Automated procedure for the protection of electronic data for the purpose of data processing by third parties including transparent and uninterruptible remuneration

Inventor: Jean-Fabian Wenisch

Current assignee: MADANA UG (haftungsbeschränkt)

Original assignee: MADANA UG (haftungsbeschränkt)

Application date: 22.03.2018

Application number: 102018204447.3

Disclaimer: This document is a machine translation of our patent submitted to the German Patent and Trade Mark Office (DPMA).

Computerized translations are only an approximation of the original content. The translation should not be considered exact and in some cases may include incorrect or offensive language. MADANA does not warrant the accuracy, reliability or timeliness of any information translated by the system.

Field of invention

The invention is a method and a system for the protection of electronic data from the production on up to data processing by third parties, whereby a data recipient can reimburse the data producer without knowing the identity of a data producer.

State of the art

Today, digitization covers more and more areas of our lives. As a result, electronic data is also becoming an increasingly valuable resource. The existence of large data streams can therefore not only create new business or policy models, but also new economic models. However, digital information is like no other resource we know so far. It is obtained, processed, evaluated and traded in a different way.

Everyone these days is a data producer. One example is the use of digital services such as apps, browsers or the use of social networks such as Facebook, Twitter, Instagram and co. Every electronic device that helps people, such as temperature sensors in rooms, milling machines, pulse counters, etc., also generates electronic data that can be evaluated and is therefore valuable. However, in most cases the data producer cannot freely determine his data. It is common for the data producer to transfer the rights to his data to a service provider by agreeing to the service provider's non-transparent terms and conditions in order to use the service. Large companies in particular then use this data to make a profit, but without the data producer being able to control this data or even participate in the profit.

A system for the transaction of electronic data between a buyer and at least one seller is known from the international application WO 2000075888 A1. Between the buyer and seller a third party, an administration network, is activated, which knows the data (financial capacity, authenticity, etc.) of both parties. The third party in a transaction can therefore check whether both sides have the required capacities. The administration network is based on a server and sales software that can access a database in which the private data of buyers and sellers is stored. The database here is stored on a centralized data management system. As we know from the messages, these centralized data servers are increasingly being attacked and the data stolen by hackers. This is an enormous danger, especially for data producers, if personal data such as bank details, addresses and telephone numbers etc. fall into the hands of unwanted parties.

It is therefore desirable to have an automated and modular system available which implements a procedure to eliminate the disadvantages mentioned above. Furthermore, a method and system would be desirable which would allow access to analysis results based on different types of data from different sources, while respecting the privacy of data producers and protecting the data itself from unauthorised access. It would also be desirable if the system and procedure could comply with all the directives of the European Data Protection Declaration and provide an opportunity to fairly compensate participants for their share of the data for the analysis results.

Abstract

It is therefore a task of the present invention to provide an automated and modular system which implements a procedure to eliminate the disadvantages of the current state of the art. The task of the invention also includes providing a method and system that allows access to analysis results based on different types of data from different sources, while preserving the privacy of data producers and protecting the data itself from unauthorized access. The system and the procedure also comply with all the guidelines of the European Data Protection Declaration and also offer a way to fairly compensate participants for their share of their data for the analysis results.

The invention solves the task by a procedure for the data security of the data of a data producer, suitable for processing by a third party:

- Recording of the data by a user device of the data producer and a first application;
- Retrieve a globally valid data model via a second software-based interface with an interface to the first application;
- Standardization of data using the globally valid data model via the second software-based interface;
- Storage of the standardized data in a local encrypted database, whereby the number and type of the encrypted data are communicated to a main system;

- Calling an analysis processing entity located on a separate physical unit to the main system and execution of the analysis in a secured execution environment when the main system receives a request, where a first key pair is assigned to a requestor from the main system;
- Dynamic generation of a second key pair by the analysis processing entity at runtime;
- Sending a public key of the second key pair to the data producer, with which the data producer encrypts the requested data before transmission to the main system and then to the analysis processing entity;
- Transfer the encrypted data via the main system back to analysis process entity, where the requested data is decrypted with a private key from the second key pair and analyzed within the trusted execution environment and an analysis result is generated;
- Sending the analysis result, which is encrypted with a public key from the first key pair of the requester, of the analysis processing entity to the main system for inspection by the requester, where only the requester can decrypt the analysis result using a private key from the second key pair of the requester, so that the analysis result can only be viewed by the ordering party and the data can only be viewed by the data producer in order to guarantee the security protection of the data during the processing of third parties.

Data is generally understood to be information, (numerical) values or formulated findings obtained through measurement, observation, etc. According to the invention, data is all electronically recorded information that relates to an object or event. When data is processed, data is defined as characters (or symbols) that represent information and serve the purpose of processing. Data is generally understood to be information, (numerical) values or formulated findings obtained through measurement, observation, etc. According to the invention, data is all electronically recorded information that relates to an object or event. When data is processed, data is defined as characters (or symbols) that represent information and serve the purpose of processing. Data protection law essentially refers to personal data, i.e. information about natural persons, such as gender, date of birth or place of residence. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data is a 1995

European Community Directive on the protection of the privacy of individuals with regard to the processing of personal data. The Directive describes minimum standards for data protection which must be guaranteed by national laws in all Member States of the European Union. In Germany, the European Data Protection Directive was only implemented by the Act amending the Federal Data Protection Act and other laws of 18 May 2001, which came into force on 23 May 2001. It is a claim of the invention to comply with these guidelines. Several data records are also called data records and are used as synonyms.

A data producer can be a natural person who enters information about themselves, such as their clothing sizes when shopping online. A data producer may be a legal person or a community of persons. The data producer can also be a machine that either generates data itself by executing instructions or contains sensors that record the temperature of a room, for example.

A third party is any person or instance that is not represented in the data of the data producer. For example, it is often a platform that users can only use (Facebook, Twitter, Google + etc) by agreeing to transfer certain rights of their data to the provider (third party). Any broker who transfers data from one provider to a buyer and receives the data is a third party. A direct purchaser of user data is also a third party in this sense.

A user device can include any electronic application that has an input and an output or interface to process the data. The user device may also include any type of data processing device capable of receiving and transmitting data over a network. For example, the user device can be a computer, a mobile phone, a laptop, a tablet, a server, a smart watch or any combination of these devices. The user device is there to record the data of a data producer. In the case of a machine being a data producer, the data producer is the same as the user device.

The user device has a first application. The first application is a software (application) that can record data. The recording can be done by different sources. The recording can be done for example by a direct input of a user or data producer into the user device, or by measured data by corresponding sensors on the device or in its environment. External sources, such as existing databases from the Internet, for example, can also be used to record data on the user device.

After the first application of the user device has gained access to the data sources, it can call a second software-based interface that initiates a new storage step. The second software-based interface can be divided into a data interface and a connection interface. These interfaces are e.g. open source and can be implemented flexibly in any kind of application. This has the advantage that the inventive method and system can be used independently of an operating system of the user or data producer. These two interfaces can be used to encrypt and store all types of data generated by the application. The interfaces can also update the metadata stored on the main system. Preferably, the application itself must trigger events that lead to the activation of the continuation of the inventive process.

When the second software-based interface is called by the first application on the user device, the data interface automatically executes the connection interface and authenticates both the user and the application on a main system. The main system validates the information sent and responds with a suitable globally valid data model, which is redirected to the data interface and with which the data is reconstructed or normalized before it is stored.

A data model determines how the structure of the data is defined and in what form the data is stored. Data models are used for all participating data interfaces to create a general standard for each type of data in different applications. The inventive data model is globally valid. It defines how values are stored in a locally encrypted database. Furthermore, the data model can be used to detect rule violations, which has the advantage that a constant degree of quality and consistency can be guaranteed. The globally valid data model defines different units, length and structure of the stored data, so that a further continuation of the inventive process is possible in an analysis processing entity. Continuation is only possible if the data is accurate, reliable and standardized formatted. The application itself must also ensure that the generated data meets the requirements of the data model. If the data does not meet these requirements, the data will not be accepted by the data interface and a further continuation will be suspended in this case. The normalization is based on an interpretation of the data before the data is stored in a local database. The standardization process reformats the data and creates a consistent data representation with fixed and discrete columns based on the data model. The advantage of standardization is that the conformity of the data guarantees simpler and secure further processing of the data, or as error-free as possible. All data models are provided in such a way that they comply with the standard or other conventions. The globally valid data model is retrieved via an interface for the first application. The data model is retrieved via the main system.

A local database is an encrypted storage unit in which data is stored consistently, efficiently, consistently and permanently. The data interface allows the connected application to delete, store, retrieve and modify information from the database that is based on globally valid data models. The data models also include features of other common databases. These are for example formatting of fixed column width and the corresponding tables are limited to certain data types. Entries in the database can correspond to the tuple definition within relational algebra with all values separated by separators.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Short description of the illustrations

Fig. 1 Method for generating data from a data producer

Fig. 2 Inventive procedures for the protection of electronic data for the purpose of data processing by third parties, including transparent and interruption-proof remuneration

Fig. 3 Remuneration process of a data producer and a plug-in provider according to the inventive process with so-called smart contracts

Detailed description

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

List of reference characters

1	decentralized application
10	data
20	data producer
30	a third party
32	request
34	requester
40	user device
41	first application
42	second software-based interface
43	data interface
44	connection interface
45	direct input of a user
46	measured data by sensors
47	external data sources
48	local database

50	main system
52	globally valid data model
60	analysis processing entity
62	analysis result
70	plug-in provider
80	smart contract
100	inventive method
210	encryption of the data of the data producer with public key of a second key pair
220	sending the encrypted data of the data producer to the analysis processing entity
310	transfer crypto currency to the smart contract
410	recording of data in the first application of the user device
420	retrieve the second software-based interface of the user device
430	automatic triggering of a connection interface within the second software-based interface of the user device
440	authentication of the data producer and the first application on a main system
450	sending a globally valid data model from the main system to the second software-based interface of the user device
460	standardization of data in the second software-based interface
470	encryption and storage of standardized data in a local database on the user device
480	sending information about type and number of stored records to the main system
510	request to the main system for an analysis result
520	assignment of a first key pair from the main system to the requestor
530	retrieve the analysis processing entity
540	waiting for receipt of a block with payment from the requestor
550	sending the identifier
560	transfer of the plug-in provider's wallet ID to smart contract
610	dynamic generation of a second key pair at runtime
620	sending the public key from the second key pair to the data producer
630	decryption of the data of the data producer by the analysis processing Entity

640	analysis of the decrypted data of the data producer by the analysis processing entity
650	sending the encrypted analysis result to the requester
810	sending a message with identifier
820	reimbursement of the data producer
830	reimbursement of the plug-in provider
1000	inventive system

Claims

1. A method (100) for the security protection of data (10) of a data producer (20) suitable for processing by a third party (30), comprising:
   - recording (410) of the data (10) by a user device (40) of the data producer (20) and a first application (41);
   - retrieving (450) a globally valid data model (52) via a second software-based interface (42) with interface to the first application (41);
   - normalizing (460) the data (10) via a second software-based interface (42) using the globally valid data model (52);
   - storing (470) the normalized data in a local encrypted database (48), the number and type of the encrypted data being communicated (480) to a main system (50);
   - calling (530) an analysis processing entity (60) located on a separate physical unit to the main system (50) and executed in a secured execution environment when the main system (50) receives (510) a request (32), wherein a first key pair (36) is assigned (520) to a requester (34) by the main system (50);
   - dynamically generating (610) a second key pair (22) by the analysis processing entity (60) at runtime;
   - sending (620) a public key (24) from the second key pair (22) to the data producer (20), whereby the data producer (20) encrypts (210) the requested data before transmission to the main system (50) and then to the analysis processing entity (60);
   - transferring (220) the encrypted data via the main system (50) back to the analysis processing entity (60), from where the requested data is decrypted (630) and analyzed within the secured execution environment with a private key (26) from the second key pair (22) and an analysis result (62) is generated (640);
   - sending (650) the analysis result (62), which is encrypted with a public key (38) from the first key pair (36) of the requester (34), the analysis processing entity (60) to the main system (50) for inspection by the requester (34), wherein only the requester (34) can decrypt the analysis result (62) using a private key (39) from the first key pair (36), so that the analysis result (62) can only be viewed by the requester (34) and the data (10) can only be viewed by

the data producer (20), thereby ensuring the security protection of the data (10) in the processing of third parties (30).

2. The procedure (100) according to claim 1,
is characterized in a way,
in that the second software-based interface (42) is divided into a data interface (43) and a connection interface (44). The data interface (43) checks the type and number of data generated and the connection interface (44) establishs a connection to the main system (50). The main system (50) returns rules for data conformity to the second software-based interface (42) using the globally valid data model (52) so that the data in the data interface (43) can be normalized according to the rules of conformity.

3. The procedure (100) according to claim 1 and 2,
is characterized in a way,
that the main system (50) is a cloud application or a decentralized application (1).

4. The procedure (100) according to one of the foregoing claims
is characterized in a way,
that the encryption of the database (48) is performed asymmetrically or symmetrically by common algorithms.

5. The procedure (100) according to one of the foregoing claims
is characterized in a way,
in that the request (32) contains the type and number of data (10) required for the analysis result (62), as well as an identification identifier of an executing algorithm, so-called plug-ins, the executing algorithms being provided by plug-in providers (70) so that the main system (50) can include the corresponding data producers (20) and plug-in providers (70) for analyzing the data (10) of the requestor (34).

6. The procedure (100) according to claim 5,
is characterized in a way,
that the request (32) contains a sum of a remuneration for the analysis result (62) which is sent to the analysis processing entity (60) together with a wallet ID and a

remuneration claim of the data producer (20) for its data (10), wherein the analysis processing entity (60) checks whether the remuneration claim is part of the sum of the remuneration for the analysis result (62).

7. The procedure (100) according to one of the foregoing claims
is characterized in a way,
that the remuneration is paid in cryptocurrency in order to make the course of the remuneration transparent and unfalsifiable.

8. The procedure (100) according to claim 5 and 6,
is characterized in a way,
that the plug-in provider (70) provides the analysis processing entity (60) with an executing algorithm that can analyze the data (10), wherein the plug-in provider (70) receives a portion of the sum of the remuneration, if the executing algorithm uploaded by it to the main system (50) is used to process the data (10) without obtaining access to the data (10) of the data producer (20), which guarantees the data (10) protection during processing.

9. A system (1000) for the security protection of data (10) of a data producer (20), suitable for processing by a third party (30) according to the inventive method (100) in claim 1, involves:
   - data (10) recorded by a user device (40) of the data producer (20) and a first application (41);
   - a globally valid data model (52) which is retrieved via a second software-based interface (42) with an interface to the first application (41);
   - data (10) that is normalized via the second software-based interface (42) using the globally valid data model (52);
   - normalized data stored in a local encrypted database (48), the number and type of encrypted data being communicated to a main system (50);
   - an analysis processing entity (60) located on a separate physical unit to the main system (50) and executed and called in a secured execution environment when the main system (50) receives a request (32), wherein a first key pair is assigned to a requester (34) from the main system (50);

- a second key pair which is dynamically generated by the analysis processing entity (60) at runtime;
- a public key from the second key pair sent to the data producer (20), whereby the data producer (20) encrypts the requested data before transmission to the main system (50) and then to the analysis processing entity (60);
- encrypted data of the data producer (20) that is transferred back to the analysis processing entity (60) via the main system (50), from where the requested data is decrypted and analyzed with a private key from the second key pair within the secured execution environment and an analysis result (62) is generated;
- an analysis result (62) encrypted with a public key from the first key pair of the requester (34) and sent by the analysis processing entity (60) to the main system (50) for inspection by the requester (34), wherein the analysis result (62) can only be decrypted by the requester (34) using a private key from the first key pair, so that the analysis result (62) can only be viewed by the requester (34) and the data (10) can only be viewed by the data producer (20), thereby ensuring the security protection of the data (10) in the processing of third parties (30).

Recap

It is the task of the present invention to provide an automated and modular system (1000) with a method (100) which enables access to analysis results (62) on the basis of different types of data (10) from different sources, while preserving the privacy of the data producers (20) and at the same time protecting the data (10) itself from unauthorized access. The system (1000) and the procedure (100) also comply with all the guidelines of the European Data Protection Declaration and also offer an opportunity to fairly compensate participants for their share of the data (10) for the analysis results (62).

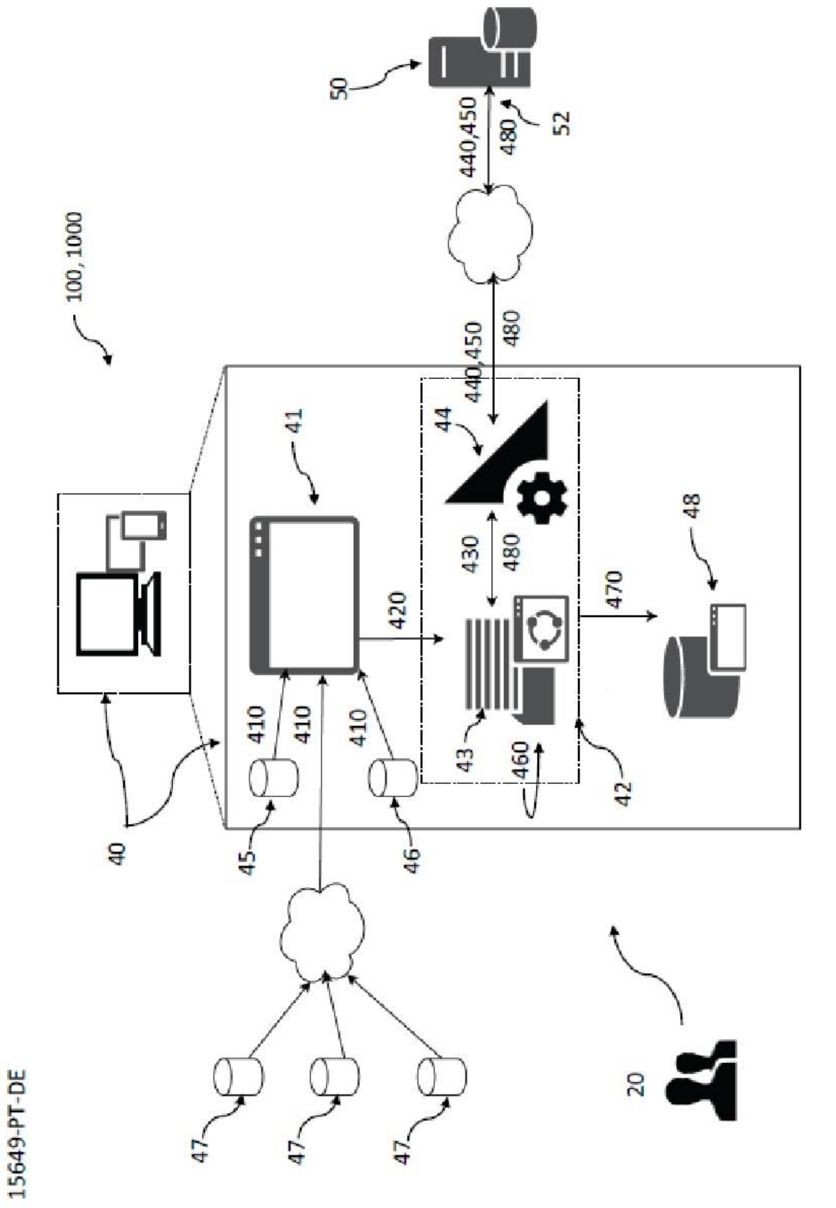
15649-PT-DE
100, 1000
50
52
440,450
480
440,450
480
41
44
430
480
420
470
48
410
410
410
43
460
42
40
45
46
47
47
47
20

Fig.1

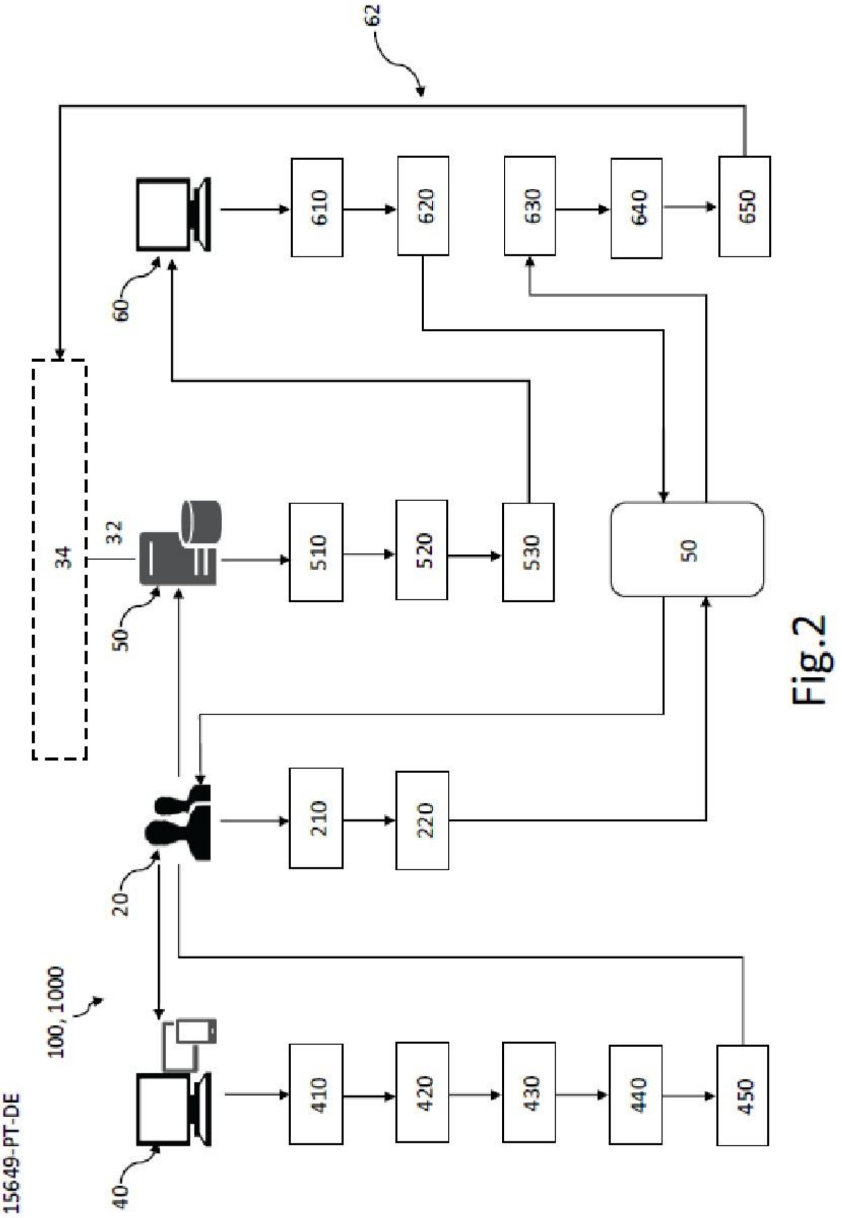
15649-PT-DE
100, 1000
40
20
50
32
34
60
62
410
420
430
440
450
210
220
510
520
530
50
610
620
630
640
650

Fig.2

15649-PT-DE

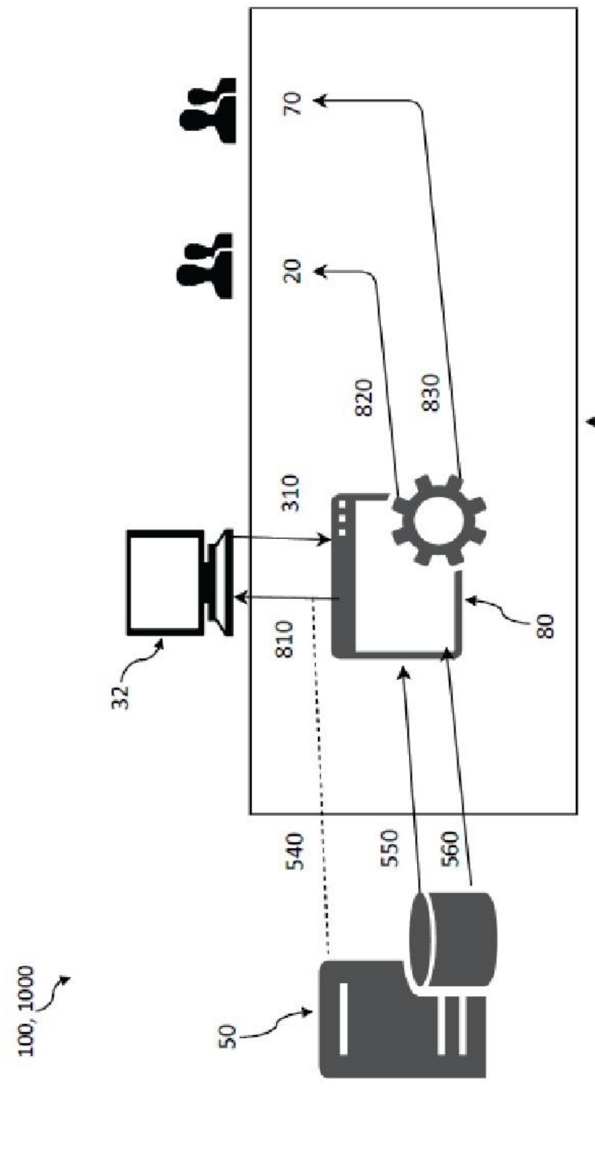

Fig.3