



- (51) **International Patent Classification:**
G06Q 30/02 (2012.01) *G06F 21/60* (2013.01)
- (21) **International Application Number:**
PCT/AU2016/000307
- (22) **International Filing Date:**
1 September 2016 (01.09.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/312,075 23 March 2016 (23.03.2016) US
- (71) **Applicant:** WESTPAC BANKING CORPORATION
[AU/AU]; Level 20, 275 Kent Street, Sydney, NSW 2000 (AU).
- (72) **Inventors:** GILLIGAN, Danny; Level 20, 275 Kent Street, Sydney, NSW 2000 (AU). CANT, Simon; Level 20, 275 Kent Street, Sydney, NSW 2000 (AU). McCARNEY, Paul; Level 20, 275 Kent Street, Sydney, NSW 2000 (AU). DE RIGOULIERES, Juan Delard; Level 20, 275 Kent Street, Sydney, NSW 2000 (AU). WARD, Andrew John; Level 20, 275 Kent Street, Sydney, NSW 2000 (AU).
- (74) **Agent:** ALLENS PATENT & TRADE MARK ATTORNEYS; 101 Collins Street, Melbourne, VIC 3000 (AU).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) **Title:** A METHOD OF AND SYSTEM FOR ANONYMISING DATA TO FACILITATE PROCESSING OF ASSOCIATED TRANSACTION DATA

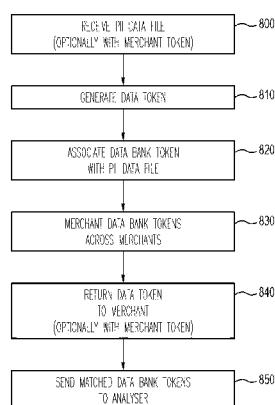


Figure 15

(57) **Abstract:** A computer-implemented method of anonymising personally identifiable information (PII) data across multiple PII data sources which facilitates anonymous analysis of associated transaction data and includes one or more secure computer processors of an anonymising agent receiving from merchants a plurality of PII files, each PII file including fields, a token engine in the one or more secure computer processors generating a data bank anonymising token for each PII file and associating the data bank anonymising token with the PII file, a matching engine in one or more computer processors matching the PII files from each merchant using matching fields to provide matched sets of data bank anonymising customer tokens across the merchants, returning only the respective data bank anonymising tokens to their respective merchants, and the one or more secure computer processors sending the matched sets of data bank anonymising customer tokens to a data analysing agent.



A METHOD OF AND SYSTEM FOR ANONYMISING DATA TO FACILITATE PROCESSING OF ASSOCIATED TRANSACTION DATA

Technical Field

[001] The invention relates generally to computer-implemented anonymisation of personally identifiable information and computer-implemented anonymous analysis of transaction and other information associated with the personally identifiable information.

Background

[002] Businesses are required to record data relating to the transactions with which they are involved, including personally identifiable information (PII). Using that information, certain conclusions can be drawn about a person with whom they have transacted. The person concerned would not necessarily want the information or the conclusions made public and/or utilised for further profit by the same or other businesses, or for the satisfaction of idle curiosity.

[003] Therefore in accordance with the law and the person's desire for privacy, businesses securely store the information.

[004] It is often the case that the same people who want their PII kept secret from other traders also want to be offered certain discounted products to complement other products which they have purchased, or which in other ways complement their lifestyle; a product or discount which cannot be supplied from the original business with which they transacted.

[005] This latter customer desire can be facilitated if businesses share certain information about their customers with other businesses.

[006] Some businesses store transaction records that include certain PII details – name, email address, account number, age, city, street, post code – while others require only certain other PII details – employer, income range, age, post code, and the transaction detail itself.

[007] Due to the above and other factors, the competing desires in the same person of privacy and lifestyle improvement are difficult and cumbersome to satisfy.

[008] The invention seeks to provide a new method and system for 'data banking'. Data banking can be understood in its known forms as storing and anonymising PII from a

plurality of customers. Certain embodiments of the invention facilitate matching of customers across merchants to facilitate analysis of their behaviour beyond one merchant. In some embodiments the technology seeks to facilitate useful and private analysis of certain other data.

Summary of the invention

[009] In a broad aspect the invention relates to the use of an anonymising data matching agent. Embodiments of the technology facilitate market analysis and segmentation using anonymised transaction data shared by a plurality of merchants.

[010] In one broad aspect a system of the present invention is configured to match anonymised individual customer data files across a plurality of merchants in a secure environment. In a connected but separate environment, embodiments or components of the invention analyse and segment transaction data associated with each anonymised customer data file across the plurality of merchants by accessing a master token stored in the secure environment to unlock further transaction data relating to the same anonymised customer data file from a different merchant. Some embodiments provide anonymised matching of similar customer data files based on one or more selected personal information parameters.

[011] In yet another broad aspect, a method of anonymising matching customer data files across a plurality of different merchants is provided. In embodiments of the method, each customer data file extracted from transaction records from a plurality of merchants is associated with a merchant anonymising token and sent to a secure anonymising agent; each customer data file there being associated with a data bank anonymising token. The secure anonymising agent then identifies any matches so as to provide matched customer data files (relating to the one person) on the basis of a plurality of selected PII parameters of a customer or a match to a similar customer based on one or more other selected matched PII parameters across different merchants and records each customer's data bank anonymising tokens as a matching token set. Each matched token set is associated with a unique master token, in one embodiment for auditing purposes, so as to provide a map back to the other tokens in the matching token set. The master token could also be used for purposes other than audit in other embodiments, for example, it may provide a common identifier for two merchants to reference a customer without knowing the other merchant's token for that customer. The merchant and data bank anonymising tokens are returned as a

pair to their respective merchants for analysis of the transaction records associated with the merchant and data bank anonymising tokens.

[012] The invention has advantages in that it can interface with a method of facilitating the segmenting of anonymised customer transaction data. In the method, a data analysing agent receives appended anonymised customer transaction data files from a plurality of merchants, the anonymised customer transaction data files having transaction data appended with pairs of anonymising tokens from an anonymising matching agent, such that the files do not include any Personally Identifiable Information (PII). The data analysing agent then analyses and segments the appended anonymous customer transaction data files and requests a master token from the anonymising matching agent to unlock further data from a different merchant of the same anonymous customer for greater segmentation insights.

[013] In a further aspect of the invention, a method of facilitating market segmentation is provided. In the method, a plurality of merchants append a merchant anonymising token to a Personally Identifiable Information (PII) file and send the PII file to an anonymising matching agent. The PII files are returned stripped of PII and appended with a data bank anonymising token. Each merchant sends transaction data associated with the pair of merchant and data bank anonymising tokens to a data analysing agent, which conducts post-hoc market segmentation and is configured to access master tokens to facilitate access to other anonymising tokens from the same anonymous customer stored by the anonymising matching agent.

[014] In yet another broad aspect, a method of anonymising and matching Personally Identifiable Information (PII) files across a plurality of merchants to facilitate anonymous post-hoc market segmentation is provided. In the method, each one of a plurality of PII files relating to a customer of a merchant, is provided with a merchant anonymising token. Then a plurality of merchants transmit their PII files to a store in a secure environment. Each PII file is then associated with a data bank anonymising token and matched with those files of corresponding customers across the plurality of merchants and associated with a master token to provide a route back to the anonymising tokens of the corresponding customers after the PII has been removed.

[015] In a further broad aspect, each one of a plurality of Personally Identifiable Information (PII) files relating to customers of a first merchant are provided, optionally with a merchant anonymising token by the first merchant, and then transmitted to a secure

environment. A data bank anonymising token is then appended to each PII file. One or more selected PII fields in the PII files are then compared with the same fields in the PII data in corresponding files transmitted by a plurality of other merchants, or even indeed the same merchant, to improve the quality of data held by one merchant. If the PII field comparison results in a match between two or more corresponding PII files, which indicates that the files relate to the same customer (or group of customers), the merchant token (if present) and data bank anonymising token from the matched PII files are associated and stored in the secure environment together with a master token identifying the match. The PII data is retained in the secure environment; only the merchant and data bank anonymising tokens are returned to their respective merchants for further processing to gain insights into market segments.

[016] In selected embodiments the PII data is purged after a selected period of time or event after matching and/or analysis.

[017] In some examples of the method, the master token associated with the matched PII files' anonymising tokens provides a route map back to the corresponding anonymising tokens' associated PII files in the matched PII files to facilitate further anonymised data processing.

[018] In accordance with one aspect, the invention provides a computer-implemented method of anonymising PII data across multiple data sources to facilitate anonymous analysis of associated data, the method including the steps of:

- receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of fields;

- generating by a token engine in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files, and associating the data bank anonymising token with the PII file to create appended PII files;

- matching, by a matching engine in one or more computer processors, the plurality of appended PII files from each merchant using a plurality of matching fields, to provide matched sets of data bank anonymising tokens;

- returning the data bank anonymising token associated with a customer of a respective merchant to that merchant; and

- sending the matched sets of data bank anonymising customer tokens from the one or more secure computer processors to the data analysing agent.

[019] In one embodiment each PII file from each one of the plurality of merchants is, by a computer processor, associated with a merchant anonymising token by each one of the plurality of merchants.

[020] In one embodiment the secure computer processor returns the merchant and data bank anonymising tokens to their respective merchants. Advantageously, the return of the merchant and data bank anonymising tokens facilitates anonymous analysis by a data analyzing agent.

[021] The method of embodiments of the invention is advantageous in that market segments generated by the data analysing agent can be associated with anonymous matching customer data, transaction and other attribute data from other merchants.

[022] In one embodiment the method includes the further step of generating by another token engine in the one or more secure computer processors, a plurality of master tokens and adding one of the plurality of master tokens to each matched set of data bank anonymising tokens to provide a key or a map to audit or unlock respective matched sets of data bank anonymising tokens.

[023] Advantageously, the method stores matched PII and its associated unlocking tokens in a secure environment. In use the secure environment allows access to third parties only to matched sets of data bank anonymising tokens. That is, the analysing agent and the anonymising agent are separated by secure data walls and only sets of data bank anonymising tokens and (in some embodiments) their associated master token are accessible by the analysing agent.

[024] In one embodiment each one of the plurality of merchants generates, in a token engine in one or more computer processors, a plurality of the merchant anonymising tokens and associates each merchant anonymising token with respective ones of the plurality of PII files.

[025] In one embodiment the method further includes the step of, in one or more merchant computer processors, augmenting the pair of merchant and data bank anonymising tokens received from the anonymising agent, with transaction data so as to form respective appended anonymised transaction data files, or appended anonymised attribute data files.

[026] In one embodiment the method includes the step of encrypting each one of the plurality of PII files, whether appended or not, for sending in a secure fashion to the secure computing processors.

[027] In one embodiment the method further includes the step of transmitting the anonymised transaction data, whether in the form of appended anonymized transaction or attribute data files or not, from the merchant computer processors to a data analysing agent for anonymous data analysis.

[028] In one embodiment the method further includes the step of analysing the anonymised transaction data in an analysing engine in a data analysing computer processing system to obtain information regarding market segments and other intelligence regarding behaviour of the anonymous customers.

[029] In one embodiment the analysing step further includes requesting from the anonymising agent a master token associated with respective matched sets of data bank anonymising tokens so that transaction data across the other merchants from the same anonymous customer may be analysed for greater customer insight.

[030] In one embodiment the method further includes the step of transmitting anonymised customer insights from the computer processing system of the analyzing engine back to respective merchants so that they can use the data to offer their customers, say, better service, better deals, or more suitable products at suitable times of their buying cycle.

[031] In one embodiment the merchant anonymising token is a numerical identifier and is referred to as a contributor key or a natural key; each one is generated so as to be substantially unique across each merchant and is the token or key by which the respective merchant will know the PII file and any associated transaction file.

[032] The data fields in the PII files may include, without limitation, state of residence, family name(s), Mobile phone number, suburb name, home phone number, contact email address, gender, aus_dpid, First name, work phone number, date of birth, postcode, zip code, country code, driver licence number, middle name(s), and/or address. There may be other data fields.

[033] In one embodiment the PII files include corresponding fields across merchants. In one embodiment a filtering engine provides data in a consistent format so that matching is simple, by matching field to field. In some embodiments the filtering engine is configured to amend certain PII fields in the PII files so that they are longer or shorter than initially provided, by truncating them or appending field strings.

[034] In one embodiment the filtering engine is provided in the secure computing processor.

[035] In some embodiments the matching engine includes a fuzzy matching module so that certain PII field variances or tolerances such as for example spelling errors or other like issues are accommodated to provide likelihood of matching across PII fields which are not strictly identical.

[036] In one embodiment a permission engine is provided so as to inhibit matching in the matching engine across different merchant files if certain conditions are satisfied. The permission engine in some embodiments includes a lookup table disposed on a storage element of the secure computing processor and/or a database, either of which is accessible by the secure computing processor. The lookup table may include rules which inhibit matching between certain merchants for competition reasons and the like. The lookup table also may be directional wherein the customer of one merchant may not want matches with some other merchants, but the other merchant may permit matches with customers of the one merchant. Permissions in the permission engine may be set by merchants themselves by including fields in the PII file, or in the token, or associated or separate data element sent previously or with the plurality of PII files.

[037] In one embodiment the data bank anonymising token is generated in the secure environment and is an anonymised version of the natural key.

[038] In one embodiment the quality of the PII data in the PII file is checked by the secure computer processor in a quality engine so as to ensure at least one compulsory data field is present in the PII file. In one embodiment the compulsory data field is surname. In one embodiment a second quality check is also carried out by the secure computer processor to ensure that the merchant anonymising token is not duplicated in PII data from the same merchant. Other suitable data quality checks may be conducted before the file is received in the secure computer processor such as for example to enforce date of birth and postcode. In one embodiment the PII file will be rejected from the secure computer processor environment if any of the checks fail and the PII file will be returned to the merchant from which it originated before any token appending or matching in the matching engine.

[039] In one embodiment the rejection and return steps are undertaken by a file transfer gateway. In one embodiment the rejection and return steps are undertaken by an API.

[040] In one embodiment the secure computer processor includes an API server internal to receive the PII files from the merchant.

[041] Advantageously, the invention interfaces with an analyser for analysing anonymized transaction data from multiple merchants, the analyser comprising:

an analysing engine;

a server coupled at one end to the analysing engine and configured to receive a plurality of appended anonymised transaction or attribute data files from a plurality of merchant computer processing systems, each one of the plurality of files having a pair of anonymising tokens associated with transaction or attribute information from a merchant;

the server also configured to request and/or receive one or more sets of matched tokens from an anonymising engine to unlock a connection to other anonymised transaction information from other merchants relating to the same anonymous customer.

[042] The server may be configured to request a master (or audit) token from the anonymising engine so that the server may provide an audit trail for a customer that may request an explanation of how their personal information was used and any insights tracked to them.

[043] In one embodiment the server coupled to the plurality of merchant computer processing systems and the analysing engine is an API server. In one embodiment the API server is coupled to a reverse proxy server which in turn is coupled at its other end to the plurality of merchant computer processing systems and the anonymising engine.

[044] In accordance with another aspect, the invention provides an anonymiser for anonymizing personally Identifiable Information (PII) for use in anonymous transaction analysis of transaction data from multiple merchants, the anonymiser including a computer processing system and including:

a server coupled to the computer processing system and configured to receive appended PII files from multiple merchants, each one of the appended PII files having PII fields and appended with a merchant anonymising customer token;

a data bank token engine coupled to the computer processing system, the data bank token engine configured to generate a data bank anonymising customer token associated with each appended PII file;

a matching engine coupled to the computer processing system, the matching engine configured to match the plurality of PII files from each merchant using a plurality of matching PII fields, to provide matched sets of anonymising customer tokens across the plurality of merchants;

a networked server coupled to the computer processing system, the networked server configured to transmit the matched sets of anonymising customer tokens to an analyser over a network.

[045] In another embodiment the anonymiser includes a master token engine coupled to the computer processing system, the master token engine configured to generate a master token associated with each matched set of anonymising customer tokens so as to provide an audit trail back to explain to a customer how their personal information was securely matched and analysed.

[046] In another aspect the invention provides a token handling engine, the token handling engine coupled to a computer processing system and comprising:

- a merchant token engine configured to generate a merchant token associated with a Personally Identifiable Information (PII) file relating to a customer of the merchant, each PII file having a plurality of PII fields;

- a gateway coupled to the computer processing system for transmitting a plurality of the PII files and associated merchant tokens to an anonymising agent for augmenting with a data bank customer anonymising token and to receive the token pairs back from the anonymising agent without the PII fields;

- a server coupled to the computer processing system and configured to transmit a plurality of the token pairs to an analysing agent;

- a server coupled to the computer processing system and configured to receive information regarding market segments from the analysing agent.

[047] In another aspect the invention provides a computer-readable storage medium containing instructions to implement a method of anonymising data to facilitate further analysis and segmentation of associated transaction data, the method including the steps of:

- receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of fields;

- generating, in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files, and appending the data bank anonymising token to the PII file;

- matching, by one or more computer processors, the plurality of PII files from each merchant using a plurality of matching fields, to provide matched anonymising customer tokens across the plurality of merchants;

- providing the anonymising tokens to their respective merchants; and

- sending the sets of the data bank anonymising tokens and/or the master token from the one or more secure computer processors to a data analysing agent so that market

segments generated by the data analysing agent can be associated with anonymous data from other merchants.

[048] In one embodiment the PII file also includes a merchant anonymising token for association with transaction and/or attribute data relating to the customer.

[049] Advantageously the instructions on the storage medium can interface with a data analysing agent to facilitate anonymous analysis by the data analysing agent.

[050] In one embodiment the method includes an audit step which includes adding a master token to matched anonymising customer tokens to provide a key to unlock those matched anonymising customer tokens. In that embodiment there is provided a transfer step which transfers the master token for auditing of the process.

[051] In yet another aspect the invention provides a computer-implemented method of anonymising customer data to facilitate further analysis and segmentation of associated transaction data, the method including the steps of:

- receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of PII fields;

- generating, in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files, and appending the data bank anonymising token to the PII file;

- matching, by one or more computer processors, the plurality of PII files from each merchant using a plurality of matching PII fields, to provide matched anonymising customer tokens across the plurality of merchants;

- returning only the anonymising tokens to their respective merchants to facilitate anonymous analysis by a data analysing agent; and

- sending the matched sets of anonymised customer tokens from the one or more secure computer processors to the data analysing agent so that market segments generated by the data analysing agent can be associated with anonymous matching customer data from other merchants.

[052] In one embodiment a PII file includes a merchant anonymising token provided by a respective merchant.

[053] In one embodiment the method includes the step of adding a master token to matched anonymising customer tokens to provide a key to unlock those matched anonymising customer tokens.

[054] In accordance with a yet further aspect, the invention provides a computer-implemented method of anonymous analysis of transaction data, the method including the steps of:

- generating, in one or more merchant computer processors, a customer Personally Identifiable Information (PII) data file;

- transmitting to one or more secure computer processors of a secure anonymising agent, from a plurality of merchants, a plurality of customer PII data files;

- generating, in the one or more secure computer processors of the secure anonymising agent, a data bank anonymising token for each one of the plurality of PII files, and appending the data bank anonymising token to the PII file to provide a further appended customer PII data file;

- matching, by one or more computer processors, the plurality of further appended PII data files of each merchant using a plurality of matching fields, to provide matching pairs of anonymising tokens corresponding to individual customers across the plurality of merchants;

- sending via a computer network only the anonymising token to their respective merchants to facilitate anonymous analysis by a data analysing agent;

- associating in each merchant's computer processors the anonymising tokens with related transaction data to provide anonymous transaction data files;

- sending the anonymous transaction data files over a computer network to the data analysing agent;

- analysing the anonymous transaction data files with one or more computer processors in the data analysing agent;

- sending the matched sets of anonymising customer tokens from the one or more secure computer processors to the data analysing agent so that broader market segments generated by the data analysing agent can be identified by association of anonymised customer data of one merchant with anonymous matching customer data from other merchants; and

- returning market segments to the merchant's computer processors.

[055] In one embodiment the generating step includes generating a first substantially unique ID token to be appended to the PII data file to provide an appended customer PII data file.

[056] In one embodiment the transmitting step includes transmitting the appended customer PII data files.

[057] In one embodiment the sending step includes sending the ID token with the anonymising token to the merchant.

[058] In one embodiment the association step includes associating the ID token and anonymising tokens with related transaction data.

[059] In one embodiment the method includes the step of adding by one or more computer processors a master token to the matching pairs of tokens to provide a token key to unlock those corresponding matched pairs of tokens.

[060] In accordance with one aspect, there is provided a method of segmenting anonymised customer transaction data, the method including the steps of:

- receiving, in one or more computer processors of an analysing agent, anonymised transaction data files from a merchant, the files including transaction data associated with pairs of anonymising tokens, at least one anonymising token being from an anonymising agent;

- analysing the anonymised transaction data files in an analysing engine to produce information on market segments;

- requesting a plurality of matched tokens from the anonymising agent to provide a link between anonymised transaction data of one anonymous customer, across different merchants.

[061] Throughout this specification, unless the context requires otherwise, the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

[062] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is solely for the purpose of providing a context for the present invention. It is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention as it existed before the priority date of each claim of this specification.

Brief description of the figures

[063] In order that the invention may be more clearly understood, preferred embodiments will now be described by way of non-limiting examples, with reference to the following Figures.

[064] Figure 1 is a schematic view of a system in accordance with an embodiment of the invention, showing the interactions and information flows between each component – being the merchant computer processing systems, the anonymising agent computer processing systems and the data analysing agent computer systems;

[065] Figure 2 is another kind of schematic view of the system in accordance with an embodiment of the invention;

[066] Figure 3 is a flow diagram of the steps in an embodiment of the method of the invention;

[067] Figure 4 shows the integration schematics of an embodiment of the invention;

[068] Figure 5 is an example PII data file created by a merchant/data contributor;

[069] Figure 6 shows the kinds of tokens and rules by which they are generated in the system;

[070] Figure 7 is a high level schematic view of a computer system forming part of one embodiment of the invention;

[071] Figure 8 is a schematic diagram of a computer processing system forming part of one embodiment of the invention;

[072] Figure 9 is a schematic diagram of a portable computer processing system forming part of one embodiment of the invention, which may for example be a client;

[073] Figure 10 is a schematic diagram of a portable computer processing system forming part of one embodiment of the invention, which may for example be a client;

[074] Figure 11 is a block diagram of the system in accordance with an embodiment of the invention;

[075] Figure 12 is a schematic diagram of connectivity between various elements of an embodiment using encryption to secure the PII data files;

[076] Figure 13 is a schematic representation of docker container architecture, on which some components of the system of the invention are built;

[077] Figure 14 is a lookup table which is one embodiment of the basis of a permissions engine which is a filter to the matching engine;

[078] Figure 15 is a summary flow chart of one embodiment of the method described herein; and

[079] Figure 16 is a high level architecture of probabilistic matching system.

Detailed description of the preferred embodiments

Definitions

[080] It is to be understood that throughout this specification, in the description, preamble, claims and drawings that follow, the term "data contributors" is interchangeable with "merchants".

[081] It is also to be understood that throughout this specification, and the claims that follow, the word "customer" can be used interchangeably with "entity", "person", "device", "household", "business", "company" and other identifiable entity. It is to be understood that the databank system 520 can be utilised to anonymise and match any entity that has attributes such as an address, postcode, phone number, IMEI and the like.

[082] Furthermore it is to be understood that PII files contain personally identifiable information and include a plurality of separate fields which may themselves be in clear text format or hashed. Hashed PII files for the purposes of this specification may not be readily identifiable as PII but a person of ordinary skill would still understand that, armed with a hash algorithm and hash parameters, the hashed PII file can be used in anonymising, matching and analysis operations. Similarly, PII files can be encrypted and still be used in anonymising, matching and analysis operations.

General computing architecture suitable for use with the technology

[083] The invention relates to systems and computer implemented methods for anonymising Personally Identifiable Information (PII) relating to a plurality of customers of a merchant, by generating anonymising tokens and associating the anonymising tokens with PII data files. It may be considered that the system and method facilitates the representation of customer PII in a consistent way across merchants without identifying the customer. The system of the invention also generates other anonymising tokens for

association with individual PII files in a secure environment to facilitate anonymous matching of the same customer or similar customers from a different merchant. Further, embodiments are described which provide mapping back to anonymised transaction information of the same customer from the different merchants. The system and method also provide analysis of anonymised data across multiple merchants. Some example system architecture on which the invention may be suited to be implemented is described herein.

[084] The system and method of the invention may be implemented on a plurality of processors including at least one merchant administrator computer processing system 500, at least one secure computer processor of a secure anonymising agent 520, and at least one computer processing system of data analysing agent 550. Each one of the computer processing systems 500, 520 and 550 may be arranged as a client-server system 300 as generally shown in Figure 7 and connected to one another via a communications network 304 as shown in Figure 1. In that case, each client-server system 300 includes a server system 301 which communicates with a client system 302 via a communications network 304 (e.g. the Internet). Communication between the server system 301 and the client systems 302 (or 500, 501, 502, say) may be via a web-client operating on the client system 302 (e.g. a web browser such as Internet Explorer, Chrome, Safari or similar) and served by a web-server of the server system 302, or by a specific programmatic client running on the client system 301 and served by an application program interface (API) server running on the server system 302. Other implementation architecture is also contemplated as shown in the Figures and described herein.

[085] System 200 shown in Figure 8 depicts various features and components, however as will be appreciated, alternative computer systems architecture suitable for implementing aspects of the invention may have additional, alternative, or fewer components. Figure 8 is a block diagram of one example of a computer processing system 200 suitable for implementing at least some of the various features of the invention, including the secure anonymising agent 520, the data analysing agent 550 and the merchant administrator computer processing system 500, 501, 502, etc. In further examples, server system 301 of Figure 7 may be a computing system (e.g. server) having components similar to system 200 and client systems 104 (Figure 9) (such as desktops, laptops, notebooks, netbooks, tablet computers, mobile phones, PDAs etc) may also be computing systems having components similar to system 200. As will be appreciated, the particular type of computing system will determine the appropriate hardware and architecture, and alternative computer systems

suitable for implementing aspects of the invention may have additional, alternative, or fewer components than those depicted.

[086] As shown in Figure 8, computer processing system 200 includes at least one processing unit 202. The processing unit 202 may include a single processor (e.g. a microprocessor or other computational device), or may include a plurality of processors. In some instances all processing or determining steps will be performed by processing unit 202, however in other instances processing or determining steps may also, or alternatively, be performed by remote processors accessible and useable (either in a shared or dedicated manner) by the system 200.

[087] Through a communications bus 204 the processing unit 202 is in data communication with a system memory 206 (e.g. a BIOS), volatile memory 208 (e.g. random access memory including one or more DRAM modules), and non-volatile memory 210 (e.g. one or more hard disk drives, solid state drives, and/or ROM devices such as EPROMs). Instructions and data for controlling operation of the processing unit 202 are stored on the system, volatile, and/or nonvolatile memory 206, 208, and 210. The databases

[088] The computer processing system 200 also includes one or more input/output interfaces (indicated generally by 212) which interface with a plurality of input/output devices. As will be appreciated, a wide variety of input/output devices may be used, including intelligent input/output devices having their own memory and/or processing units. By way of non-limiting example, the system 200 may include: one or more user input devices 214 (e.g. keyboard, mouse, a touch-screen, trackpad, microphone, etc); one or more user output devices 216 (e.g. CRT display, LCD display, LED display, plasma display, touch screen, speaker, etc); one or more ports 218 for interfacing with external devices such as drives and memory (e.g. USB ports, Firewire ports, eSata ports, serial ports, parallel ports, SD card port, Compact Flash port, etc); and one or more communications interfaces 220 (e.g. a Network Interface Card allowing for wired or wireless connection to a communications network such as a local or wide area network). The computer processing system 200 will run one or more applications to allow a user to operate the system 200. Such applications will typically include at least an operating system (such as Microsoft Windows®, Apple OSX, Apple IOS, Android, Unix, or Linux).

[089] In one embodiment, various aspects of the invention are embodied in computer software programs/applications. The programs include computer-readable instructions which can be executed by a processing unit (such as unit 202) to implement the relevant

aspects of the invention. The instructions may be conveyed to the computer processing system by means of a data signal in a transmission channel. Examples of such transmission channels include wired or wireless network connections enabled by the communications interface 220 and various communications protocols.

EXAMPLE

High Level System Architecture

[090] With reference to the attached drawings, in particular Figures 1 to 3, the invention relates to a new system and method of computer-implemented data banking. The new system and method for data banking provides novel functionality in that it is capable of anonymising PII data (in a secure Data Bank computer processor 520) relating to customers or entities, and finding and matching the same anonymous customer or entity across multiple merchant sources 500, 501, 502. Embodiments facilitate, in a separate system and method step, anonymous analysis of associated transaction data or other attribute data across a plurality of merchants.

[091] A computer system as herein described and shown in Figures 1, 2 and 11 (amongst others) may be used to implement embodiments of the method. For efficient and flexible use of resources, it is to be understood that at least some of, or all of, the computer processing systems are contemplated to be implemented via cloud technology, including as virtual machines. For example, in a production environment of the secure Data Bank computer processor 520, the virtual server architecture will be hosted on a proprietary virtual server (known as MTE vBlock), with the hosts running Red Hat (RHEL) deployed via satellite over stretched VLANs between a proprietary system known as IIR into MTE vBlock. The location of servers will be according to a strategic approach which uses MTE vBlock platform to obviate the need for future relocation and benefits from its elastic demand scaling features.

[092] The Data Bank 520 may be hosted on a dedicated VLAN in MTE to inhibit malicious attacks. Transport Layer Security (TLS) is implemented for all communication channels over network 304 within and in between zones such as 520 – 500 and 520 and 550. Inter zone firewalls at transfer gates 510 are implemented to ensure that trust boundaries are validated.

[093] The application is run using docker containers on a base RHEL server with the following tools deployed:

- Docker for containerisation and orchestration
- OpenSSH (server for SFTP)
- Nginx for web server
- Node.js with Express and selected modules (Passport, etc) as API backend
- ETL tool

[094] Example docker architecture to provide certain of the functions discussed herein is shown in Figure 12.

[095] File transfer/upload between merchants 500, 501, 502 and the anonymising agent 520 in the embodiment shown is over network 304 via SFTP. Access permissions are set so that merchants will only be able to see their own upload directory and no others. Security is provided via a DMZ AD account and Public key provided by the merchant . Each merchant is only be able to access their own folder when they connect to the SFTP server, due to security set via the SFTP server and protocol.

[096] Once a merchant uploads an appended PII file to the SFTP server 510 the appended PII file will be collected via a script running on the API server 530 as shown on Figure 12.

[097] The system architecture is configured to be scalable and to provide substantially full-time availability. In that regard, the Databank 520 is segmented into different functional areas such as APIs 520, 555 for data loading and other APIs for address cleansing, for example, and other functions. The disposition of these functional areas as independent but connected provides a configuration that provides independent operation and at least some fault tolerance and scalability. The design and implementation of each functional area facilitates the leverage of techniques such as load balancing, replication or application duplication.

Merchant (data contributor) admin processing

Method 1

[098] In Figures 1, 2 and 11 there is shown high level architecture of individual merchant administrator computer processing systems 500, 501, 502, etc, all securely linked with

appropriate TLS and SFTP server security as discussed herein via network 304 to a secure computing processor in the form of DataBank anonymising server 520.

[0099] The Databank anonymising server 520 itself may be virtually implemented as discussed herein as one or more cloud machines having distributed architecture.

[0100] Each computer system has a token engine 505, 527 coupled thereto for generating merchant tokens (by the merchant token engine 505) and Databank anonymising tokens (by the databank token engine 527).

[0101] The merchant administrator computer processing system may include a merchant GUI 507. An administrator of the GUI 507 may cause, or some other stored and/or transmitted code may cause, each merchant computer processing system (500, 501, 502 etc) to generate for each customer of the merchant, a customer Personally Identifiable Information (PII) data file. Each merchant computer processing system 500, 501, etc then causes the merchant token engine 505 to generate a first substantially unique anonymising ID token, termed a merchant anonymising token, and associate it with the customer PII data file to provide an appended customer PII data file. This step is shown at step 600 in Figure 3.

[0102] Utilising network 304 and file transfer gateways 510, an instruction by the merchant administrator computer processing system 500, 501, 502, etc, is then given via the administrator GUI 507 or some other code, whether stored or transmitted, to securely transmit each appended customer PII data file (which includes each one's respective first substantially unique anonymising ID token) to one or more secure computer processors of a secure anonymising agent (Data Bank) 520. The appended customer PII files (appended with merchant anonymising token) are received in a secure anonymising agent database 525 in the Data Bank computer processing system 520 via an internal API server 530. Aspects of the contents of the anonymising agent database 525, and control thereof, may be controlled via the anonymising agent GUI 535. The transmission step to the database of the secure anonymising agent (Data Bank) 520 is shown at step 610 in Figure 3.

[0103] It is to be understood that a plurality of merchant computer processing systems 500, 501, etc, each generate their own separate customer PII files in their own token engines 505 that are coupled to their own respective computer processing systems 500. They then transmit the appended customer PII files with merchant anonymising tokens, which are themselves unique across each merchant, the files being sent from the file transfer

gateways via a selected protocol, being across the network 304 by the merchants' computer processing systems 501, 502, etc and received in the secure anonymising database 525.

[0104] The secure anonymizing agent computer processing system 520 is configured to validate tokens originating from a particular merchant using a validation engine 590. In that process, in order to validate that a merchant anonymizing token is from an authorized merchant, the validation engine 590 in the secure anonymizing agent 520 causes an API call to be made using API server 530 and transfer gate 510, using both the merchant anonymizing token and the merchant identifier as values. The API will return the value "TRUE" from the merchant computer system 500 if the combination of token/identifier is valid, indicating the origin of the customer PII data file is from an authorized source.

[0105] The merchants may generate and assign merchant tokens based on their internal customer numbers, say, frequent flyer numbers, or other customer number.

[0106] The merchants may then purge PII data associated with the appended customer data files from the computer processing systems 500, 501, 502, etc, retaining the transaction and/or attribute data in files appended/associated with the merchant anonymising ID token.

Further admin functions and processes

[0107] In some arrangements the appended customer PII files from each merchant are stored in individual databases inside the Data Bank databases 525, 525A, 525B to facilitate additional security. In those arrangements the appended customer PII files from each merchant are encapsulated; access controls can be set for groups of appended customer PII files at different levels, and in one embodiment, the access controls to appended customer PII files are set at the level of an individual merchant appended. The encapsulation data in one embodiment represents a set of appended customer PII files which are proposed to have individual backups, the configuration being such that all backups for a merchant can be destroyed without impacting backups of other merchants.

[0108] The computer processors of the secure anonymizing agent 520 are configured to provide data extraction capability for one or more selected merchants for reconciliation purposes. This capability is provided by decrypting a merchant's appended customer PII files from the data bank database 525 and reencrypting it using a combination of the Databank encryption engine 529 and merchant PGP public and shared encryption engine 509. The encrypted file is then transmitted back to the data contributor via a secure mechanism (for

example, the existing sFTP service used to load appended customer PII files to the databank database 525 from the merchant processor 500) over network 304.

Security engine

[0109] In one embodiment of the invention the merchants or data contributors 501, 502, 503 communicate with via network, or operate internally in its computer processing system 501, 502, 503 etc, a security engine 508 to provide additional security to the appended customer PII data file. The security engine 508 may be an encryptor, and in the embodiment shown is also in the form of a hashing engine 509 to receive from 501, 502, etc customer PII data files and then generate hashed PII data and return it to the computer processing system 501, 502, 503 etc or provide it to the anonymising agent 520 through its own file transfer gateway. The hashed customer PII data is provided to the anonymising agent 520 with hash salt generated by the hashing engine 509 in its own appended customer PII file so as to facilitate resolution of the hashed PII data.

[0110] Recursive key management is provided in the security engine embodiment shown, managed by a system provided by Quintessence labs or similar vendor. The system is a virtual appliance running on a customized Linux distribution.

[0111] In some embodiments, there is provided an encryption key on a per-merchant basis. There is a 2-part key such that the Data Bank processing system 520 is inhibited from accessing customer PII data files from a merchant without a key from that merchant. In this embodiment, the customer PII data files (clear text or hashed) stored and used in the Databank processing system 520 is encrypted using an encryption key unique to each merchant that is held by the Databank processing system 520. Each key is further encrypted by a key unique to each merchant and held by each merchant. Hence to encrypt/decrypt a customer PII data file from a selected merchant, the Databank system 520 requests access from a key store of the selected merchant. This allows the merchant to control access to their own customer PII data files within the Databank system 520.

[0112] For databank 520 access to the merchant key, existing standard protocols and mechanisms for secure key exchange are used, for example, using the KMIP standard.

[0113] Transport layer security is implemented for all the communication channels within and between zones (such as between merchant servers and anonymising servers and the like). Firewalls by Netscaler Web Applications are configured to inspect an external API call

from the analyzing engine to the anonymising engine (for the request of tokens and the token sets request).

Hash detection and filtering

[0114] Upon receipt of an appended PII file (appended with a merchant anonymising token) by the internal API server 530, a hash detection engine 531 operates to detect whether the appended PII file includes hashed PII data or non-hashed PII data. If a hashed PII data file is detected then that data is transferred to a hash engine 529 which extracts a (non-hashed) merchant anonymising token. The hashed PII data itself is then filtered by the hash detection engine 531 into a separate anonymising server partition since the process to anonymize is slightly different from anonymising non-hashed PII data. That is, hashed PII data is to be matched with other hashed PII data in a different server partition since there is different encoding with hashed matching, as compared with plain text PII data files transferred over SFTP and other encrypted customer PII data files, which require decrypting with key management using key management server 519.

[0115] Hash engine 529 works to initially, or even periodically, provide over the network 304, to each merchant computer processing system 500, 501, etc, the hash algorithm used in the Databank hash engine 529, as well as the hash parameters for salting the hash. The hash engine 529 during anonymising and matching operations, resolves the hashed data files using the salt previously provided to the merchant so as to be able to match appended PII data files in the (separated for hashed files) matching engine as described below.

[0116] It is contemplated that the hash engine 529 in some embodiments may automatically generate a hash from the clear text data to facilitate matching between non-hashed data from merchants and hashed data from merchants.

[0117] It is worth repeating that in hashed PII files, each PII data field is separately hashed, and the natural key (merchant anonymising token) is not hashed.

Anonymising agent processing

[0118] A data bank token engine 527 is coupled to the computer processing system of the secure anonymising agent 520. The data bank token engine 527 receives the appended customer PII data file from a plurality of merchants 500, 501, 502 etc, in some embodiments via the hash detection engine 531, and then generates a data bank anonymising token for

each one of the plurality of appended PII files received from each merchant and associates the data bank anonymising token with each appended PII file to form modified appended PII data files. This step is shown at step 620 in Figure 3.

[0119] The token engine 527 generates a random number and assigns that number to the appended PII data file as a data bank token. If the PII data file is hashed, the token engine requests the hash engine 529 to hash the data bank token.

[0120] A token duplicate check is conducted in the token engine 527 by reviewing a list of previously-generated numbers and if the check is clear, the data bank token is assigned to the appended PII data file.

Permissions engine

[0121] A permission engine is provided at 569 in the embodiment shown, so as to inhibit matching in a matching engine 528 across different merchant customer PII data files if certain conditions are satisfied. The permission engine in some embodiments includes a lookup table, one example of which is shown at Figure 14, disposed on a storage element of the secure computing processor and/or a database, either of which is accessible by the secure computing processor. The lookup table may include rules which inhibit matching between certain merchants for competition reasons and the like. The lookup table also may be directional wherein the customer of one merchant may not want matches with some other merchants, but the other merchant may permit matches with customers of the one merchant. The permissions may be set by merchants themselves by including fields in the customer PII data file, or in the token, or associated or separate data element sent previously or with the plurality of customer PII data files.

[0122] The permissions engine 569 also processes opt-out requests by entities, in response to which, no matching of entities across merchants is conducted for those entities. In this embodiment, two "exclusion" accounts (say, account1 and account2) are created (one each for hashed and non-hashed records) by the permissions engine 569, and customer PII data files for entities that have opted-out of the matching process are uploaded to a respective exclusion account. The opt-out upload uses the existing upload process, which utilizes network 304.

[0123] Furthermore, during the assignment of the opted-out entity PII data file to either account1 or account2, two additional matching processes are executed if an "exclusion" account already exists for this merchant. (ie hashed or non-hashed). These two additional

matching processes are:

account1/exclusion-account; and

account2/exclusion-account.

All three matching sets are then assigned master-tokens using token engine 541 and stored in a master-token table.

[0124] The account1/account2 matches are then filtered/reduced by the exclusion records in the permissions engine 569, the process being such that where any record in the account1/exclusion-account match-set has the same merchant token as a record in the account1/account2 match-set, then that record is removed from the account1/account2 match-set (not from the master-token table). Similarly, the account1/account2 matches are filtered against the account2/exclusion-account match-set, so that the remaining account1/account2 match-set has all referenced exclusion records removed.

[0125] The final account1/account2 match-set count is then returned in the response to the match request.

[0126] This processing is also used in the /databank/api/v1/<account_id>/associated' API call to only return the count of the filtered set of master-tokens for the account-pair, and not include any "exclusion" accounts.

Matching engine processing

[0127] A matching engine 528 is coupled to the anonymising agent computer processing system 540 which then matches the plurality of modified PII files from each different merchant using a plurality of matching PII fields, to provide matched customer PII data files by matching anonymising customer tokens across the plurality of merchants. This step is shown at 630 in Figure 3. It is to be understood that the matching agent may provide pairs of matched tokens so that they are with the PII information in the customer PII data files or without the PII information in the customer PII data files.

[0128] The matching engine 528 includes a matching algorithm prepared in software code, which is stored in the storage portion of the computer processing system (Data bank) 520 or transmitted thereto. The algorithm causes the processing system (data bank) 520 to seek at least one PII parameter, for example by searching for a field in each file such as for example family name, month, day, year of birth, suburb, street address, and deciding whether there is a match by assessing whether the customer is similar or the same.

[0129] For example, the following matching rules are used in the system, that is, if the conditions on any one of the following lines of this paragraph are satisfied, there is taken to be a match of entity:

- FIRST_NAME, LAST NAME, EMAIL_ADDRESS
- FIRST_NAME, LAST NAME, MOBILE_NUMBER
- FIRST_NAME_INITIAL, LAST NAME, DOB, MOBILE_NUMBER
- FIRST_NAME_INITIAL, LAST NAME, DOB, EMAIL_ADDRESS
- FIRST_NAME, D.O.B, EMAIL_ADDRESS
- FIRST_NAME, D.O.B, MOBILE_NUMBER

[0130] The matching engine firstly limits searching time by searching for broad categories of matching such as postcode if available, then family name if available, and then narrows the search by checking for the availability of birthdate and then searching on the basis of birthdate.

[0131] The computer processing system (data bank) 520 makes decisions on whether there is a likelihood of matched customer PII files based on matches in these areas and decides whether to keep on searching after each match. For some searches the matching engine 528 on the computer processing system (data bank) 520 will be satisfied with a postcode match and for others the matching engine 528 instructs the computer processing system to keep searching until three, four or five PII parameters are matched. After that, the matching appended PII files results are returned to the anonymising agent database 525.

[0132] The matching engine 528 is configured to provide matches, in accordance with the matching algorithm. The algorithm facilitates matching of customer PII data files independent of case and, in some cases, spelling of name, and allows a decision to be made to match when the date of birth of a person is not exactly the same but is very close to a person of, say, the same name and postcode and street address. This allows matching and accurate analysis in the case of keystroke errors or deliberate obfuscation by customers.

[0133] The matching engine 528 is further configured to provide extensible attributes for matching. That is, in operation, individual merchants contribute an extended attribute name regarding a selected customer PII data file. The extended attribute names are encapsulated in a first portion of an input file or named in an API call. In some embodiments, the extended attribute names provided by the merchant are from a standard vocabulary to ensure consistency across a plurality of merchants, however in some embodiments a merchant provides an extended vocabulary. Depending on the

embodiment, different extended attributes provided may be used in defining different matching rules.

[0134] In some embodiments, there are provided extensible matching approaches. That is, there are different options provided, including deterministic, probabilistic, as well as ranges of acceptable matching confidence. In these embodiments, Databank matching engine 528 provides matching between two merchants by one of several different approaches, for example, by deterministic or probabilistic rules. The Databank matching engine 528 is configured to define both the approach to matching and level of confidence that defines a match using that approach. In one example, a match using a probabilistic approach will consider there to be a match between two customer PII data files where there is over 0.8 similarity between the two customer PII data files, but the actual probability can vary and there may be utilized a probability of any one of 0.99, 0.98, 0.97, 0.96, 0.95, 0.90, 0.85, 0.83, 0.82, 0.81, 0.75 or a suitable probability thereabouts.

[0135] One suitable probabilistic approach is one implemented by Informatica. The Informatica solution, involving address correction and update services, is shown in the matching engine 528 shown in Figures 12 and 16 as part of the DataBank solution.

[0136] The matching engine 528 is configured to provide entity matching on either raw data or encrypted/obfuscated data (e.g. pre-hashed). The data files provided by merchants in some embodiments may be either in clear text format or in hashed format (it is to be understood that regardless of clear text or hashed format, all data provided will be encrypted). In embodiments where the customer PII data files are hashed, not all cleansing or matching techniques can apply and those techniques that do not apply will be automatically excluded from the matching processing in the matching engine 528.

[0137] The matching engine 528 passes the customer data files through a filtering engine that inhibits matching between hashed and clear text customer PII data files as this would result in no matches. However, it is to be understood that the filtering engine may transmit customer PII data files that are in clear text format to the hashing engine 529 to be hashed and then passed through the matching engine 528 for appropriate matches to be matched to hashed customer PII data files.

Logical matching

[0138] Furthermore, there is provided a further method of matching – inferred matching. There is provided a method, deployed by the matching engine 528, of inferring matches,

wherein, say, if entity A matches to entity B, and entity B matches to entity C, then entity A should match entity C.

[0139] For example, when performing matches between a first and a second merchant, the method contemplated is to use data from other merchants to improve the speed at which matches are found, and the quality of those matches. Advantageously, in this process, the matching engine 528 may perform a match with selected other merchants where explicit permission has not been granted for matching with those other merchants.

[0140] For example, in a scenario where Merchant 1 only has email addresses in the customer PII data file, Merchant 2 has mobile phone numbers customer PII data file, and Merchant 3 has both email addresses and phone numbers customer PII data file, if we were to match between Merchant 1 and Merchant 2 we would attain no matches, however if data from Merchant 3 could be used to link data from Merchant 1 and Merchant 2, then a higher rate of matches would be found.

Data field Internationalisation

[0141] The Databank processing system 520 is configured to provide configurable data fields to support different national conventions for PII data. Matching rules are configurable to meet different national standards for optimised matching.

Token compression for improved performance

[0142] In native text form, since each Databank token must be substantially unique, the tokens are a relatively large number of bytes. In one embodiment the token is generated in the Databank token engine 527 and then a compression engine 563 compresses the tokens using an algorithm that keeps the tokens in a natural language form, or at least in a person-readable, transportable text datatype by re-basing a number to base 62. Any suitable base may be used, including 20, 25, 30, 35, 40, 45, 50, 55, 60, 64, 66, 68, 70, 75, 80, 85, 90 or any other suitable base.

[0143] In the embodiment shown, the Databank token has been reduced to 22 characters and the Master Token ID has been reduced to 27 characters.

Enhancement of details provided by merchant

[0144] Databank 520 is configured to provide alternate details for matching. For example, primary and alternate addresses, emails and phone numbers may be received. The anonymizing database 525 and matching engine 528 will automatically store fields provided by a merchant and automatically update and include them in any matching-specific rules. The matching engine 528 combines the matching rules into rulesets such that they may be specified in the matching process between two merchants. Databank processing system 520 is configured to provide a filter in the permission engine 569 wherein the rules are only applicable if both merchants have the alternate details.

Sampling

[0145] Rather than devoting the entire processing power of the matching engine 569 to matching all results, the matching engine is configured to provide indicative matching overlap between customer PII data files provided by two different merchants before the matching process is conducted on all the customer PII data files from those two merchants. This is achieved by, among other methods:

- matching only a sample of customer PII data files, summarizing the sample results so the end result is anonymous;

- matches on general data such as post/zip code.

In this embodiment, to minimise the likelihood of any re-identification all summarised results less than a prescribed value will not enable re-identification.

Isolation of tokens from PII data files for match retrieval for external API

[0146] External access of token pairs via API server 530 or API server 555 can be isolated from other data stored in anonymizing Database 525 such as customer PII data files from a selected merchant processor 500. In some embodiments the isolation is by means of a separately-constructed infrastructure and access controls.

Real time matching

[0147] One embodiment of the technology includes a batch matching method which runs generally once per day, usually at night. It is contemplated that the matching process run in realtime, supported by real-time data contributions from merchants. The resulting real-time matches across merchants will be transmitted to external marketing systems to seize opportunities to market to entities.

Anonymising - post matching processing

[0148] The anonymising agent computer processing system 540 is coupled to a master token engine 541 which generates a master token. The computer processing system 540 then adds the master token to any matched sets of anonymising customer tokens to provide a key to unlock those matched anonymising customer tokens. The computer processing system 540 then stores the PII, matched token sets and master token in the secure database 525. This step is also shown at 630 in Figure 3.

Token return

[0149] The secure anonymising agent computer processing system 540 then returns via the File Transfer Gateways 510 only the pair of merchant anonymising ID token and data bank anonymising token to their respective merchant computer systems 500 to facilitate subsequent anonymous analysis by a data analysing agent 550. For clarity, the associated customer PII is retained in the database 525 of the Data Bank 520 but removed from the tokens in a data stream returned to the merchants 500, 501, 502 etc – only the tokens are returned to each respective merchant's computer system 500, 501, etc, based on the first anonymising token ID generated by the respective merchant's token engine 505. This step is shown at 640 in Figure 3.

Linking transaction data with anonymised token matches

[0150] Each merchant's computer processing systems 500, 501 etc associates the merchant anonymising token ID and data bank anonymising tokens with related transaction data from the merchant to provide anonymous transaction data files and sends via file transfer gateways those anonymous transaction data files to the data analysing agent 550. This step is shown at 650 in Figure 3.

Data analysis and auditing

[0151] The data analysing agent 550 then analyses the anonymous transaction data files by an analysing engine, which is coupled to one or more computer processors. This step is shown at 660 in Figure 3.

[0152] The data analysing agent 550 then requests the grouped or paired data bank tokens from across merchants, and may also request the master token from the one or more secure computer processors (data bank) 520 via an API server 555 and reverse proxy server 560 of the data analysing agent 550. The grouped or paired data bank tokens and master token are sent from the secure computer processors 520 and secure database 525 so that information relating to market segments generated by the data analysing agent can be associated with anonymous matching customer data from other merchant's computer systems 500, 501, etc. This step is shown at 670 in Figure 3.

[0153] The data analysing agent 550 then conducts further analysis in its computer processing system based on the anonymous matched customer data sets from the plurality of merchants 500, 501 and via the file transfer gateways, and returns market segments to the merchant's computer processors 500, 501, or whichever one actually requested the analysis.

[0154] The data analysing agent 550 requests metadata from the secure anonymising server 520 via the API server 555 and reverse proxy server 560 to check quality of data and type of data matched for each anonymous customer across merchants. It is to be understood that this data is not actual PII but it is a list of the plurality of PII fields which have been matched in the anonymising server 520 so as to check the quality of the matches made in the anonymising server 520 and the level of trust that can be placed in the conclusions made when the master token unlocks the data sets from the same anonymised customer across the plurality of merchants. The analysis is instructed by a user via admin GUI 536.

[0155] In summary, and referring to the Figures, when in operation, embodiments of the technology provide a computer-implemented method of anonymising PII data across multiple PII data sources to facilitate anonymous analysis of associated transaction data, includes the steps of:

- receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of fields (step 800);

- generating by a token engine in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files (step 810), and associating the data bank anonymising token with the PII file (step 820);

- matching, by a matching engine in one or more computer processors, the plurality of PII files from each merchant using a plurality of matching fields, to provide matched sets of

data bank anonymising customer tokens across the plurality of merchants (step 830);
returning only the respective data bank anonymising tokens to their respective merchants (step 840); and
sending the matched sets of data bank anonymising customer tokens from the one or more secure computer processors to the data analysing agent (step 850).

Further processing functions

\Operational reporting

[0156] The method further includes an operational reporting step which includes reports, such as:

- statistics on data contribution by each merchant, for each merchant;
- summary of tokens, number of match requests and master tokens for each merchant;
- summary of match rates between each merchant;
- summary of data quality of customer PII files from each merchant;
- summary of operational metrics of the Databank processing system 520; and
- summary of users and activity on the Databank system 520.

[0157] The operational reporting step is provided via use of a combination of specially-produced data logs and the outputs of the databank 520 processing steps. The data bank 520 is configured to produce the reports in the reporting engine 571 and then configured to securely transmit the reports, first via the encryption engine 529 for encryption and then via the transfer gate 510 which is available to respective merchants and Databank processing system 520 administrators operating the GUI 535. The operational reports are sensitive and the data bank 520 is configured to provide them in a secure way, such as for example by facilitating their authentication by authorised users using filtering on the data visible to the authorised user.

[0158] The operational reports may be encapsulated and transmitted to a merchant via network 304 and in that case the method includes the step of encrypted the report using the encryption engine 529 of the anonymising processing system 520 and each merchant's PGP public and private encryption keys residing in the encryption engine 509.

Self-service B2C portal

[0159] In some embodiments, a service portal in the form of a web page GUI or mobile application is provided at 535A to facilitate controlled access for an entity, after appropriate authentication, to its own customer PII data files stored in the anonymizing database 525. This service portal will facilitate Databank 520 securely recording the entity's consent and preferences regarding selected data contributors the entity will permit to be matched and the purposes they will allow it to be used for. The information recorded by the service portal 535A is stored in Databank 520 for use in permissions engine 569.

Self-service B2B portal

[0160] Another form of self-service portal in one embodiment is in the form of an API so that merchants can contribute, modify or delete data in / from Data Bank processing system 520. It is to be appreciated that although a suitable method of uploading of customer PII data files is direct upload via the API server 530, there is also contemplated an API method where a separate merchant-facing API server is configured to provide an authenticated merchant with direct, secure maintenance of their data.

[0161] This B2B portal is contemplated to provide Data Bank personnel with a UI that provides customisable matching services for maximum optimisation and in the alternative, a merchant can choose to on-board and manage services online with no interaction with Data Bank personnel. The external portal would be secure, and through which merchants can logon to in order to perform a number of self-service functions. This functionality will remove the need for Databank staff to perform these functions manually, e.g: the merchant onboarding process.

Updating merchants with PII data

[0162] Personal information of entities regularly changes. The Databank processing system 520 is configured to detect updated data regarding an entity upon its receipt from a merchant. The Databank processing system 520 is configured to transmit information to selected merchants that there has been a change of details for the entity without naming the entity, but instead using a selected Databank token for that selected entity for that selected merchant. The transmission is via the network 304 in a suitable format, being a message or file of bulk changes. The transmission is via the encryption engine 529 and the API server 530 to the merchant processing system 500, 501, 502 etc. The PII is de-identified by the use of a Databank token and it is therefore secure.

Address cleansing

[0163] To enhance the accuracy of matching, the Databank processing system 520 will standardise and validate data such as addresses, phone numbers and email addresses. This enhanced data can be returned to the data contributor via a secure means for example the same method that the tokens are returned to a data contributor.

[0164] Validation of data is conducted by comparing data for an entity with data from online services such as for example voter registration records, telephone directories, workplace directories such as for example LinkedIn and like resources.

[0165] This address cleansing function is provided by Informatica and shown in Figure 12.

Maintenance of historical personal information

[0166] When an update request for a selected customer PII data file is received in Data bank processing system 520, existing PII data will not be over-written and will be kept, which has the effect of building up a historical profile for each entity. This maintenance of historical and current data facilitates the improvement of match rates by having more data on which an individual could be matched. For example, if a selected entity updates their address with one merchant and has not updated the information with a different merchant, and the abovedescribed update has not been effected because of insufficient time or permissions, a match can still be made across merchants.

Method 2

[0167] In another example method of uploading the PII files, a merchant token ID is not utilized, or is at least only implied. In this example an administrator having a web app open, say, for onboarding a customer and utilising an API, may, in real time, upload, on a record by record basis, a PII file without having reference to the token engine 505. This means that the Data Bank 520 would exclusively serve as the repository for the PII, and the PII is not stored at the merchant 500 computer system.

[0168] In other embodiments of this method, the PII files are uploaded and exchanged for a Data Bank anonymising token on a record-by-record basis. In this method, it may be that merchant tokens are not generated or are implied, but a window is opened to a selected

customer file or ID having attribute data, while a request to the data bank 520 data bank token engine 527 is made. The data bank anonymising token is associated with the attribute data and then uploaded to the analyser.

Advantages

[0169] Advantageously, the approach maintains matched PII and its unlocking tokens in the secure database 525 of a secure anonymising agent 520 to allow access to anonymised customers across a plurality of merchants in a secure environment. The analysing agent 550 and the anonymising agent 520 are separated by secure firewalls; only pairs of anonymising tokens and their associated master token are accessible by the analysing agent 550.

[0170] The first anonymising token generated by the merchant computing processing systems 500, 501 etc is a numerical identifier and is referred to as a contributor key or a natural key; each one is substantially unique across each merchant and is the token or key by which the respective merchant will know the PII file and any associated transaction file.

[0171] The data fields in the PII files may include state of residence, family name(s), Mobile phone number, suburb name, home phone number, contact email address, gender, aus_dpid, First name, work phone number, date of birth, postcode, zip code, country code, driver licence number, middle name(s), and/or address.

[0172] In one embodiment the second anonymising token is generated in the secure environment 520 and is an anonymised version of the natural key.

[0173] In one embodiment the quality of the PII data in the PII file is checked by the secure computer processor 520 so as to ensure at least one compulsory data field is present in the PII file. The compulsory data field is surname. A second quality check is also carried out by the secure computer processor to ensure that the first anonymising token is not duplicated in PII data from the same merchant. Other suitable data quality checks may be conducted before the file is received in the secure computer processor such as for example to enforce date of birth and postcode. In one embodiment the PII file will be rejected from the secure computer processor environment 520 if any of the checks fail and the PII file will be returned to the relevant merchant computer processing system 500, 501, etc from which it originated.

[0174] In one embodiment the rejection and return steps are undertaken by the file transfer gateway 510. In one embodiment the rejection and return steps are undertaken by an API.

A portable electronic device

[0175] A portable electronic device is shown in Figures 9 and 10 on which example embodiments of the technology may be carried out to enter customer data, conduct administrator tasks on GUI 507, arrange the importation of customer data to the merchant computer processing systems 500, 501 and other relevant steps such as for example, operating the secure database 525. The device is a portable communications device such as a mobile telephone that also contains other functions, such as PDA and/or music player functions.

[0176] In some embodiments, in addition to a touch screen, the device 100 may include a touchpad (not shown) for activating or deactivating particular functions. In some embodiments, the touchpad is a touch-sensitive area of the device that, unlike the touch screen, does not display visual output. The touchpad may be a touch-sensitive surface that is separate from the touch screen in the display system 112 or an extension of the touch-sensitive surface formed by the touch screen.

[0177] It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS

1. A computer-implemented method of anonymising PII data across multiple PII data sources to facilitate anonymous analysis of associated transaction data, the method including the steps of:

receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of fields;

generating by a token engine in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files, and associating the data bank anonymising token with the PII file;

matching, by a matching engine in one or more computer processors, the plurality of PII files from each merchant using a plurality of matching fields, to provide matched sets of data bank anonymising customer tokens across the plurality of merchants;

returning only the respective data bank anonymising tokens to their respective merchants; and

sending the matched sets of data bank anonymising customer tokens from the one or more secure computer processors to the data analysing agent.

2. The method in accordance with claim 1 wherein each PII file from each one of the plurality of merchants is, by respective merchant computer processors, associated with a merchant anonymising token.

3. The method in accordance with claim 2 wherein the secure computer processor returns the merchant and data bank anonymising tokens to their respective merchants.

4. The method in accordance with any one of claims 1 to 3 further including the step of generating by another token engine in the one or more secure computer processors, a plurality of master tokens and adding one of the plurality of master token to each matched anonymising customer token set to provide a key to unlock respective matched anonymising customer token sets.

5. The method in accordance with any one of claims 1 to 4 further including the step of encrypting each one of the plurality of PII files, for sending in a secure fashion to the secure computing processors.

6. The method in accordance with any one of claims 2 to 5 wherein the merchant anonymising token is a numerical identifier and is referred to as a contributor key or a

natural key; each one is substantially unique across each merchant and is the token or key by which the respective merchant will know the PII file and any associated transaction file.

7. The method in accordance with any one of claims 1 to 6 further including a filtering step which provides data in a consistent format so that matching is conducted by matching corresponding fields.

8. The method in accordance with claim 7 wherein the filtering step amends certain PII fields in the PII files so that they are longer or shorter than initially provided, by amending the length of field strings.

9. The method in accordance with any one of claims 1 to 8 wherein the matching step includes a fuzzy or probabilistic matching step so that certain PII field variances or tolerances are accommodated to provide likelihood of matching across PII fields which are not strictly identical.

10. The method in accordance with any one of claims 1 to 9 further including a permission step to inhibit matching in the matching engine across different merchant files if certain conditions are satisfied.

11. The method in accordance with any one of claims 1 to 10 wherein the permission step deploys a permissions engine which includes a lookup table disposed on a storage element of the secure computing processor and/or a database.

12. The method in accordance with any one of claims 1 to 11 further including a quality checking step wherein the quality of the PII data in the PII file is checked by the secure computer processor in a quality engine so as to ensure at least one compulsory data field is present in the PII file.

13. The method in accordance with claim 13 wherein a PII file will be rejected from the secure computer processor environment if any of the quality checks fail and the PII file will be returned to the merchant from which it originated before any token appending or matching in the matching engine.

14. An anonymiser for anonymising Personally Identifiable Information (PII) for use in anonymous transaction analysis of transaction data from multiple merchants, the anonymiser including a computer processing system and including:

a server coupled to the computer processing system and configured to receive appended PII files from multiple merchants, each one of the appended PII files having

PII fields and appended with a merchant anonymising customer token;

a data bank token engine coupled to the computer processing system, the data bank token engine configured to generate a data bank anonymising customer token associated with each appended PII file;

a matching engine coupled to the computer processing system, the matching engine configured to match the plurality of PII files from each merchant using a plurality of matching PII fields, to provide matched sets of anonymising customer tokens across the plurality of merchants;

a server coupled to the computer processing system, the server configured to transmit the matched sets of anonymising customer tokens to an analyser over a network.

15. The method in accordance with claim 14 wherein the anonymiser includes a master token engine coupled to the computer processing system, the master token engine configured to generate a master token associated with each matched set of anonymising customer tokens so as to provide an audit trail back to explain to a customer how their personal information was securely matched and analysed.

16. A computer-readable storage medium containing instructions to implement a method of anonymising data to facilitate further analysis and segmentation of associated transaction data, the method including the steps of:

receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of fields;

generating, in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files, and appending the data bank anonymising token to the PII file;

matching, by one or more computer processors, the plurality of PII files from each merchant using a plurality of matching fields, to provide matched anonymising customer tokens across the plurality of merchants;

providing only the anonymising tokens to their respective merchants; and

sending the master token from the one or more secure computer processors to a data analysing agent so that market segments generated by the data analysing agent can be associated with anonymous matching customer data from other merchants.

17. The method in accordance with claim 16 wherein the PII file also includes a merchant anonymising token for association with transaction and/or attribute data relating to the customer.

18. The method in accordance with claim 16 further including an audit step which includes adding a master token to matched anonymising customer tokens to provide a key to unlock those matched anonymising customer tokens.

19. A computer-implemented method of anonymising customer data to facilitate further analysis and segmentation of associated transaction data, the method including the steps of:

receiving, in one or more secure computer processors of an anonymising agent, from a plurality of merchants, a plurality of PII files, each PII file including a plurality of PII fields;

generating, in the one or more secure computer processors, a data bank anonymising token for each one of the plurality of PII files, and appending the data bank anonymising token to the PII file;

matching, by one or more computer processors, the plurality of PII files from each merchant using a plurality of matching PII fields, to provide matched anonymising customer tokens across the plurality of merchants;

returning only the anonymising tokens to their respective merchants to facilitate anonymous analysis by a data analysing agent; and

sending the matched sets of anonymised customer tokens from the one or more secure computer processors to the data analysing agent so that market segments generated by the data analysing agent can be associated with anonymous matching customer data from other merchants.

20. The method in accordance with claim 19 wherein a PII file includes a merchant anonymising token provided by a respective merchant.

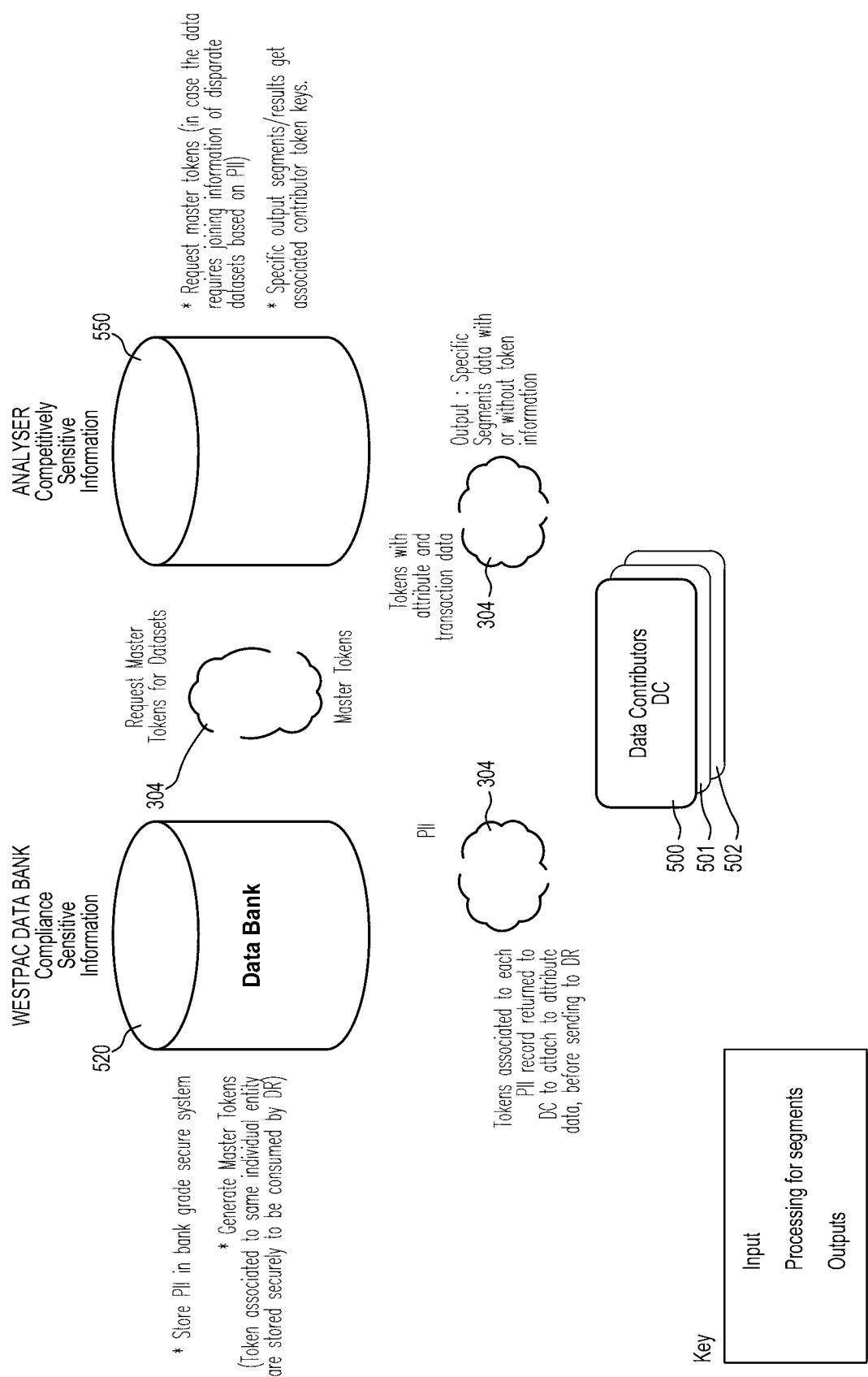


Figure 1

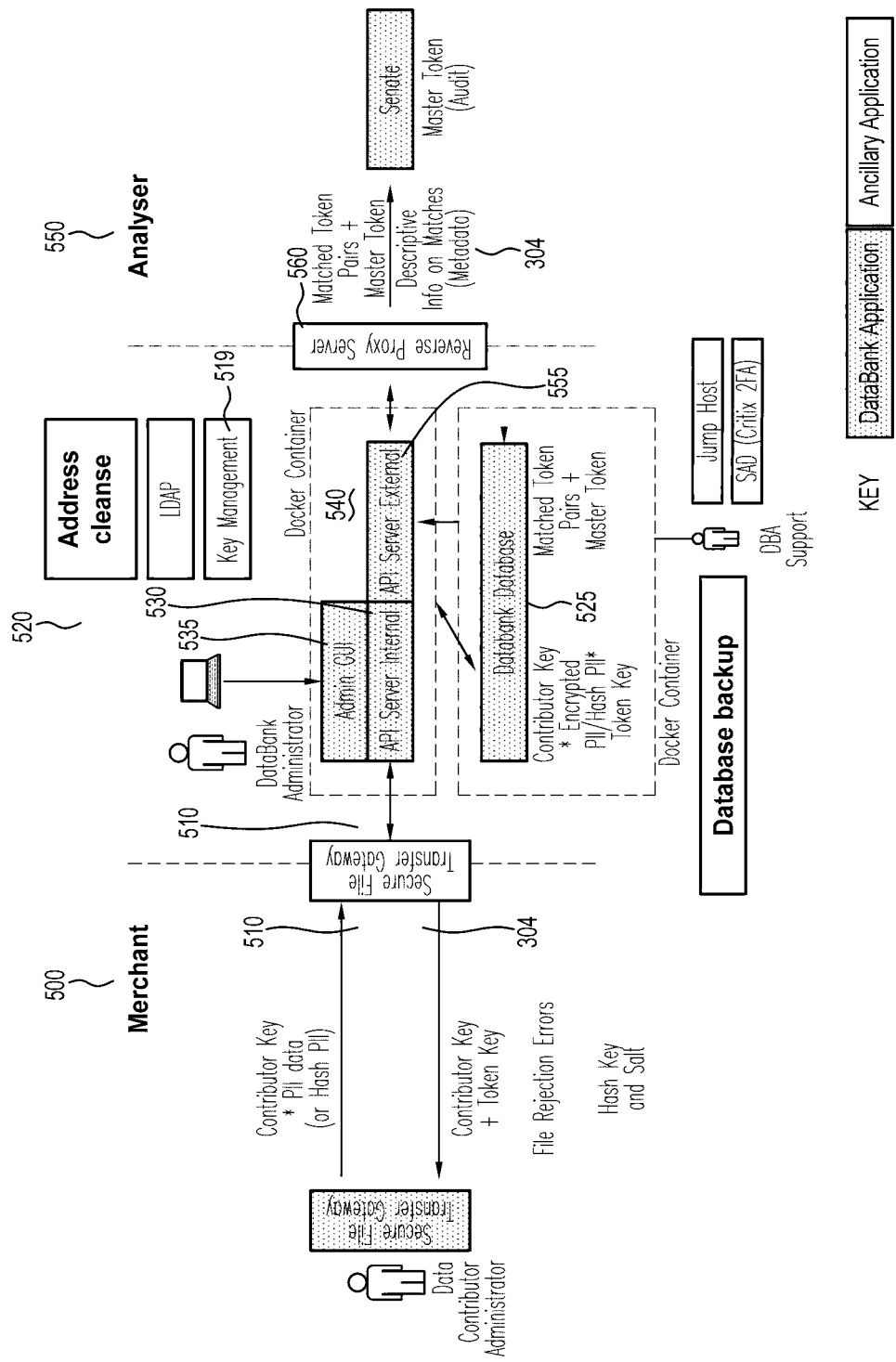
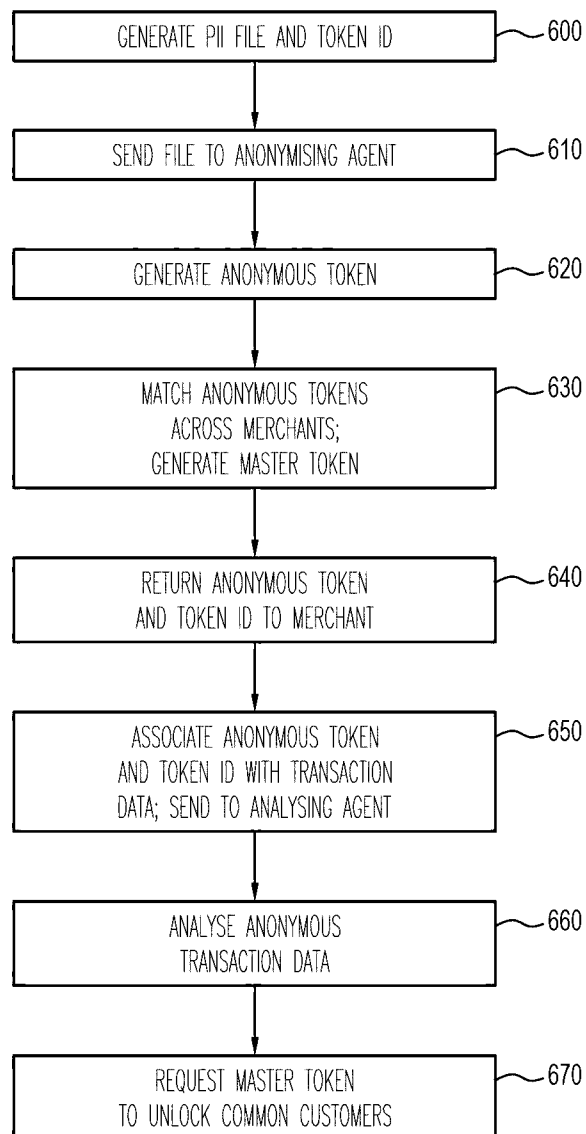
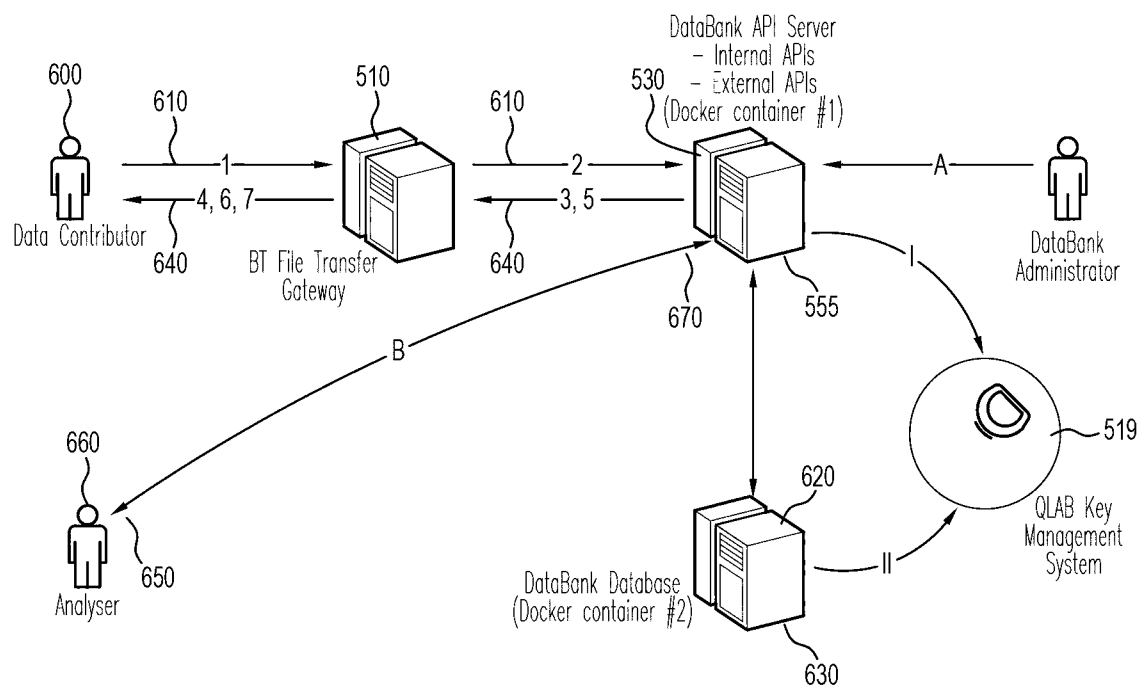


Figure 2

3/16

**Figure 3**

4/16

**Figure 4**

Data from Data Contributor					
Field Order Number	Field Name	Example	Data Type	Constraints / Values	General Comments
1	natural_key	77146c2d-c367-42cb-bc01-b6a69c944e4	VarChar(255)	unique, not blank, not null	Mandatory Natural key is unique from each contributor
2	state	Victoria	VarChar(255)	Standard abbreviations	Optional
3	family_names	Citizen	VarChar(255)	not blank, not null	Mandatory
4	mobile_phone_number	+61 400 123456	VarChar(255)	no spaces, no leading zero for are code, no special characters (e.g. +, -, (,)) begins with country code	Optional
5	suburb_name	Melbourne	VarChar(255)		Optional
6	home_phone_number	+61399995555	VarChar(255)	no spaces, no leading zero for are code, no special characters (e.g. +, -, (,)) begins with country code	Optional
7	contact_email_address	john@test.mail	VarChar(255)	** is empty	Optional
8	gender	female	VarChar(255)	"male", "female" or "unknown"	Optional
9	aus_dpid	12345	Integer	0=null	Optional
10	first_name	John	VarChar(255)	** is empty	Optional
11	work_phone_number	+61399995555	VarChar(255)	no spaces, no leading zero for are code, no special characters (e.g. +, -, (,)) begins with country code	Optional
12	date_of_birth	1978-03-08	Date 'yyyy-mm-dd'	** is empty	Optional, although date format of 'yyyy-mm-dd' must be used otherwise matches are unlikely to occur
13	postcode	3000	VarChar(255)		Optional
14	country_code	AUS	VarChar(255)	ISO values	Optional
15	drivers_licence_number	123456789	VarChar(255)	no spaces, ** is empty	Optional
16	middle_names	Kane	VarChar(255)	no spaces, ** is empty	Optional
17	address	Unit 1/1 Letsbe Avenue	VarChar(255)		Optional, single spaces between words and no commas, street types e.g. street, avenue, lane must not be abbreviated

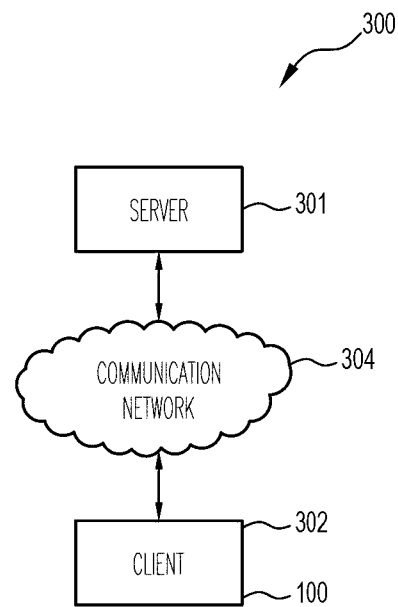
Figure 5

6/16

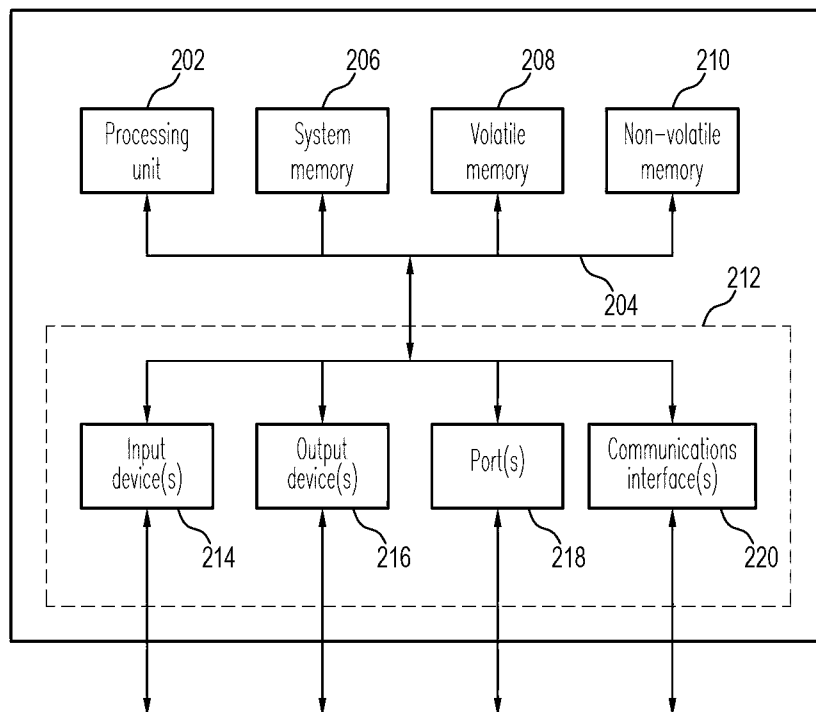
Record identifier	Table Column Name	Description
Account ID	Account. ID	Created by DataBank on creation of the data contributor
Natural Key	record_{account id}.c_natural_key	Provided by Data Contributor, enforced to be unique for a contributor.
Token Key	record_{account id}.c_token	Created by DataBank as part of the file load process. Unique accross ALL Data Contributors.
Master Token	Mastertoken.c_audit_id	Created by DataBank as part of the matching between Data Contributors process. Unique across ALL Data Contributors.

Figure 6

7/16

**Figure 7**

8/16

**Figure 8**

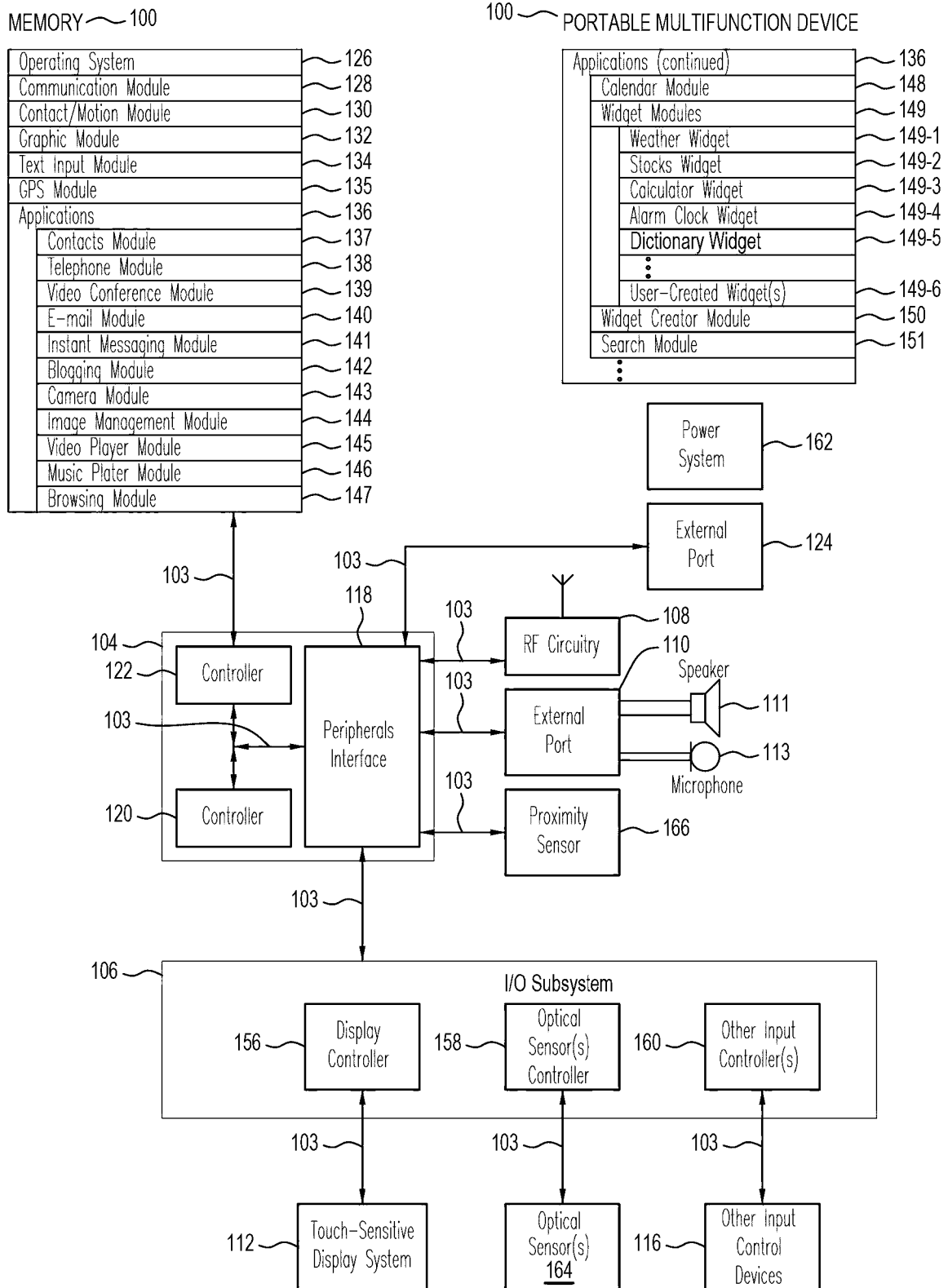
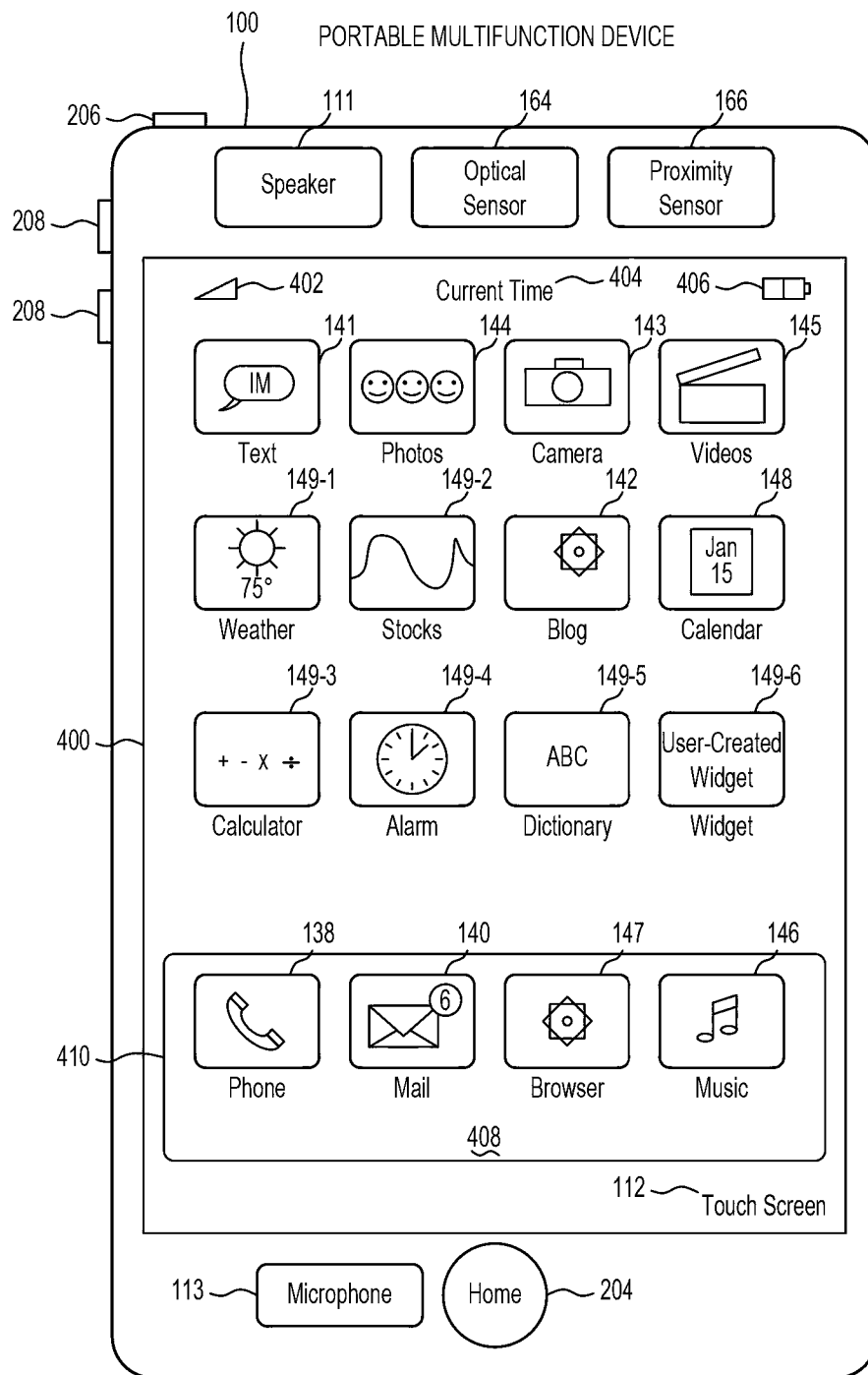
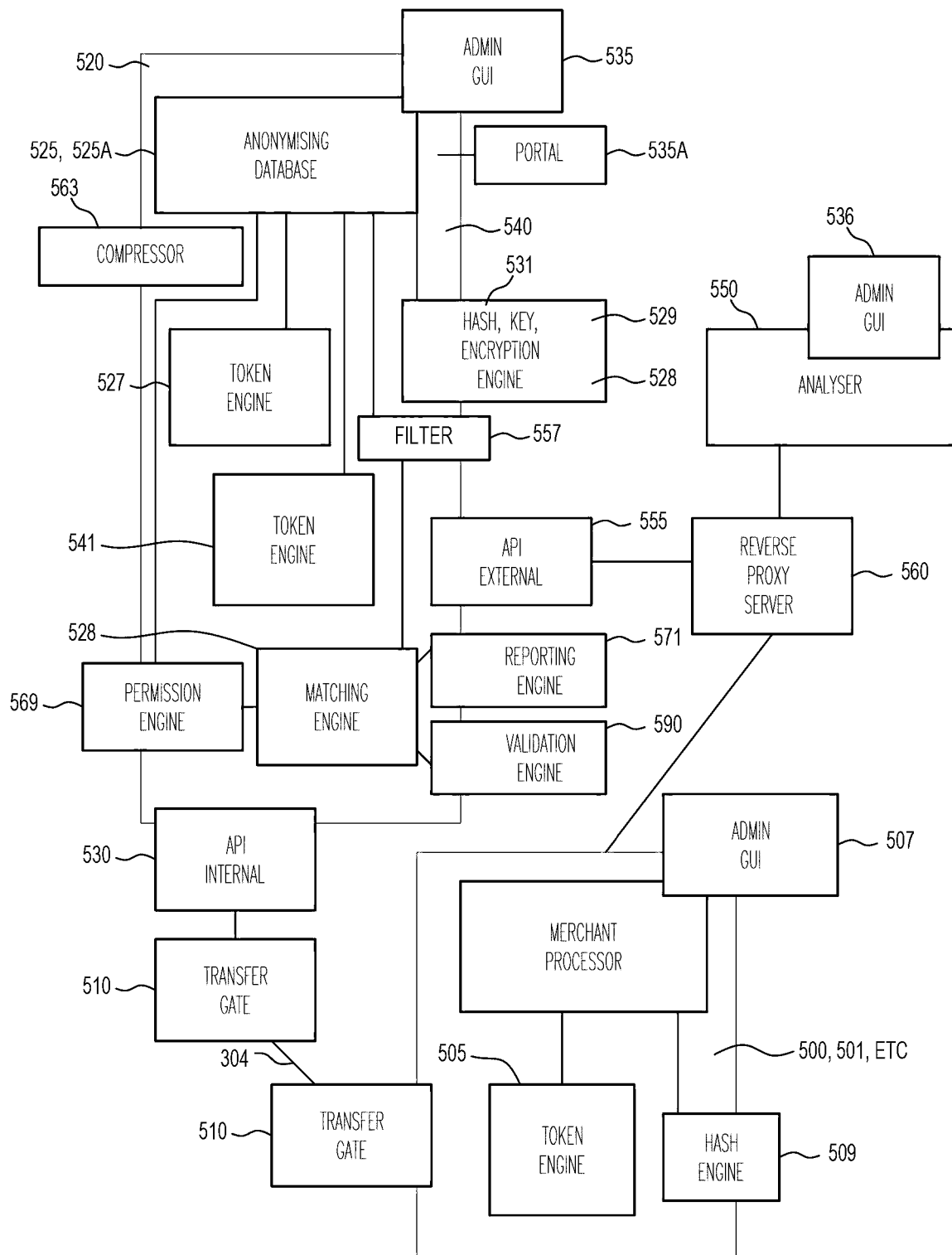


Figure 9

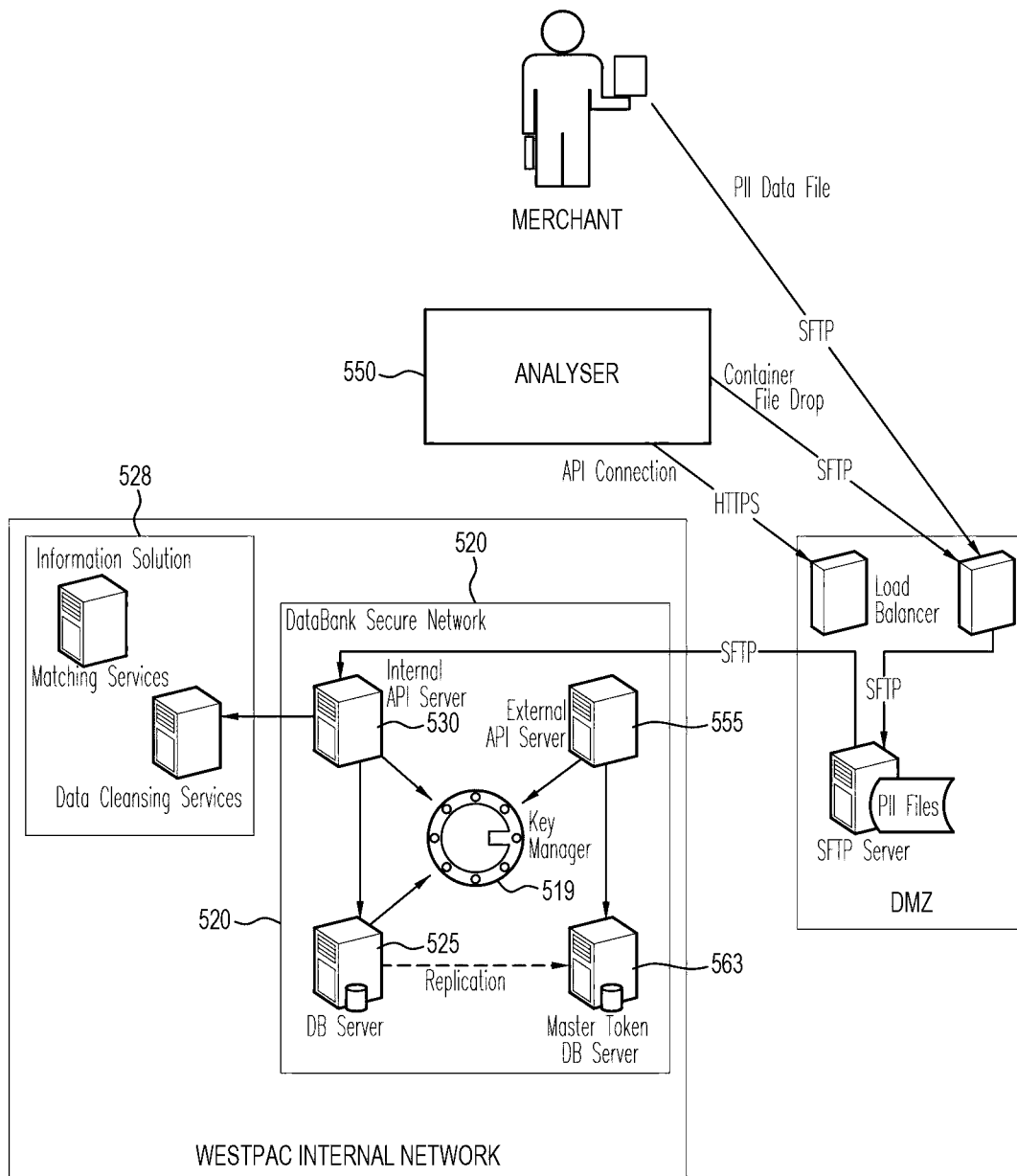
10/16

**Figure 10**

11/16

**Figure 11**

12/16

**Figure 12**

DOCKER ARCHITECTURE

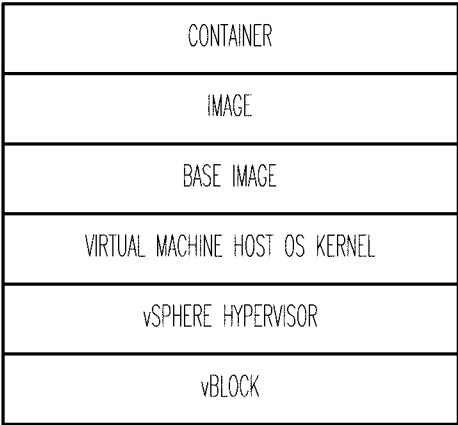
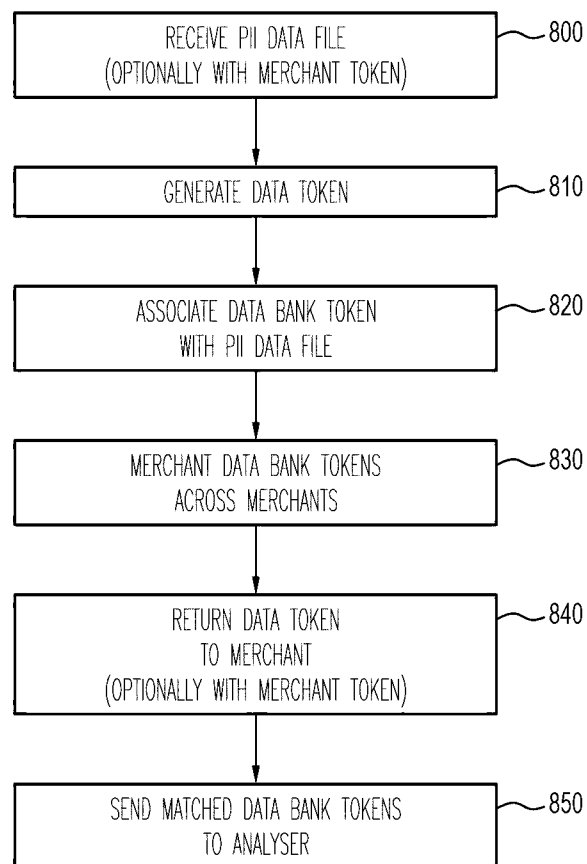


Figure 13

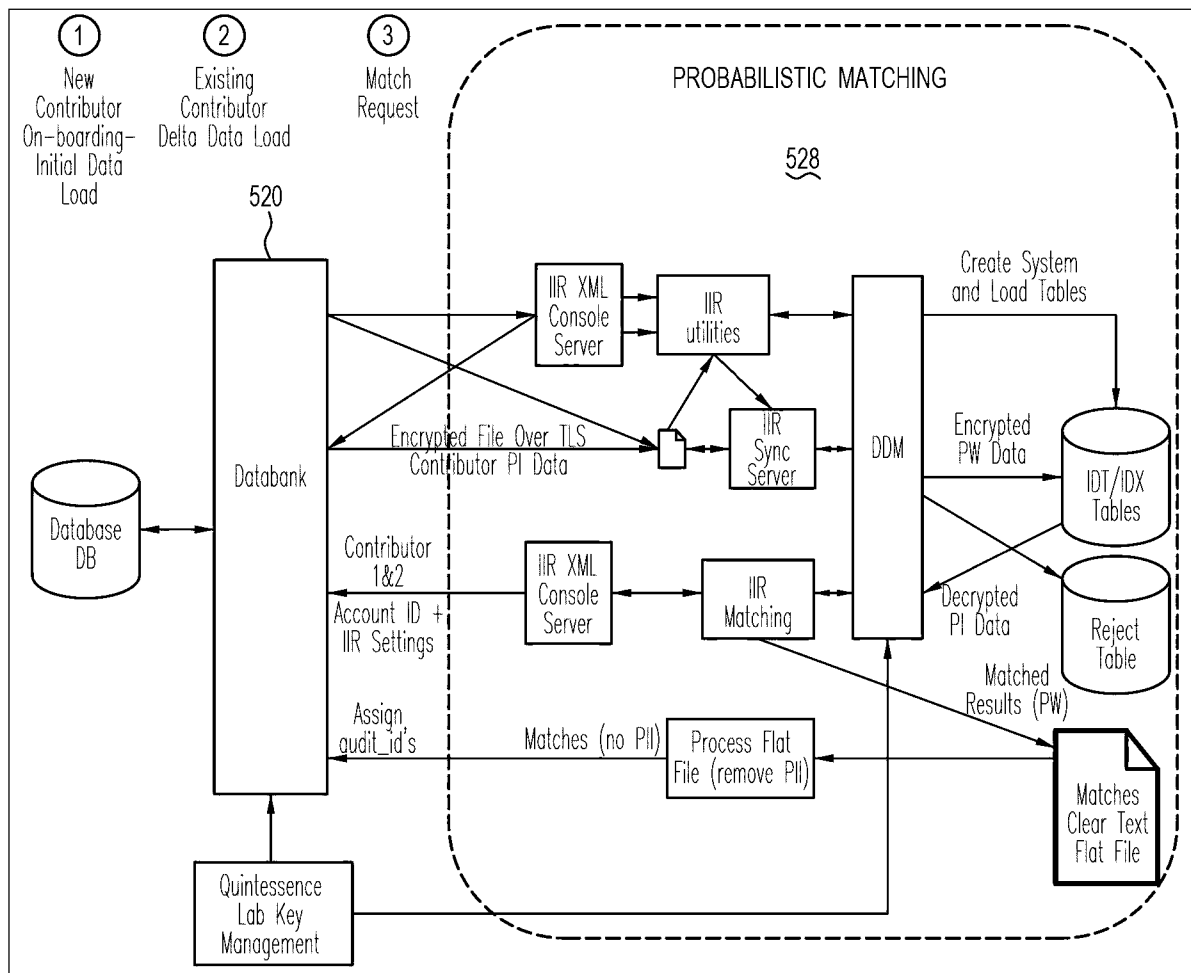
	M1	M2	M3
M1	N/A	YES	NO
M2	NO	N/A	YES
M3	NO	YES	N/A

Figure 14

15/16

**Figure 15**

16/16

**Figure 16**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU2016/000307

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 30/02 (2012.01) G06F 21/60 (2013.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)

Epoque Internal (WPIAP): sanitise, anonymise, de-identify, scrub, cleans, private, identifier, sensitive, token, hash, match, compare, analysis, preference, purchase, behavior, consumer, customer, vendor, merchant, promotion, campaign, advertisement, target, PII, personally, identifiable, information, SPI & like terms; Google Patent: anonymized, de-identified, merchant, master, tokens, transactions, consumers, targeted, analysis, keys, hashed, 6523041, 9355273, 20080147554; Espacenet & IP Australia internal databases: Applicant & inventor name search.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	



Further documents are listed in the continuation of Box C



See patent family annex

* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
4 November 2016

Date of mailing of the international search report
04 November 2016

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
Email address: pct@ipaustalia.gov.au

Authorised officer

Peter Thong
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No. +61 262832128

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		PCT/AU2016/000307
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/0035414 A1 (BARTON et al.) 10 February 2011 Paragraphs 5, 34, 36, 65, 80, 85, 86, 88, 104, 127-128, 226-227, 261-262, 372-373, 382-387, 400, 403-405, 408, 436- 439, figures 1, 2a, 2b, 2c, 5 and 7a in particular.	1-20
A	US 2008/0147554 A1 (STEVENS et al.) 19 June 2008 Whole document.	1-20
A	US 2014/0372214 A1 (SEGMINT INC.) 18 December 2014 Whole document.	1-20
A	US 9292707 B1 (MANAGEMENT SCIENCE ASSOCIATES, INC.) 22 March 2016 Whole document.	1-20

Form PCT/ISA/210 (fifth sheet) (July 2009)

INTERNATIONAL SEARCH REPORT		International application No.	
Information on patent family members		PCT/AU2016/000307	
This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.			
Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	Publication Date	Publication Number	Publication Date
US 2011/0035414 A1	10 February 2011	US 2011035414 A1	10 Feb 2011
		US 8478765 B2	02 Jul 2013
		US 9336532 B1	10 May 2016
US 2008/0147554 A1	19 June 2008	US 2008147554 A1	19 Jun 2008
		US 9355273 B2	31 May 2016
		CA 2615292 A1	18 Jun 2008
		EP 1939785 A2	02 Jul 2008
		EP 1939785 B1	18 Feb 2015
		EP 2953053 A1	09 Dec 2015
		HK 1120316 A1	07 Aug 2015
		MX 2007016358 A	23 Feb 2009
		US 2014/0372214 A1	18 December 2014
BR PI0715289 A2	11 Jun 2013		
CN 101536024 A	16 Sep 2009		
CN 102027500 A	20 Apr 2011		
CN 103038793 A	10 Apr 2013		
CN 103098084 A	08 May 2013		
EP 2115681 A2	11 Nov 2009		
EP 2272037 A2	12 Jan 2011		
EP 2569746 A1	20 Mar 2013		
EP 2569747 A2	20 Mar 2013		
US 2009234708 A1	17 Sep 2009		
US 8234159 B2	31 Jul 2012		
US 2009234715 A1	17 Sep 2009		
US 8239256 B2	07 Aug 2012		
US 2011270661 A1	03 Nov 2011		
US 8825520 B2	02 Sep 2014		
US 2012284127 A1	08 Nov 2012		
US 8874465 B2	28 Oct 2014		
US 2012310732 A1	06 Dec 2012		
US 8918329 B2	23 Dec 2014		
US 2008091535 A1	17 Apr 2008		
US 2011276374 A1	10 Nov 2011		
US 2011276383 A1	10 Nov 2011		
US 2013036009 A1	07 Feb 2013		

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT		International application No.	
Information on patent family members		PCT/AU2016/000307	
This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.			
Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	Publication Date	Publication Number	Publication Date
US 9292707 B1	22 March 2016	US 2014012669 A1	09 Jan 2014
		WO 2008042853 A2	10 Apr 2008
		WO 2009117322 A2	24 Sep 2009
		WO 2011143166 A1	17 Nov 2011
		WO 2011143170 A2	17 Nov 2011
		WO 2011143176 A1	17 Nov 2011
		WO 2013043654 A2	28 Mar 2013
		US 9292707 B1	22 Mar 2016
		CA 2702682 A1	30 Oct 2010
		CA 2762740 A1	10 Jul 2012
		MX 2010004649 A	01 Nov 2010
		MX 2012000479 A	16 Jul 2012
		US 2011154748 A1	30 Jun 2011
		US 9080344 B2	14 Jul 2015
		US 2010275529 A1	04 Nov 2010
		US 9249598 B2	02 Feb 2016
		US 2016138292 A1	19 May 2016
		US 9458643 B2	04 Oct 2016
		US 2016182231 A1	23 Jun 2016
		US 2016251871 A1	01 Sep 2016
End of Annex			