators into a single probability value denoting the collective suspicion assessment related to the purchase order data being analysed. The combination of the fragmentary indicators may be performed using various aggregation functions, e.g., weighted addition/summation, average, maximum, minimum, and so on, as appropriate or desired such as based on the requirements of the framework adopter.

Tier 3 (Order History Indicators)

[0076] Tier 3, an intermediate tier, may analyse the history of entities involved in the purchase order (transaction or proposed transaction), such as past indicators associated with the entities (e.g., past Order Suspicion Indicators of purchase orders related to a requester/buyer). For example, in contrast to the previous tiers, Tier 3 may not involve a comparative study of the purchase order data being analysed with reference information (i.e., is independent of the purchase order data being analysed) but glimpse into past indicators associated with the entity of interest (e.g., indicators previously computed for the entity of interest for other orders).

Tier 4 (Order Suspicion Indicator)

[0077] Tier 4, a final tier, may aggregate all the primary indicators (e.g., primary indicator values from Tier 2 and Tier 3). Tier 4 involves combining all the computed primary indicators and presents an overall indication of whether the transaction or proposed transaction is subject to fraud as a signal fraud suspicion probability value (e.g., rank/rating), via various aggregation functions, such as weighted additional/summation. In the various aggregation functions, various weights may be assigned to the primary indicators from Tiers 2 and 3 and to, for example, set or rank their importance in the final Order Suspicion Indicator (overall indicator).

Exemplary Usage Illustration

[0078] As shown in FIG. 6, the framework architecture introduces a number of configurable and extensible elements/features, such as any number of fragmentary

indicators 1, 2, ... N, and any number of order history indicators 1, 2 ... N, as appropriate or desired. Therefore, it will be appreciated to a person skilled in the art that the framework architecture can be implemented in a number of ways. By way of example only and for illustration purpose, FIG. 7 illustrates an exemplary implementation that involves three types of fragmentary/anomaly indicators (namely, order split indicator, cut-off rate indicator, and price deviation indicator) and two types of order history indicators (namely, requester suspicion indicator and vendor suspicion indicator), and will now be described below.

Fragmentary/Anomaly Indicators (Tier 1)

[0079] In the exemplary implementation, the following three fragmentary indicators are generated:

[0080] 1) Order Split Indicator (OSPI) - provides an indication of the presence of a type of anomaly relating to a purchase order being a result of a purchase order splitting. For example, the OSPI may indicate the probability that selected transaction x is involved in requester splitting a bigger purchase into smaller purchases, and may be determined using the following equation:

$$OSPI(x) = \frac{similarTransactionCount(x)-1}{TC_{max}+STC_{min}} \quad \text{(Equation 1)}$$

where: similarTransactionCount(x) is the number of neighbouring transactions of purchase order x which are detected as similar (e.g. same vendor and similar item descriptions); TC_{max} is the maximal number of similarTransactionCount(x) for all orders in the entire dataset; and STC_{min} is a constant value which defines a minimum similar transaction count for an order group (group of purchase orders) to be recognized/considered as suspicious (Suspicious Transaction Count).

[0081] 2) Cut-off Rate Indicator (CRI) - provides an indication of the presence of a type of anomaly relating to a purchase order having a value higher than but close to a minimal predetermined value requiring a purchase order to be subjected to a tender process. For example, CRI may indicate if a given transaction x is suspiciously close to the limit for an un-tendered order, and may be determined using the following equation:

$$CRI(\_x) = 1 - \left|\frac{orderValue\{x\}-tenderLowerRange}{tender\ LowerRange}\right| \quad \text{(Equation 2)}$$

where: orderValue(x) is the value of order x; and tenderLowerRange is a minimum order value as predefined in an organization which obliges the purchase order requester to make a tender rather than regular purchase without making a tender.

[0082] Price Deviation Indicator (PDI) - provides an indication of the presence of a type of anomaly relating to a purchase order for one or more times having a value deviating from an expected or average value for the one or more items included in the purchase order. For example, PDI may indicate if a transaction *x* value is suspiciously far from the average transaction value for an item *y*, and may be determined using the following equation:

$$PDI(x) = \left| \frac{itemUnitValue(x) - averageItemUnitValue(x)}{averageItemUnitValue(x)} \right| \quad \text{(Equation 3)}$$

where: itemUnitValue(x) is the unit value of the item *y* being subject of the order; and averageItemUnitValue(x) is the average unit value of the same item *y* from other orders in the dataset involving that itemj.

Primary Indicators (Tiers 2 and 3)

[0083] In the exemplary implementation, the following three primary indicators are generated:

[0084] 1) Order Suspicion Indicator Base (OSIB) - provides a collective indication of whether the purchase order is subject to fraud based on the types of anomalies being detected (in the exemplary implementation, the above-mentioned three types of anomalies). For example, the OSIB may be computed based on a weighted sum of the fragmentary indicators using the following equation (assuming the above-mentioned three types of fragmentary indicators):

$$OSIB(x) = OSPI(x) * weight_{OS'} + PDI(x) * weight_{PDI} + CRI(x) * weight_{CRI} \quad \text{(Equation 4)}$$

where: $weight_{xyz}$ is a value between 0 and 1 denoting the importance of a particular fragmentary indicator for the end result (e.g., OSIB or OSI). In the exemplary implementation, the sum of all the weights used for all the indicators is equal to 1.

[0085] 2) Requester Suspicion Indicator (RSI) - provides an indication of a reliability of the requester, such as, based on the requester's purchasing history. For example, the

RSI may indicate the probability for the requester to be involved in a suspicious transaction, and may be determined using the following equation:

$$RSI(x,t) = \frac{\sum_{x=1}^{yOrdersByRequester(x,t)} OSI(x)}{ordersByRequester(x,t)} \quad \text{(Equation 5)}$$

where: ordersByRequester(x,t) is the number of purchase orders made by the same requester (examined/processed purchase order "x") up until certain time "t".

[0086] 3) Vendor Suspicion Indicator (VSI) - provides an indication of a reliability of the vendor, such as, based on the vendor's purchasing history. For example, the VSI may indicates the probability for vendor to be involved in a suspicious transaction, and may be determined using the following equation:

$$VSI(x,t) = \frac{\sum_{x=1}^{yOrdersByVendor(x,t)} OSI}{ordersByVendor(x,t)} \quad \text{(Equation 6)}$$

where: ordersByVendor(x,t) is the number of purchase orders made involving the same vendor (examined/processed purchase order "x") up until certain time "t".

[0087] Once all the primary indicators (e.g., in Tiers 2 and 3) have been generated, the overall indicator (OSI) may then be computed based on the primary indicators to provide an overall indication of whether the purchase order being analysed is subject to fraud based on the plurality of primary indicators. For example, the OSI may be computed based on a weighted sum of all the primary indicators (assuming the above-mentioned three primary indicators) using the following equation:

$$OSI(x) = OSIB(x) * weight_{OSIB} + RSI(x, t-1) * weight_{RSI} + VSI(x, t-1) * weight_{VS}, \quad \text{(Equation 7)}$$

Exemplary purchase order data and computations

[0088] As an example only and for illustration purpose, Table 1 below illustrates an exemplary dataset for multiple purchase orders (transaction data for multiple purchase orders).

ID	DATE	ITEM	REQUESTER	VENDOR	VALUE
1	2011/04/05	X	R1	V1	$100
2	2011/04/06	Y	R1	V1	$200
3	2011/04/07	Z	R2	V1	$50
4	2011/05/01	K	R3	V1	$49.99
5	2011/05/03	X	R1	V2	$1099

6	201 1/05/03	X	R1	V2	$1099
7	201 1/05/03	X	R1	V2	$1099
8	201 1/05/03	X	R1	V2	$1099

Table 1—Exemplary dataset including raw data for multiple purchase orders

[0089] Accordingly, based on the above-mentioned techniques/equations, the fraud indicators shown in Table 2 below may be generated/computed based on the dataset shown in Table 1 above-

ID	OSI	OSIB	RSI(t-1)	VSI(t-1)	OSPI	PDI	CRI
1	0.1424	0.178	0	0	0	0.89	0
2	0.028	0	0.1424	0.1424	0	0	0
3	0.00852	0	0	0.0852	0	0	0
4	0.24937	0.3	0	0.04686	0	0	1
5	0.40052	0.49	0.0852	0	0.3	0.2	1
6	0.45634	0.49	0.24286	0.40052	0.3	0.2	1
7	0.4698	0.49	0.3496	0.42843	0.3	0.2	1
8	0.47788	0.49	0.4097	0.4491	0.3	0.2	1

Table 2—Exemplary fraud indicators generated based on the dataset shown in Table 1

[0090] In the above examples, for example, the indicators OSI and OSIB were derived based on the following equations:

$$OSI(x) = OSIB(x) * 0.8 + RSI(x, t - 1) * 0.1 + VSI(x, t - 1) * 0.1 \quad \text{(Equation 8)}$$

$$OSIB(x) = OSPI(x) * 0.5 + PDI(x) * 0.2 + CRI(x) * 0.3, \quad \text{(Equation 9)}$$

where STC = 10 (Order Split Indicator)

[0091] From Equation 8, it can be observed that weights of 0.8, 0.1, and 0.1 were assigned to OSIB, RSI and VSI, respectively, and from Equation **9,** it can be observed that weights of 0.5, 0.2, and 0.3 were assigned to OSPI, PDI and CRI, respectively.

[0092] In various embodiments, the data analytics framework (procurement fraud analytics framework) may be incorporated into a larger analytics system, for example, where the framework may work as a service provider analysing input dataset (comprising transactional data) and outputting results of procurement fraud suspicion/risk analysis according to various embodiments of the present invention as described herein. For example, the framework may be implemented as a library or a software service in a

computer system. As such, it can communicate with other applications and provide functionalities for fraud suspicion/risk analysis. In this regard, FIG. 8 illustrates an exemplary implementation 800 of such a system according to an example embodiment of the present invention, where the procurement analytics framework may be accessed via APIs (Application Programmable Interfaces) to compute procurement fraud indicators on demand and return the results of the analysis to the main application.

[0093] In various embodiments, the framework may be accessed in multiple ways depending on application requirements at a given time, such as:

1) Continuous computation of procurement fraud indicators for new purchase orders in the procurement system - the Database (DB) Inspector component 804 of the external system monitors the Procurement Database 802 (having stored therein purchase order data (transactional data)) and invokes the Procurement Analytics Framework 812 in the API library 810 via Task Dispatcher component 806 upon creation of new purchase orders. In this manner, the output of the framework may not be noticed or visible for the end user and the data delivered by the framework may synergize with the procurement database 802.

2) Configurable on-demand indicator calculation - the framework may be invoked to compute procurement fraud indicators in a customized way using the weights feature described hereinbefore. The weights may be modifiers applicable at various tiers of the framework. The weights may for example be altered by the end-user and passed to the framework, e.g., during runtime if the external application provides such a support.

[0094] FIGs. 9 to 11 show various screen captures 900, 910, 920 of an exemplary display interface that may be generated in a method of detecting fraud in procurement according to various example embodiment of the present invention for illustration purpose only and without limitation. The screen captures illustrate various non-limiting ways indicators generated according to various embodiments of the present invention may be presented to a user. For example, as shown in FIG. 9, new purchase orders may scanned/analysed as they are inputted into the procurement database and various procurement fraud indicators (under SuspicionRank) for the purchase orders may be shown to provide an indication (e.g., likelihood or probability) of whether the corresponding purchase order may be subject to fraud. Other information, such as the

date, item description, the vendor's identification, the requestor's identification, the requester's department, and the value of the purchase order may also be shown to provide a complete overview. From FIGs. 9 to 11, it can be seen that the indicators generated advantageously enable fraud suspicion/risk to be quickly and effectively detected such that, for example, appropriate action(s) may be taken for a transaction or proposed transaction detected to be subject to fraud.

[0095] While embodiments of the invention have been particularly shown and described with reference to specific embodiments, it should be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced.

CLAIMS

What is claimed is:

1. A computer-implemented method of detecting fraud in procurement, the method comprising:

generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction; and

determining a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected.

2. The method according to claim 1, wherein the first primary indicator is determined based on a weighted sum of the plurality of anomaly indicators.

3. The method according to claim 2, wherein the sum of the weights respectively assigned to the plurality of anomaly indicators is equal to 1.

4. The method according to any one of claims 1 to 3, wherein the plurality of anomaly indicators comprises one or more of an order split indicator, a cut-off rate indicator, and a price deviation indicator, wherein:

the order split indicator provides an indication of the presence of a type of anomaly relating to a purchase order being a result of a purchase order splitting,

the cut-off rate indicator provides an indication of the presence of a type of anomaly relating to a purchase order having a value higher than but close to a

minimal predetermined value requiring a purchase order to be subjected to a tender process, and

the price deviation indicator provides an indication of the presence of a type of anomaly relating to a purchase order for one or more items having a value deviating from an expected or average value for the one or more items included in the purchase order.

5. The method according to any one of claims 1 to 4, wherein the transactional data is a purchase order data, the purchase order data comprising a first information for identifying the first entity, a second information for identifying the second entity, a third information for providing a description of the transaction or proposed transaction, and a fourth information indicative of at least one value associated with the transaction or proposed transaction.

6. The method according to any one of claims 1 to 5, further comprising:

generating a second primary indicator independent of the transactional data associated with the transaction or proposed transaction; and

determining an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator, the overall indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on the plurality of primary indicators.

7. The method according to claim 6, wherein the overall indicator is determined based on a weighted sum of the plurality of primary indicators.

8. The method according to claim 6 or 7, wherein the second primary indicator is generated based on at least one of a first entity indicator and a second entity indicator, the first entity indicator provides an indication of a reliability of the first entity and the second entity indicator provides an indication of a reliability of the second entity.

9. The method according to claim 8, wherein the first entity indicator is generated based on a history of at least one past transaction involving the first entity, and/or the second entity indicator is generated based on a history of at least one past transaction involving the second entity.

10. The method according to claim 9, wherein the history of at least one past transaction involving the first entity relates to at least the overall indicator of the at least one past transaction involving the first entity, and/or the history of at least one past transaction involving the second entity relates to at least the overall indicator of the at least one past transaction involving the second entity.

11. The method according to claim 9 to 10, wherein the second primary indicator is generated based on a weighted sum of the first entity indicator and the second entity indicator.

12. The method according to any one of claims 6 to 11, wherein the collective indication and/or the overall indication of whether the transaction or proposed transaction is subject to fraud is expressed as a single numerical value representing a probability that the transaction or proposed transaction is subject to fraud.

13. The method according to any one of claims 6 to 12, further comprises storing the overall indicator determined for the transaction or proposed transaction between the first entity and second entity in a database, wherein the overall indicator stored is associated with the first entity and the second entity involved in the transaction or proposed transaction.

14. The method according to any one of claims 1 to 13, wherein the first entity is a requester or buyer associated with the transaction or proposed transaction, and the

second entity is the vendor or supplier associated with the transaction or proposed transaction.

15. A system for detecting fraud in procurement, the system comprising:

an anomaly indicator generator module configured to generate a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction; and

a first primary indicator determining module configured to determine a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected.

16. The system according to claim 15, wherein the first primary indicator is generated based on a weighted sum of the plurality of anomaly indicators.

17. The system according to claim 15 or 16, further comprising:

a second primary indicator generator module configured to generate a second primary indicator independent of the transactional data associated with the transaction or proposed transaction; and

an overall indicator determining module configured to determine an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator, the overall indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on the plurality of primary indicators.

18. The system according to claim 17, wherein the second primary indicator is generated based on at least one of a first entity indicator and a second entity

indicator, the first entity indicator provides an indication of a reliability of the first entity and the second entity indicator provides an indication of a reliability of the second entity.

19. The system according to claim 17 or 18, further comprises a computer-readable storage medium having stored therein the overall indicator determined for the transaction or proposed transaction between the first entity and second entity in a database, wherein the overall indicator stored is associated with the first entity and the second entity involved in the transaction or proposed transaction.

20. A computer program product, embodied in one or more computer-readable storage mediums, comprising instructions executable by one or more computer processors to perform a method of detecting fraud in procurement, the method comprising:

generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction; and

determining a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected.

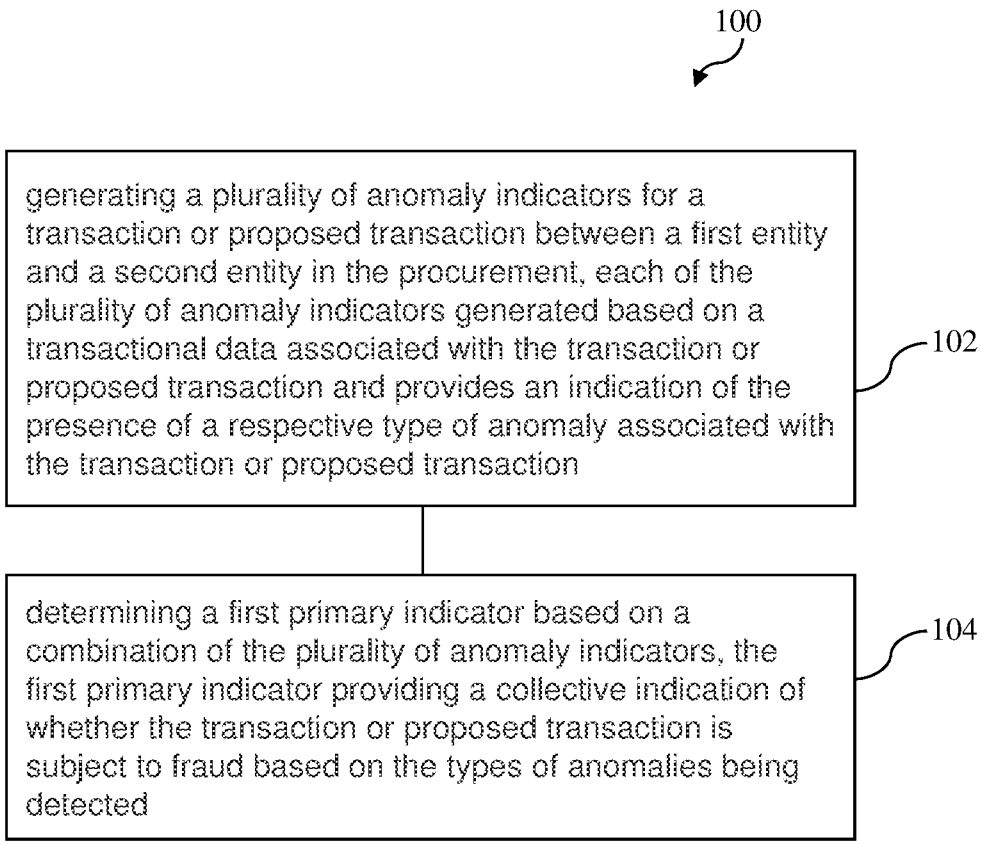
100
generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction
102
determining a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected
104

FIG. 1

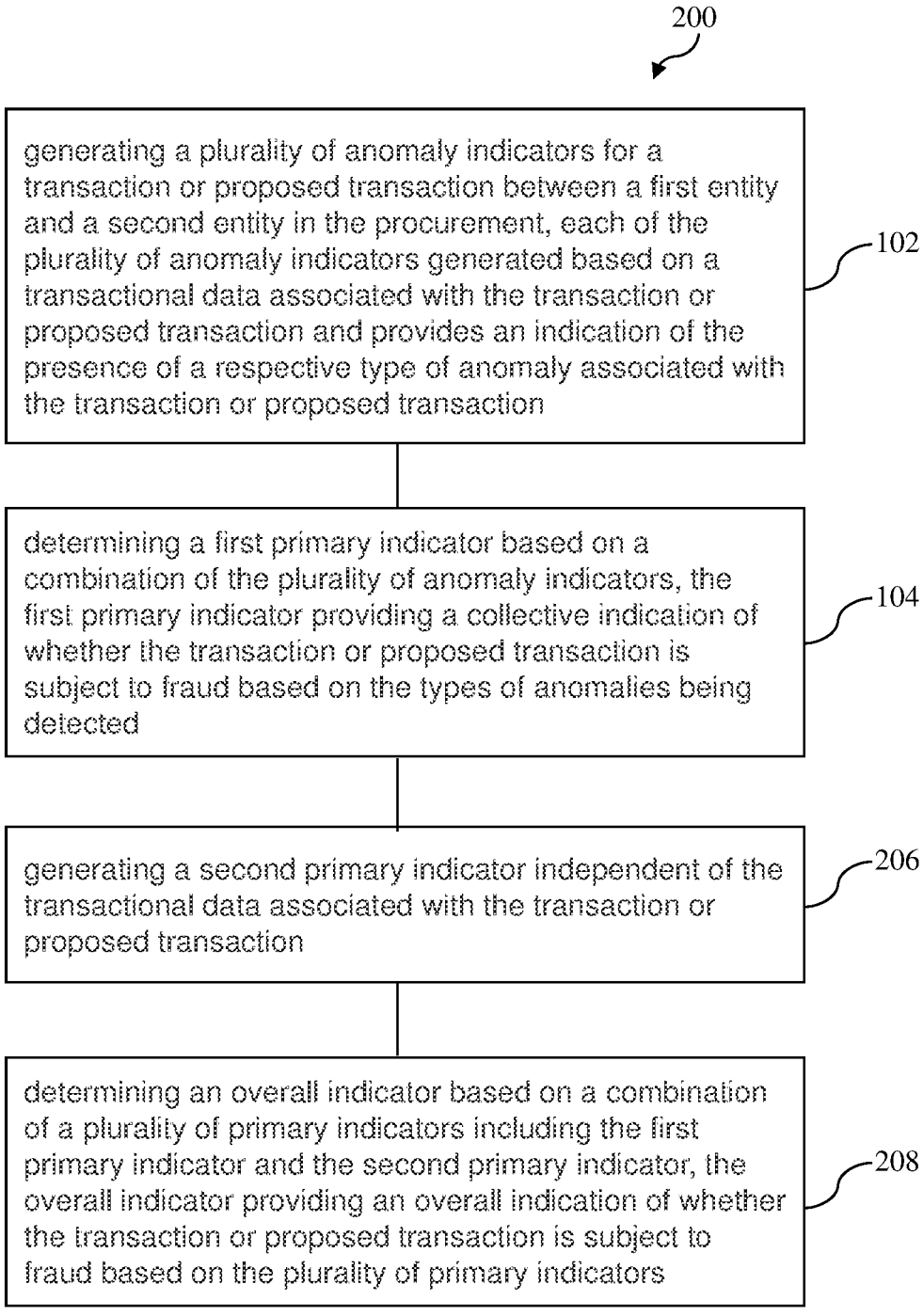
200
generating a plurality of anomaly indicators for a transaction or proposed transaction between a first entity and a second entity in the procurement, each of the plurality of anomaly indicators generated based on a transactional data associated with the transaction or proposed transaction and provides an indication of the presence of a respective type of anomaly associated with the transaction or proposed transaction
102
determining a first primary indicator based on a combination of the plurality of anomaly indicators, the first primary indicator providing a collective indication of whether the transaction or proposed transaction is subject to fraud based on the types of anomalies being detected
104
generating a second primary indicator independent of the transactional data associated with the transaction or proposed transaction
206
determining an overall indicator based on a combination of a plurality of primary indicators including the first primary indicator and the second primary indicator, the overall indicator providing an overall indication of whether the transaction or proposed transaction is subject to fraud based on the plurality of primary indicators
208

FIG. 2

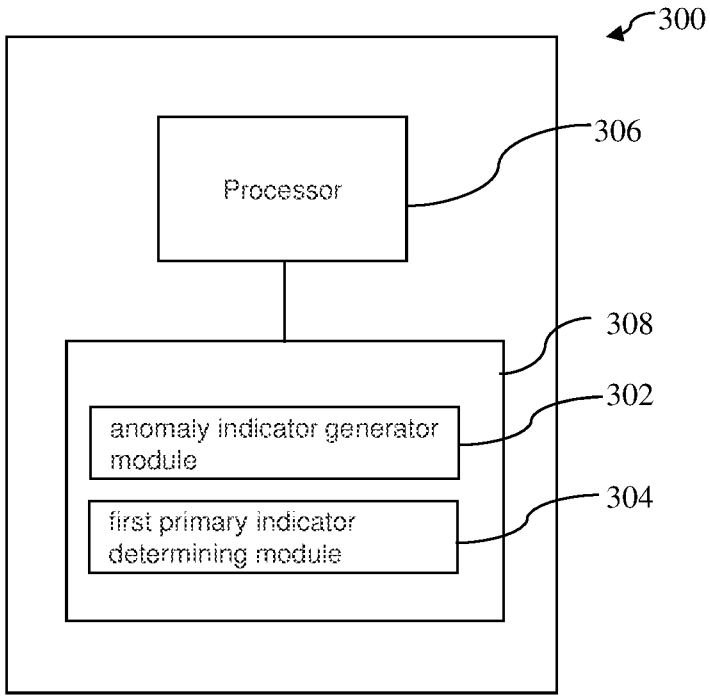
300
Processor
306
308
anomaly indicator generator module
302
first primary indicator determining module
304

FIG. 3

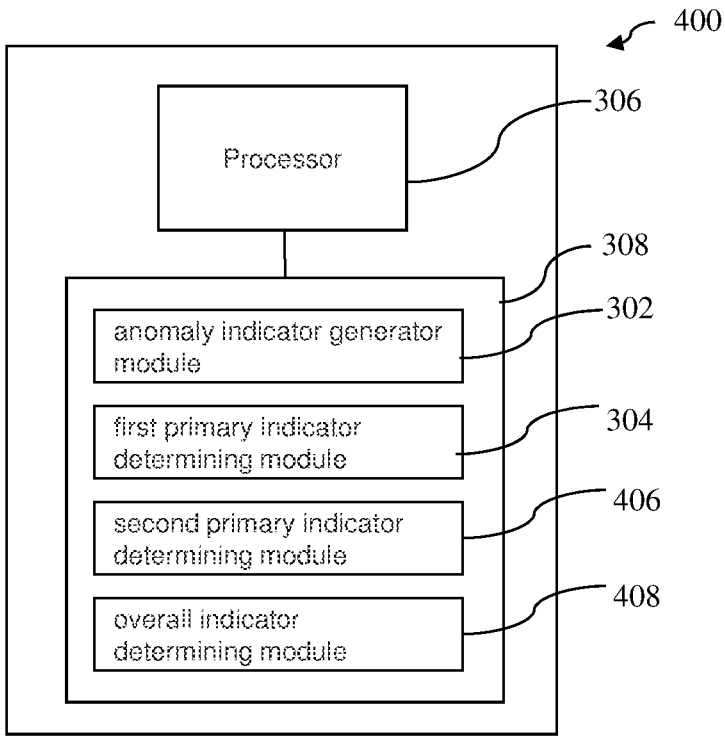
400
Processor
306
308
anomaly indicator generator module
302
first primary indicator determining module
304
second primary indicator determining module
406
overall indicator determining module
408

FIG. 4

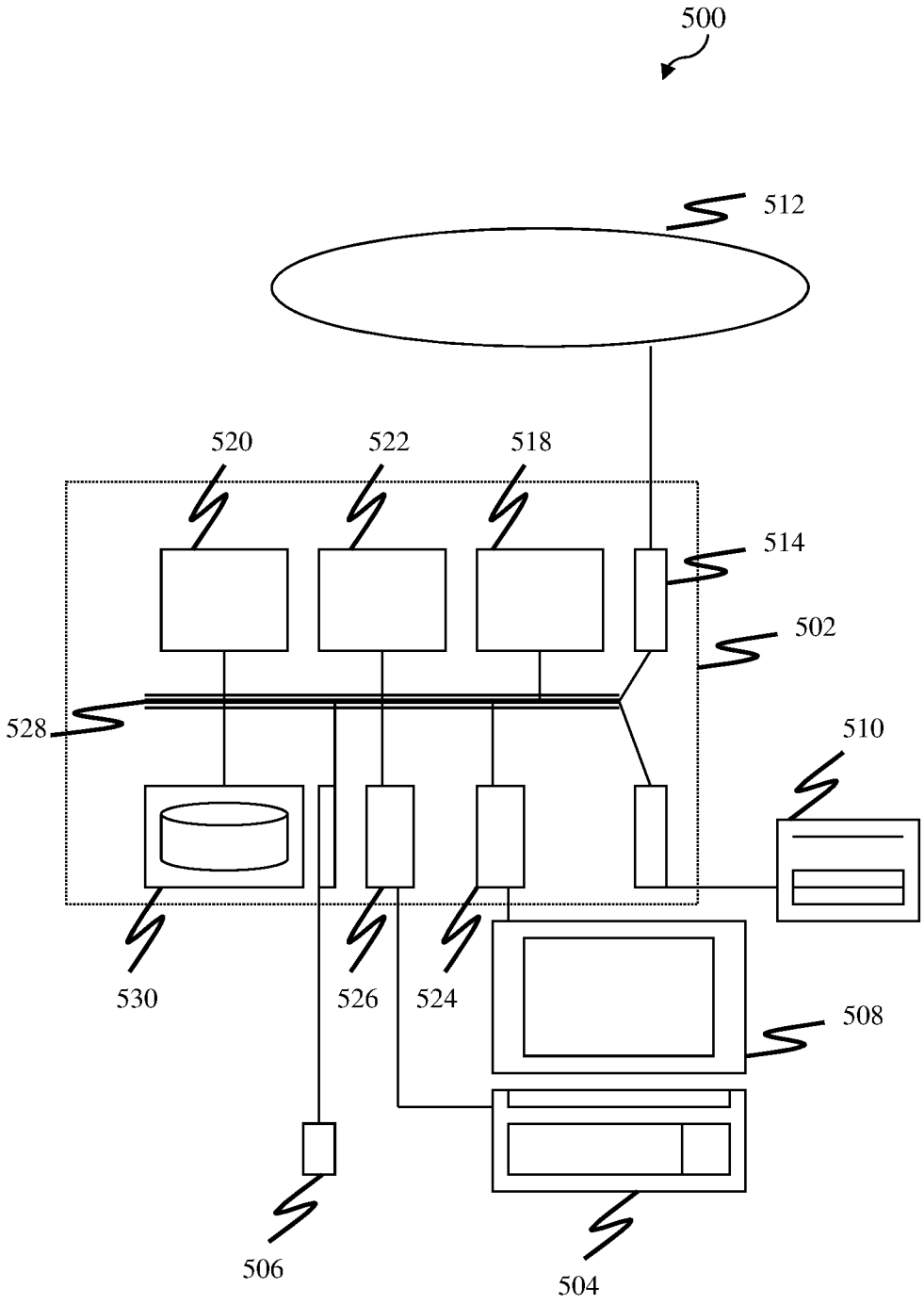

FIG. 5

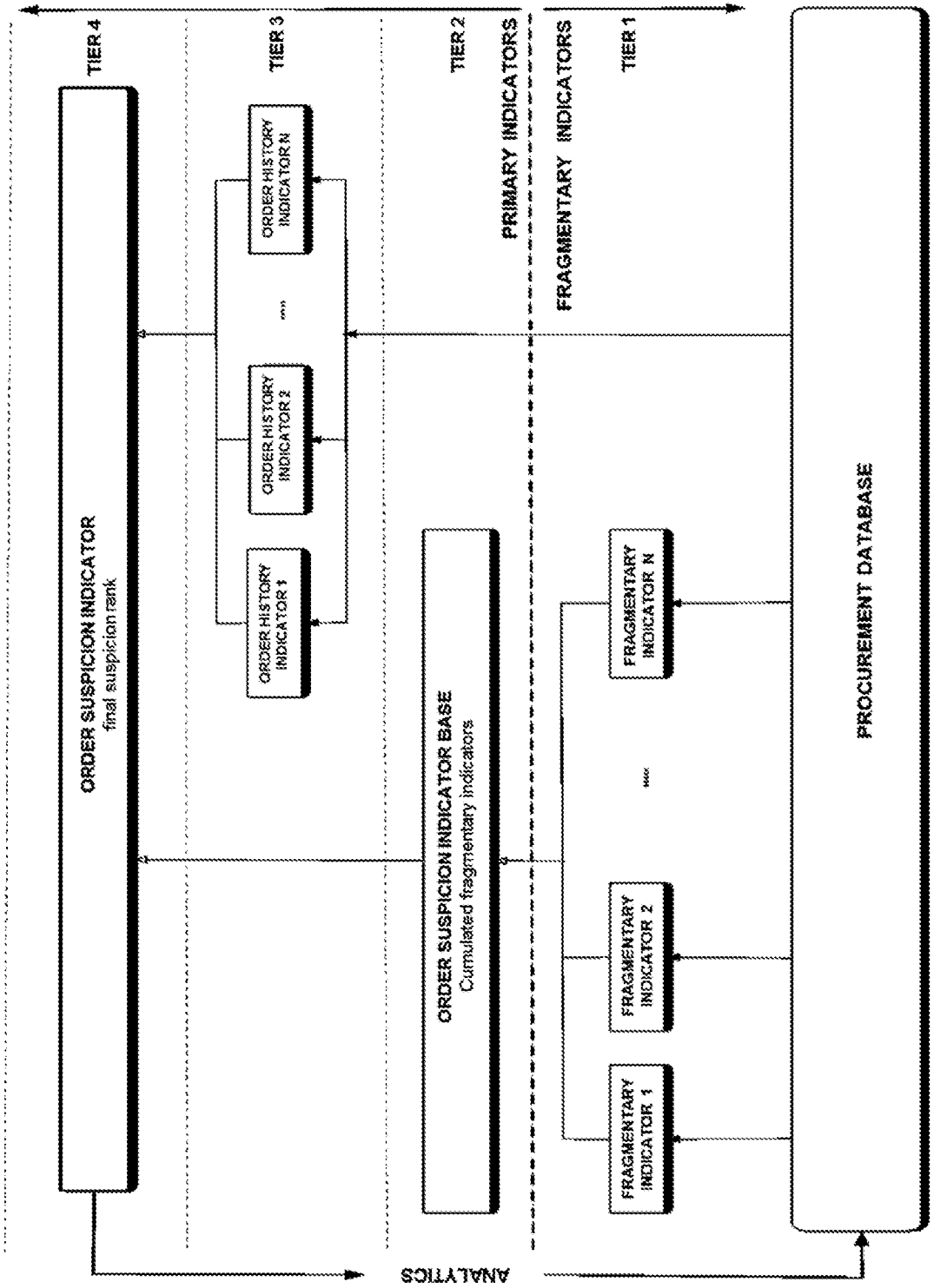
TIER 4
TIER 3
TIER 2
TIER 1
PRIMARY INDICATORS
FRAGMENTARY INDICATORS
ORDER SUSPICION INDICATOR
final suspicion rank
ORDER HISTORY INDICATOR 1
ORDER HISTORY INDICATOR 2
ORDER HISTORY INDICATOR N
ORDER SUSPICION INDICATOR BASE
Cumulated fragmentary indicators
FRAGMENTARY INDICATOR 1
FRAGMENTARY INDICATOR 2
FRAGMENTARY INDICATOR N
PROCUREMENT DATABASE
ANALYTICS

FIG. 6

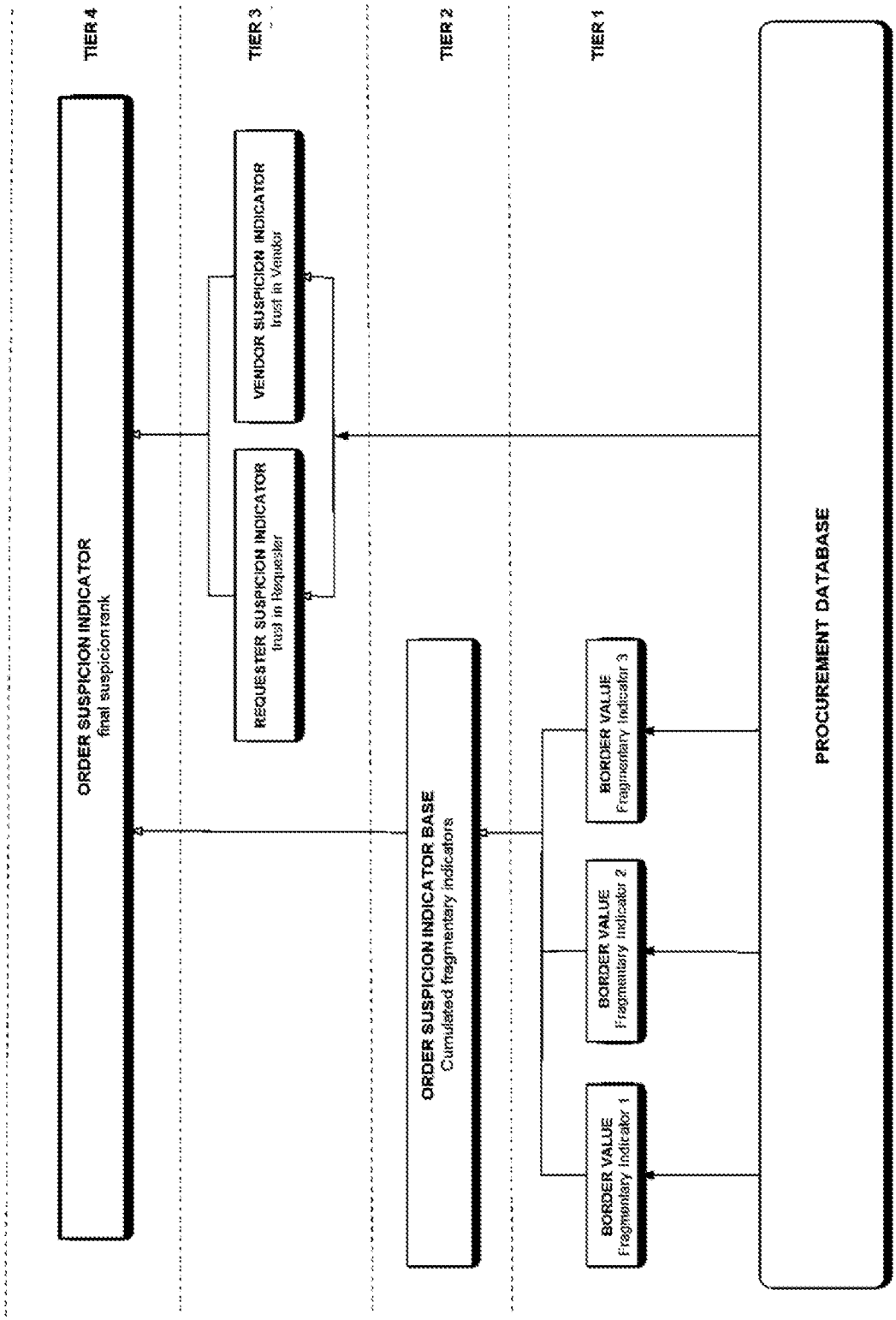
TIER 4
TIER 3
TIER 2
TIER 1
ORDER SUSPICION INDICATOR
final suspicionrank
VENDOR SUSPICION INDICATOR
trust in Vendor
REQUESTER SUSPICION INDICATOR
trust in Requester
ORDER SUSPICION INDICATOR BASE
Cumulated fragmentary indicators
BORDER VALUE
Fragmentary indicator 3
BORDER VALUE
Fragmentary indicator 2
BORDER VALUE
Fragmentary indicator 1
PROCUREMENT DATABASE

FIG. 7

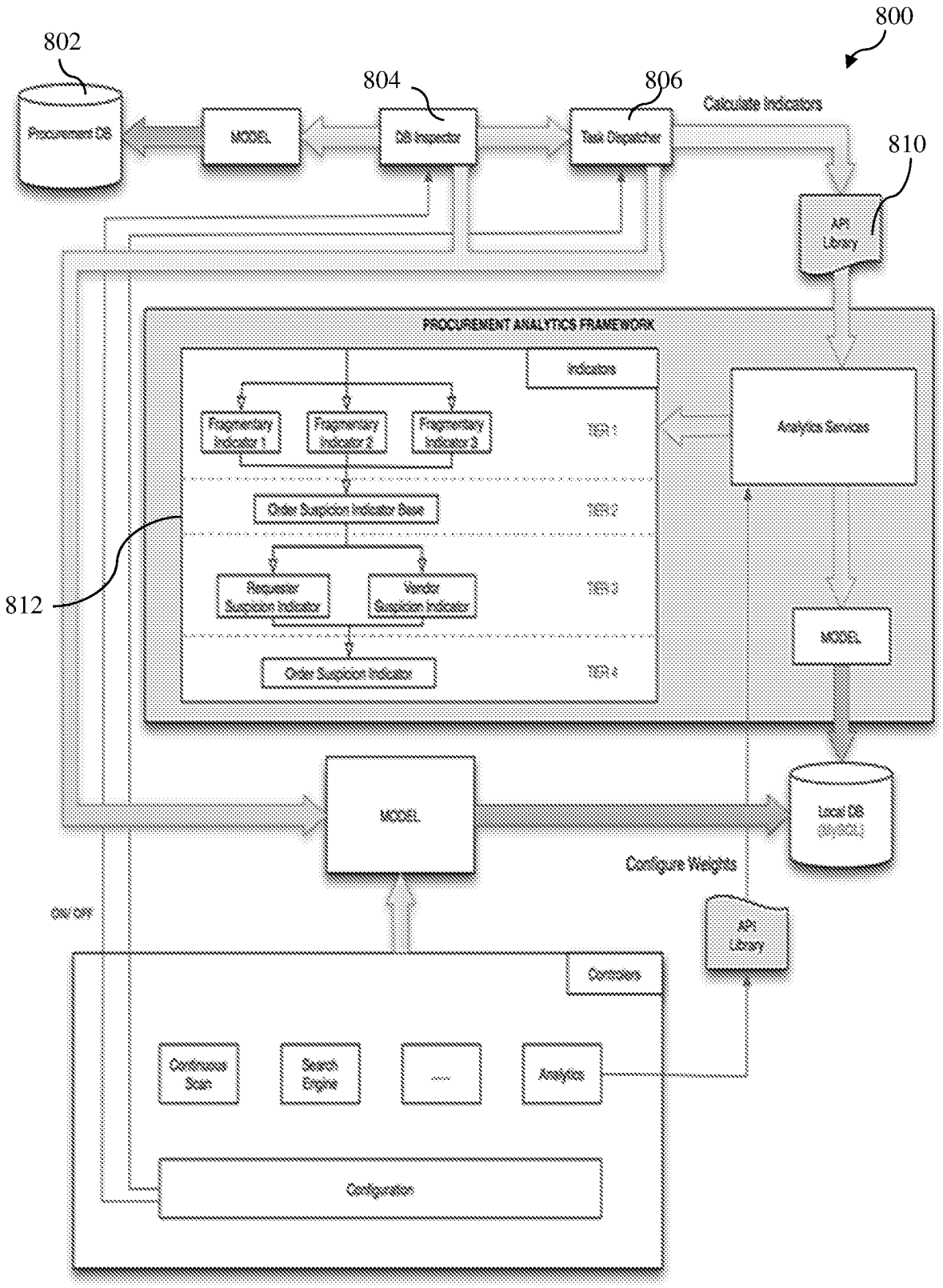
800
802
804
806
810
812
Calculate Indicators
MODEL
PROCUREMENT ANALYTICS FRAMEWORK
Indicators
Analytics Services
MODEL
MODEL
Configure Weights
Connectors
Configuration

FIG. 8

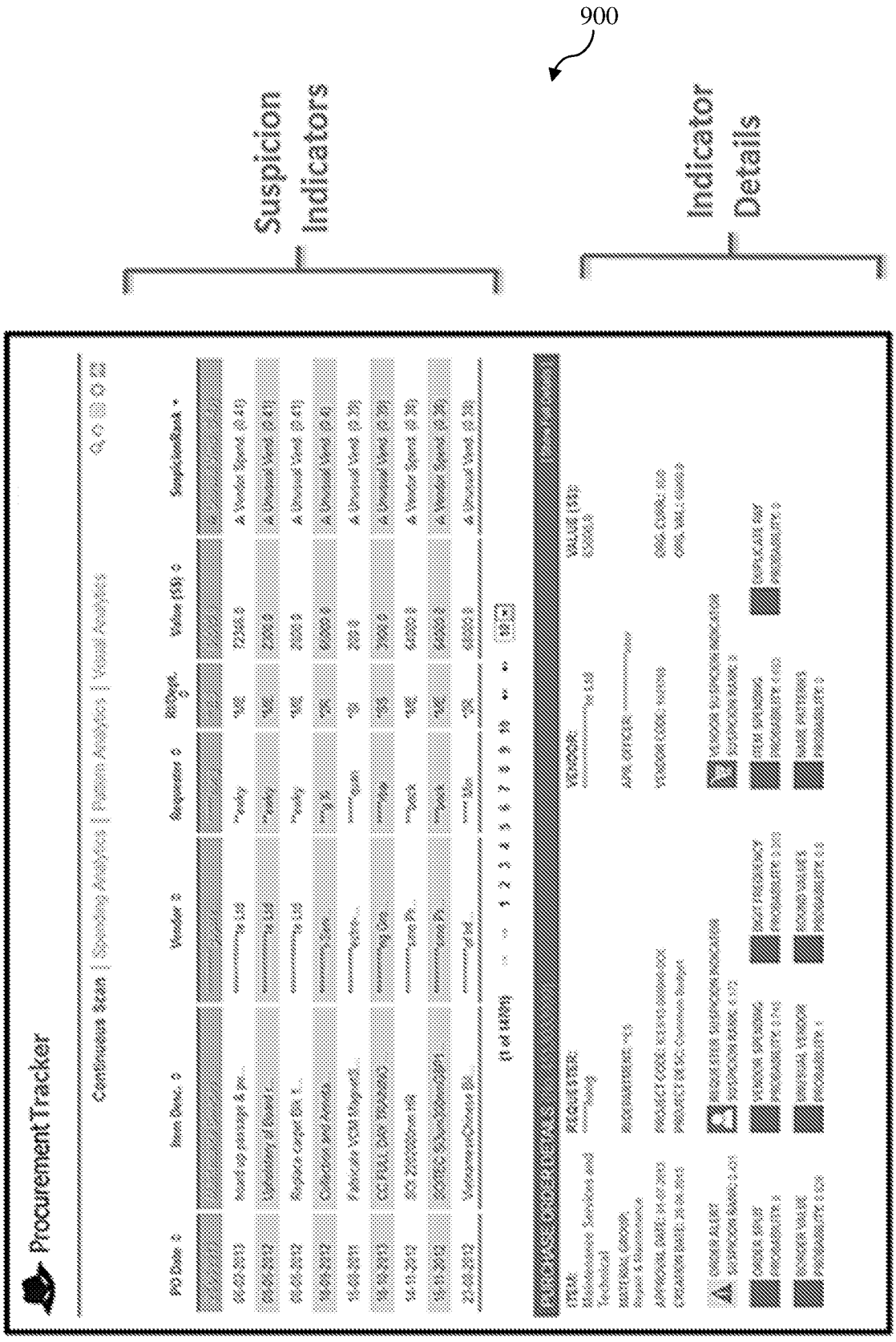
900
Suspicion Indicators
Indicator Details
Procurement Tracker

FIG. 9

910

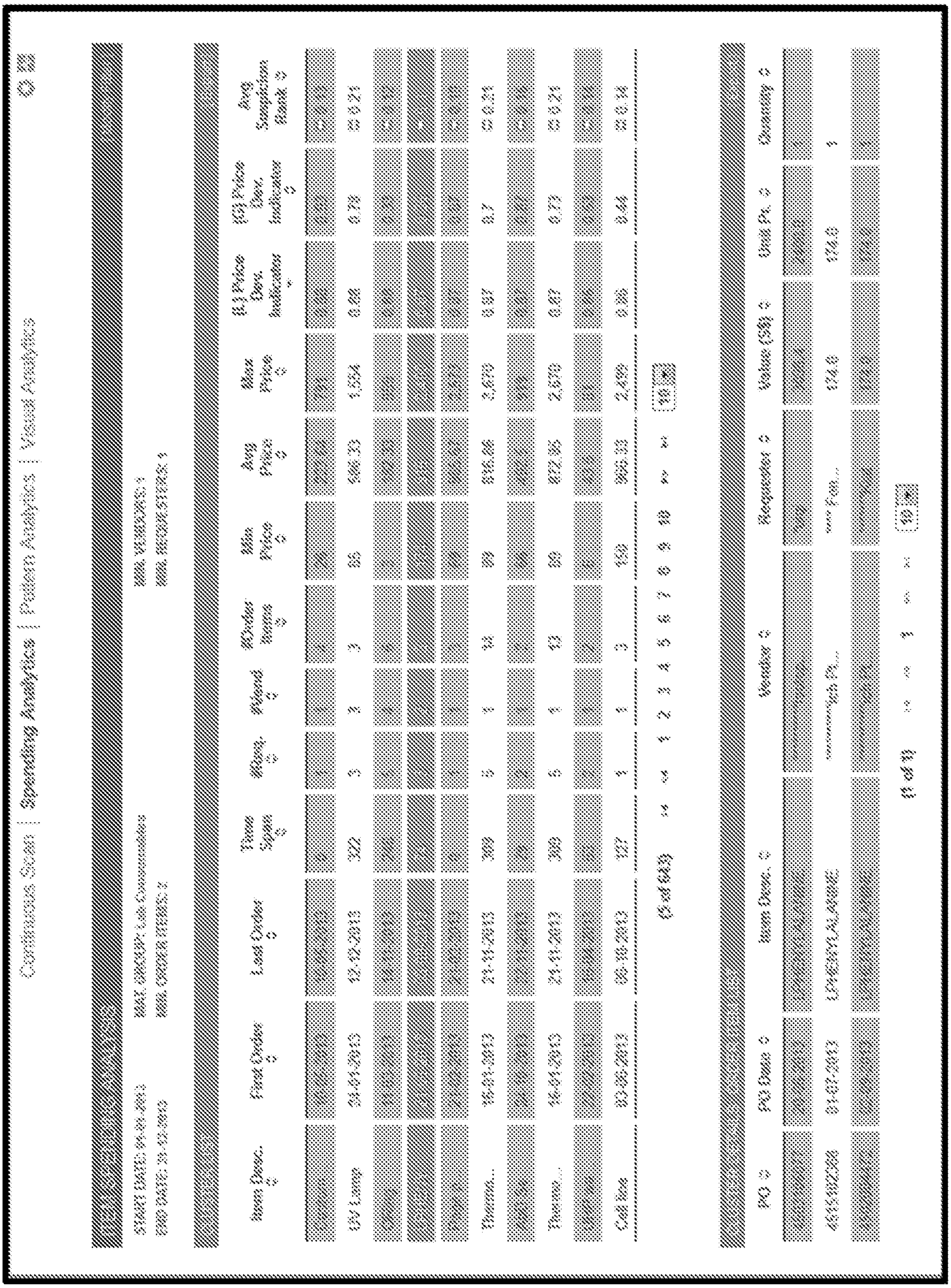
Continuous Scan | Spending Analytics | Pattern Analytics | Visual Analytics
Item Desc.
First Order
Last Order
Time Span
#Req.
#Vend
#Order Items
Min Price
Avg Price
Max Price
[L] Price Dev. Indicator
[G] Price Dev. Indicator
Avg Suspicion Rank
UV Lamp
Cell line
PO
PO Date
Item Desc.
Vendor
Requester
Value (S$)
Unit Pr.
Quantity

FIG. 10

ProcurementTracker
Continuous Scan | Spending Analytics | Pattern Analytics | Visual Analytics
Order Split | Unusual Vendor | Others
UNUSUAL VENDOR ANALYSIS
CASES COUNT: 167
REQUESTERS INVOLVED: 69
VENDORS INVOLVED: 81
AVG. ORDERS: 5.7167
START DATE: 01-07-2013
MIN. ORDER VALUE:
MIN. CLUSTER VALUE: 6666.6
MIN. ORDERS: 1
END DATE: 01-12-2013
MAX. ORDER VALUE: 70666.6
MAX. CLUSTER VALUE:
MAX. ORDERS:
PATTERN LIST
Vendor
Requester
PR
Total Value
#Orders
Unusual Vendor Indicator
Avg Suspicion Rank
(1 of 11)
10

920

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG2016/050627

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01)

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC/WPI/FAMPAT: fraud, embezzlement, detection, identify, abnormal, suspicious, combination, multiple, indicator, index, score, transaction, invoice, data, information and related terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7970701 B2 (LEWIS M. ET AL.) 28 June 2011 Column 7 Lines 63-66, Column 8 Lines 63-65, Column 9 Lines 1-67, Column 10 Lines 42-47 and Column 18 Lines 31-36	1-20
X	US 8041597 B2 (LI X. ET AL.) 18 October 2011 Column 3 Lines 4-45, Column 5 Line 9 - Column 6 Line 25 and Column 7 Lines 4-27	1-20
X	US 2013/0036038 A1 (NISAL O. & PRASANNA B.G.) 7 February 2013 Para. [0016], [0026], [0027] and [0037]; Tables 1 and 3	1-20

☒ 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	Date of mailing of the international search report
23/02/2017 *(day/month/year)*	17/03/2017 *(day/month/year)*

Name and mailing address of the ISA/SG

IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

Intellectual Property Office of Singapore
51 Bras Basah Road
#01-01 Manulife Centre
Singapore 189554

Email: pct@ipos.gov.sg

Authorized officer

Teo Ailing (Dr)

IPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050627

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 8805737 B1 (CHEN K.C. ET AL.) 12 August 2014 Column 5 Lines 7 - 31, Figure 5	-
A	US 7610040 B2 (CANTINI R. & LAUPER K. B.) 27 October 2009 Whole document, in particular column 10 Line 25 - Column 14 Line 3	-

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SG2016/050627

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7970701 B2	28/06/2011	AU 2870002 A	15/05/2005
		CA 2426168 A1	10/05/2002
		EP 1340178 A4	08/06/2005
		JP 5265213 B2	14/08/2013
		JP 2004-524599 A	12/08/2004
		US 6029154 A	22/02/2000
		US 7096192 B1	22/08/2006
		US 7403922 B1	22/07/2008
		US 7752084 B2	06/07/2010
		US 8244629 B2	14/08/2012
		US 2008/0281743 A1	13/11/2008
		US 2010/0228649 A1	09/09/2010
		WO 02/37219 A9	13/05/2004
US 8041597 B2	18/10/2011	NONE	
US 2013/0036038 A1	07/02/2013	EP 2555153 A1	06/02/2013
US 8805737 B1	12/08/2014	NONE	
US 7610040 B2	27/10/2009	AU 2004/213936 A1	02/09/2004
		CA 2516686 A1	02/09/2004
		CN 1751324 A	22/03/2006
		EP 1450321 A1	25/08/2004
		JP 2006-518895 A	17/08/2006
		WO 2004/075130 A1	02/09/2004