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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2018 (15.02.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/031342 A1

(51) International Patent Classification:
G06F 21/60 (2013.01) *H04L 9/08* (2006.01)
G06F 17/30 (2006.01) *G06F 15/173* (2006.01)

(21) International Application Number:
PCT/US2017/045149

(22) International Filing Date:
02 August 2017 (02.08.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/226,237 02 August 2016 (02.08.2016) US

(72) Inventor; and
(71) Applicant: **LEWIS, Paul** [US/US]; 120 Apgar Way, Asbury, NJ 08802 (US).

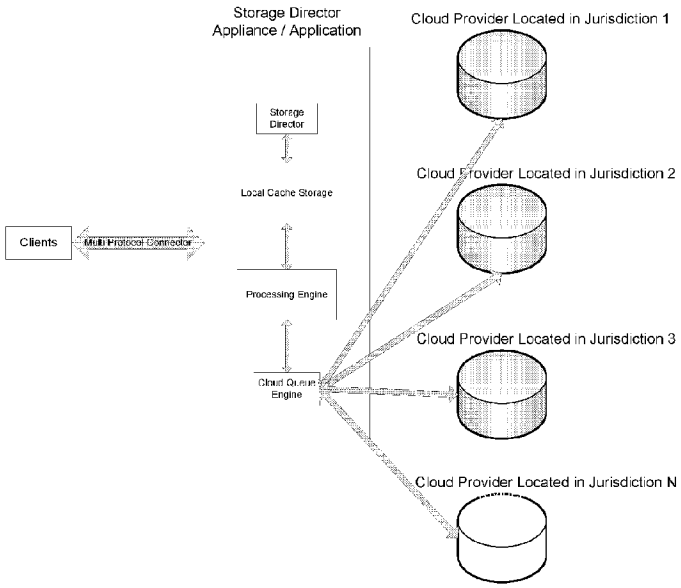
(74) Agent: **POSTOLSKI, David**; 41 River Road, Summit, NJ 07901 (US).

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

(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,

(54) Title: JURISDICTION INDEPENDENT DATA STORAGE IN A MULTI-VENDOR CLOUD ENVIRONMENT

FIGURE 1



(57) Abstract: A cloud based system for providing data security, the system having a processor which creates a source data file; wherein the source data file is split into at least one fragments; an encryption key associated with the at least one fragments; and wherein the at least one fragments is encrypted by the encryption key; a plurality of cloud storage providers; wherein the at least one fragments is distributed among the plurality of cloud storage providers whereby no single cloud storage provider possesses all of the at least one fragments; a pointer file which is created on a local computer; wherein the pointer file stores the location of the at least one fragments; and wherein the pointer file is accessed; the encryption key authenticates the plurality of cloud storage providers; the at least one fragments are transferred from the plurality of cloud storage providers to the local computer; and wherein the at least one fragments are reassembled; and the source data file is deleted.

WO 2018/031342 A1

[Continued on next page]

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))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
— *with information concerning one or more priority claims considered void (Rule 26bis.2(d))*

JURISDICTION INDEPENDENT DATA STORAGE IN A MULTI-VENDOR CLOUD ENVIRONMENT

Claim of Priority

This application claims priority of the U.S. utility application number 14/25,612 filed on June 30, 2014 and U.S. provisional patent application number 61/812,115 filed on April 15, 2013, the contents of both of which are fully incorporated herein by reference.

Field of the Embodiments

This invention relates to data protection and security in a cloud based environment. In particular, the invention allows data to be stored in a cloud environment whereby it is inaccessible to any third party and not subject to data privacy laws of any given jurisdiction.

Background of the Embodiments

With the advent of the internet, cyber security and data privacy is a growing global concern in today's world. Information technology and electronic discovery advances in a variety of industries, including the legal industry have compounded the issue. The United States and many foreign countries have enacted strict and stringent requirements on data privacy and security. Global entities and multinational corporations have struggled to comply with local data privacy laws. Data privacy laws define how companies and individuals must store and manage computer data. However, the laws are complex and sometimes the laws of one jurisdiction are in direct conflict with the laws of another jurisdiction. This has caused companies to give much thought as to how and where it stores their protected data. Because of the evolution of

technology, companies are migrating away from managing and storing data internally, and opting instead to store data with a third party. The third party provider provides the physical infrastructure and maintains the data for a large number of customers. This scenario is generally known as the "cloud" or a virtual storage system. Such cloud based systems are used by many companies, but each is maintained by a single cloud service provider or "cloud vendor".

The development of the cloud has introduced many new challenges for companies. Customers are unclear as to what jurisdiction contains their inactive digital data (i.e. data at rest), since a cloud customer does not know where a cloud vendor maintains its actual physical infrastructure. Other challenges involve data security. Cloud environments can be compromised by hackers or by a company's internal employees ultimately leading to an organization's data being accessed or transferred. If the data is sensitive, such as personally identifiable information ("PII"), the company may be required to make a mandatory disclosure to its customers. In some cases, the company is not aware of such an invasion, and thereby may not make the disclosure they are required to make. In addition, a cloud vendor may go offline or go out of business, thereby creating a potential situation where a subscriber cannot access its own data. The present invention solves many of these and other challenges.

The present invention relates to a cloud based system including the creation of a system which causes computer data to be redundant and jurisdiction independent. In the present application, a data file is segmented and encrypted wherein each data file segment is striped across multiple cloud service providers. Thus, in the event each cloud service provider maintains physical storage in a different jurisdiction, then each encrypted segment will be at rest in a different jurisdiction. Therefore, each encrypted segment contains no readable data on its own, and must be reassembled with its other segments before the whole can be decrypted. Only

once the segments from different jurisdictions are assembled can it be decrypted and read. The disclosed system enables a data file to be jurisdictionally independent until it is reassembled, and once the data is reassembled will it be able to be governed. The present application enables a company to subscribe to many cloud vendors, and not have to worry about their data at rest. For example, during the legal discovery process, a company can choose the jurisdiction for data production simply by reassembling its data in that jurisdiction.

Summary of the Embodiments

The present embodiment of the invention relates to a cloud based system for providing data security. The system comprises a processor; said processor creates a source data file; wherein said source data file is split into at least one fragments; an encryption key; said encryption key associated with the at least one fragments; and wherein the at least one fragments is encrypted by the encryption key; a plurality of cloud storage providers; wherein the at least one fragments is distributed among the plurality of cloud storage providers whereby no single cloud storage provider possesses all of the at least one fragments; a pointer file; wherein said pointer file is created on a local computer; wherein said pointer file stores the location of the at least one fragments; and wherein said pointer file is accessed; said encryption key authenticates the plurality of cloud storage providers; the at least one fragments are transferred from the plurality of cloud storage providers to the local computer; wherein the at least one fragments are reassembled; and the source data file is deleted. The system further comprises an encryption key created by the user. The system further comprises the encryption key being auto generated by the processor. The system further comprises the pointer file being stored locally on a user's computer and wherein the pointer file further comprises a lookup table.

A computer implemented method for providing data security in a cloud based system, the method comprising: creating via a processor, a source data file; splitting, via a processor said source data file into at least one fragments; associating, via a processor an encryption key with the at least one fragments; encrypting, via a processor the at least one fragments by the encryption key; distributing, via a processor the at least one fragments among a plurality of cloud storage providers; whereby no single cloud storage provider possesses all of the at least one fragments; creating a pointer file on a local computer; wherein said pointer file; storing the location of the at least one fragments; accessing said pointer file; authenticating, via a processor the plurality of cloud storage providers by the encryption key; transferring, via a processor; the at least one fragments from the plurality of cloud storage providers to the local computer; reassembling, via a processor the at least one fragments; and wherein the source data file is deleted.

A cloud based system for providing data security, the system comprising; a processor; said processor creates a source data file; wherein said source data file is split into at least one fragments; an encryption key; said encryption key created by a first user and associated with the at least one fragments; and wherein the at least one fragments is encrypted by the encryption key; a plurality of cloud storage providers; wherein the at least one fragments is distributed among the plurality of cloud storage providers whereby no single cloud storage provider possesses all of the at least one fragments; a pointer file; wherein said pointer file is created on a first local computer and the source data file is deleted; wherein said pointer files stores the location of the at least one fragments; and wherein said pointer file and said encryption key is shared with a second user; wherein said pointer file is accessed by the second user on a second local computer; and wherein the second user uses said encryption key to authenticate the plurality of cloud storage

providers; the at least one fragments are transferred from the plurality of cloud storage providers to the second local computer of the second user; wherein the at least one fragments are reassembled by the second user on the second local computer. The system further comprises the encryption key and pointer file being shared with the second user through encrypted transmission methods. The system further comprises the encryption key being created by the first user. The system further comprises the encryption key being auto generated by the processor. The system further comprises the pointer file being stored locally on a first or second user's computer and wherein the pointer file further comprises a lookup table.

A computer implemented method for providing data security in a cloud based system, the method comprising: creating via a processor, a source data file on a first local computer of a first user; splitting, via a processor said source data file into at least one fragments; wherein the first user is creating an encryption key and Associating, via a processor the encryption key with the at least one fragments; encrypting, via a processor the at least one fragments by the encryption key; distributing, via a processor the at least one fragments among a plurality of cloud storage providers; whereby no single cloud storage provider possesses all of the at least one fragments; creating a pointer file on the first local computer whereby the source data file is deleted; wherein said pointer file and the encryption is shared by the first user to a second user; and wherein said pointer file stores the location of the at least one fragments; and wherein the second user is accessing said pointer file and using said encryption key to authenticate the plurality of cloud storage provider; and cause the transferring of the at least one fragments from the plurality of cloud storage providers to a second local computer of the second user; and wherein the at least one fragments are reassembled on the second local computer of the second user.

Brief Description of the Drawings

Figure 1 shows the preferred embodiment of the system of the invention.

Figure 2 show the preferred method of the invention.

Figure 3 shows a graphical representation of the flow of a data file and data blocks in the system.

Description of the Preferred Embodiments

The preferred embodiments of the present invention will now be described with reference to the drawings. Identical elements in the various figures are identified with the same reference numerals.

Reference will now be made in detail to each embodiment of the present invention. Such embodiments are provided by way of explanation of the present invention, which is not intended to be limited thereto. In fact, those of ordinary skill in the art may appreciate upon reading the present specification and viewing the present drawings that various modifications and variations can be made thereto.

Figure 1 shows the process flow of data through the cloud based system of the present application. The process commences with a native data file, the data file is encrypted and broken into segmented parts, and the segmented data file is then forwarded to multiple cloud storage providers located in multiple jurisdictions. A client (or multiple clients) connects to a Storage Director Appliance or Software Application through a Multi-Protocol Connector. The multi-protocol connector may be via a web browser through the Internet. The Storage Director Appliance or Application has the ability to locally store a cached file in a local cache storage. The file is processed by a processing engine where it is encrypted and separated into "n" parts. Each of the parts are passed on to the Cloud Queue Engine, which transmits and deposits the

segmented parts to multiple Cloud Providers located in multiple legal jurisdictions. When the file is requested by an authorized user, The Cloud Queue Engine retrieves a copy of each of "n" parts, downloads them to the Storage Director Appliance or Application, and processes the Segmented parts to re-create the original encrypted file. The encrypted file is decrypted, and the native file becomes available to the user.

Figure 2 shows a flow chart diagram that describes the process of taking a native file and securely storing it in one of multiple cloud vendors located in more than one jurisdiction. To reassemble the file, the process is simply reversed. In step 1, local or native data is received from a Client and ready for processing. In step 2, the file and location data are written to the Storage Director module Lookup Table. In step 3, the file is processed by the Processing Engine, where it is encrypted. The encrypted file is then broken into multiple data blocks, and each block is assigned a unique name or identifier. In step 4, the Storage Director module Lookup table is updated with the block name of each data block and the total Quantity of blocks that were created from the original encrypted file. In steps 5 the data blocks are Forwarded and moved to storage providers as per a preset algorithm as instructed by the Cloud Queue Engine or Module. In step 6, the blocks are forward and moved to one of multiple cloud storage providers which are located in multiple jurisdictions as instructed by the Cloud Queue Engine or Module. The blocks are stored at cloud providers located in different jurisdictions. In step 7, the Storage Director module lookup table is updated with the data location of each block at each Cloud Provider.

In figure 3 a graphical representation of the data flow is shown. Figure 3 also illustrates how data blocks are securely and redundantly stored across Cloud Providers in "n" jurisdictions. Once a native data file is encrypted and broken into data blocks by the Storage Director Appliance or Application, the Cloud Queue Engine or module distributes the blocks to "n" Cloud

Providers in "n" legal jurisdictions. Each data block is written to two or more Cloud Providers, which "stripes" the data across multiple providers in varying jurisdictions. If a given Cloud Provider is compromised by going offline and unavailable, the Cloud Queue Engine can still retrieve the data blocks from another Cloud Provider. In addition, if a given Cloud Provider is compromised by a hacker or unauthorized user, the data blocks that may have been compromised are of no value to the hacker, because the hacker will only be in possession of encrypted blocks, and not any entire file.

The present embodiments relate to a systems and methods for secure data storage in a multi-vendor cloud environment in a manner that prevents the third party cloud provider from being able to access or be in possession of complete data files. The computer or device that creates the source data distributes only a portion of a data file to each of a plurality of cloud storage providers. The source computer or device maintains a lookup table and is able to re-assemble the data. Each storage provider only maintains part of each data file, and therefore is never in possession of any complete data file(s). The source computer or device can retrieve each portion of the file from multiple cloud providers, whereby the portions are re-assembled into the complete data file by using the lookup table. The system allows for large amounts of data to be stored across a plurality of third party cloud storage providers in a manner that prevents any third party from having access to any complete file. The data is distributed globally among a plurality of cloud storage providers. No single cloud provider has access to any complete file, as each file is broken into Encrypted segments or data blocks and only one Data block is sent to each cloud provider. Each cloud provider is in a different physical location across multiple jurisdictions. As a result, the file does not exist at rest in any one jurisdiction,

thus is not subject to legal and/or regulatory requirements of any single jurisdiction while it is stored in a multi-vendor cloud environment.

The system ensures that any data file stored in a multi-vendor cloud environment in this manner cannot be subject to the laws governing production of, privacy of, or protection of data in any jurisdiction.

In another embodiment, a system and method for securely sharing data files by using a multi-vendor cloud environment in a manner that prevents any third party from being able to access or be in possession of the original source data file is taught. The computer or device that creates the source data splits each file into multiple segments. Each segment is then encrypted using an encryption key defined by the user. Each of the encrypted fragments are then distributed to multiple cloud properties whereby only a portion of the fragments of the source data file is stored to any one of a plurality of cloud storage providers. The source computer or device maintains a pointer file that contains a lookup table and is able to re-assemble the data if it knows the encryption key and has access to the same cloud properties. Each storage provider only maintains part of each data file, and therefore is never in possession of any complete data file(s). Any computer or device that has possession of the pointer file, knows the encryption key, and has access to the cloud provider storage can retrieve each portion of the file from multiple cloud providers, whereby the portions are downloaded, decrypted using the user generated encryption key stored in the pointer file, and re-assembled into the complete data file by using the lookup table. The system allows for large amounts of data to be stored across a plurality of third party cloud storage providers in a manner that prevents any third party from having access to any complete file. The data is safe from being exploited or hacked by any third party, since

even if all cloud providers are breached, the data cannot be re-assembled without the encryption key and the lookup table.

In this embodiment, the method comprises; a source data file is created, the source data file is split into fragments; an encryption key is created by the user; each fragment is encrypted using the encryption key; the fragments are distributed in multiple cloud storage providers, whereby no single cloud storage provider is in possession of all fragments; a pointer file is created that stores the location of each fragment; the pointer file is stored locally, and the original file is deleted. The user is able to open the pointer file, enter the encryption key, and authenticate to the cloud storage providers. Each fragmented is transferred from the cloud storage providers to the local computer. The fragments are re-assembled locally on the computer.

In another embodiment, a system and method for securely sharing data files by using a multi-vendor cloud environment in a manner that prevents any third party from being able to access or be in possession of the original source data file is taught. The computer or device that creates the source data splits each file into multiple segments. Each segment is then encrypted using an encryption key defined by the user. Each of the encrypted fragments are then distributed to multiple cloud properties whereby only a portion of the fragments of the source data file is stored to any one of a plurality of cloud storage providers. The source computer or device maintains a pointer file that contains a lookup table and is able to re-assemble the data if it knows the encryption key and has access to the same cloud properties. The pointer file can be freely shared with other users using any data transmission method, including email, copy/paste, etc. Each storage provider only maintains part of each data file, and therefore is never in

possession of any complete data file(s). Any computer or device that has possession of the pointer file, knows the encryption key, and has access to the cloud properties can retrieve each portion of the file from multiple cloud providers, whereby the portions are downloaded, decrypted using the user generated encryption key stored in the pointer file, and locally re-assembled into the complete data file. The system allows for large amounts of data to be stored across a plurality of third party cloud storage providers in a manner that prevents any third party from having access to any complete file, unless the source user shares the pointer file, encryption key, and access to the cloud properties. The data at rest is safe from being exploited or hacked by any third party, since even if all cloud providers are breached, the data cannot be re-assembled without the pointer file, encryption key, and access to a complete set of fragments.

In this embodiment, the method comprises: a source data file is created; the source data file is split into fragments; an encryption key is created by user #1; each fragment is encrypted using the encryption key; the fragments are distributed in multiple cloud storage providers, whereby no single cloud storage provider is in possession of all fragments; a pointer file is created that stores the location of each fragment; the pointer file is stored locally, and the original file is deleted. The pointer file is shared with user #2. User #2 is able to access the fragments stored at the cloud storage providers; User #2 has knowledge of the encryption key; User #2 is able to open the pointer file, enter the encryption key, and authenticate to the cloud storage providers. Each fragmented is transferred from the cloud storage providers to the local computer of user #2. The fragments are re-assembled locally on the computer of user #2.

The advantages and features of the application are of a representative sample of embodiments only, and are not exhaustive and/or exclusive. They are presented only

to assist in understanding and teach the claimed principles. It should be understood that they are not representative of all disclosed embodiments. As such, certain aspects of the disclosure have not been discussed herein. That alternate embodiments may not have been presented for a specific portion of the invention or that further undescribed alternate embodiments may be available for a portion is not to be considered a disclaimer of those alternate embodiments. It will be appreciated that many of those undescribed embodiments incorporate the same principles of the invention and others are equivalent. Thus, it is to be understood that other embodiments may be utilized and functional, logical, organizational, structural and/or topological modifications may be made without departing from the scope and/or spirit of the disclosure. As such, all examples and/or embodiments are deemed to be non-limiting throughout this disclosure. Also, no inference should be drawn regarding those embodiments discussed herein relative to those not discussed herein other than it is as such for purposes of reducing space and repetition. For instance, it is to be understood that the logical and/or topological structure of any combination of any program components (a component collection), other components and/or any present feature sets as described in the figures and/or throughout are not limited to a fixed operating order and/or arrangement, but rather, any disclosed order is exemplary and all equivalents, regardless of order, are contemplated by the disclosure. Furthermore, it is to be understood that such features are not limited to serial execution, but rather, any number of threads, processes, services, servers, and/or the like that may execute asynchronously, concurrently, in parallel, simultaneously, synchronously, and/or the like are contemplated by the disclosure. As such, some of these features may be mutually contradictory, in that they

cannot be simultaneously present in a single embodiment. Similarly, some features are applicable to one aspect of the invention, and inapplicable to others. In addition, the disclosure includes other inventions not presently claimed. Applicant reserves all rights in those presently unclaimed inventions including the right to claim such inventions, file additional applications, continuations, continuations in part, divisions, and/or the like thereof. As such, it should be understood that advantages, embodiments, examples, functional, features, logical, organizational, structural, topological, and/or other aspects of the disclosure are not to be considered limitations on the disclosure as defined by the claims or limitations on equivalents to the claims. It is to be understood that, depending on the particular needs and/or characteristics of a individual and/or enterprise user, database configuration and/or relational model, data type, data transmission and/or network framework, syntax structure, and/or the like, various embodiments of the system may be implemented that enable a great deal of flexibility and customization.

All statements herein reciting principles, aspects, and embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

Descriptions herein of method steps and computer programs represent conceptual embodiments of illustrative circuitry and software embodying the principles of the disclosed embodiments. Thus the functions of the various elements shown and described herein may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software as set forth herein.

In the disclosure hereof any element expressed as a means for performing a specified function is intended to encompass any way of performing that function including, for example, a) a combination of circuit elements and associated hardware which perform that function or b) software in any form, including, therefore, firmware, microcode or the like as set forth herein, combined with appropriate circuitry for executing that software to perform the function. Applicants thus regard any means which can provide those functionalities as equivalent to those shown herein.

Similarly, it will be appreciated that the system and process flows described herein represent various processes which may be substantially represented in computer-readable media and so executed by a computer or processor, whether or not such computer or processor is explicitly shown. Moreover, the various processes can be understood as representing not only processing and/or other functions but, alternatively, as blocks of program code that carry out such processing or functions.

The methods, systems, computer programs and mobile devices of the present disclosure, as described above and shown in the drawings, among other things, provide for improved social networking platforms and aspects thereof. It will be apparent to those skilled in the art that various modifications and variations can be made in the devices, methods, software programs and mobile devices of the present disclosure without departing from the spirit or scope of the disclosure. Thus, it is intended that the present disclosure include modifications and variations that are within the scope of the subject disclosure and equivalents.

Claims

What is claimed is:

1. A cloud based system for providing data security, the system comprising;

a processor; said processor creates a source data file; wherein said source data file is split into at least one fragments;

an encryption key; said encryption key associated with the at least one fragments; and wherein the at least one fragments is encrypted by the encryption key;

a plurality of cloud storage providers; wherein the at least one fragments is distributed among the plurality of cloud storage providers whereby no single cloud storage provider possesses all of the at least one fragments;

a pointer file; wherein said pointer file is created on a local computer; wherein said pointer file stores the location of the at least one fragments; and wherein said pointer file is accessed; said encryption key authenticates the plurality of cloud storage providers; the at least one fragments are transferred from the plurality of cloud storage providers to the local computer; wherein the at least one fragments are reassembled; and the source data file is deleted.

2. The system of claim 1, wherein the encryption key is created by the user.
3. The system of claim 1, further comprising, wherein the encryption key is auto generated by the processor.
4. The system of claim 1, wherein the pointer file is stored locally on a user's computer.
5. The system of claim 1, wherein the pointer file further comprises a lookup table.
6. A computer implemented method for providing data security in a cloud based system, the method comprising:

creating via a processor, a source data file;

splitting, via a processor said source data file into at least one fragments;

associating, via a processor an encryption key with the at least one fragments;

encrypting, via a processor the at least one fragments by the encryption key;

distributing, via a processor the at least one fragments among a plurality of cloud storage providers; whereby no single cloud storage provider possesses all of the at least one fragments;

creating a pointer file on a local computer; wherein said pointer file;

storing the location of the at least one fragments;

accessing said pointer file;

authenticating, via a processor the plurality of cloud storage providers by the encryption key;

transferring, via a processor; the at least one fragments from the plurality of cloud storage providers to the local computer;

reassembling, via a processor the at least one fragments; and wherein the source data file is deleted.

7. A cloud based system for providing data security, the system comprising;

a processor; said processor creates a source data file; wherein said source data file is split into at least one fragments;

an encryption key; said encryption key created by a first user and associated with the at least one fragments; and wherein the at least one fragments is encrypted by the encryption key;

a plurality of cloud storage providers; wherein the at least one fragments is distributed among the plurality of cloud storage providers whereby no single cloud storage provider possesses all of the at least one fragments;

a pointer file; wherein said pointer file is created on a first local computer and the source data file is deleted; wherein said pointer files stores the location of the at least one fragments; and wherein said pointer file and said encryption key is shared with a second user;

wherein said pointer file is accessed by the second user on a second local computer; and wherein the second user uses said encryption key to authenticate the plurality of cloud storage providers; the at least one fragments are transferred from the plurality of cloud storage providers to the second local computer of the second user; wherein the at least one fragments are reassembled by the second user on the second local computer.

8. The system of claim 7, wherein the encryption key and pointer file is shared with the second user through encrypted transmission methods.

9. The system of claim 7, wherein the encryption key is created by the first user.

10. The system of claim 1, further comprising, wherein the encryption key is auto generated by the processor.

11. The system of claim 7, wherein the pointer file is stored locally on a first or second users computer.

12. The system of claim 1, wherein the pointer file further comprises a lookup table.

13. A computer implemented method for providing data security in a cloud based system, the method comprising:

creating via a processor, a source data file on a first local computer of a first user;

splitting, via a processor said source data file into at least one fragments;

wherein the first user is creating an encryption key and Associating, via a processor the encryption key with the at least one fragments;

encrypting, via a processor the at least one fragments by the encryption key;

distributing, via a processor the at least one fragments among a plurality of cloud storage providers; whereby no single cloud storage provider possesses all of the at least one fragments;

creating a pointer file on the first local computer whereby the source data file is deleted;

wherein said pointer file and the encryption is shared by the first user to a second user; and

wherein said pointer file stores the location of the at least one fragments; and

wherein the second user is accessing said pointer file and using said encryption key to authenticate the plurality of cloud storage provider; and cause the transferring of the at least one fragments from the plurality of cloud storage providers to a second local computer of the second user; and

wherein the at least one fragments are reassembled on the second local computer of the second user.

FIGURE 1

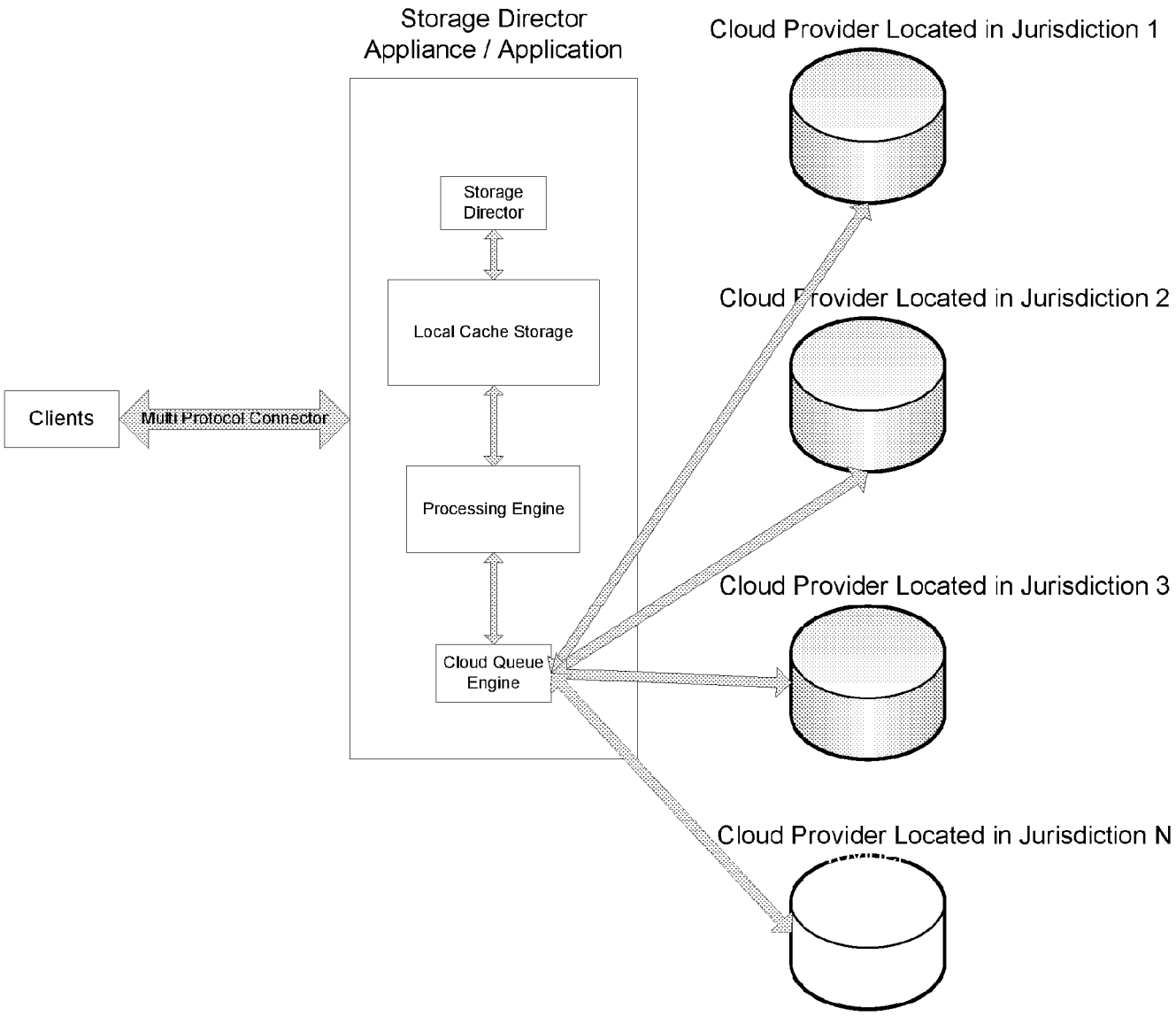

Storage Director
Appliance / Application
Storage
Director
Local Cache Storage
Processing Engine
Cloud Queue
Engine
Clients
Multi Protocol Connector
Cloud Provider Located in Jurisdiction 1
Cloud Provider Located in Jurisdiction 2
Cloud Provider Located in Jurisdiction 3
Cloud Provider Located in Jurisdiction N

FIGURE 2

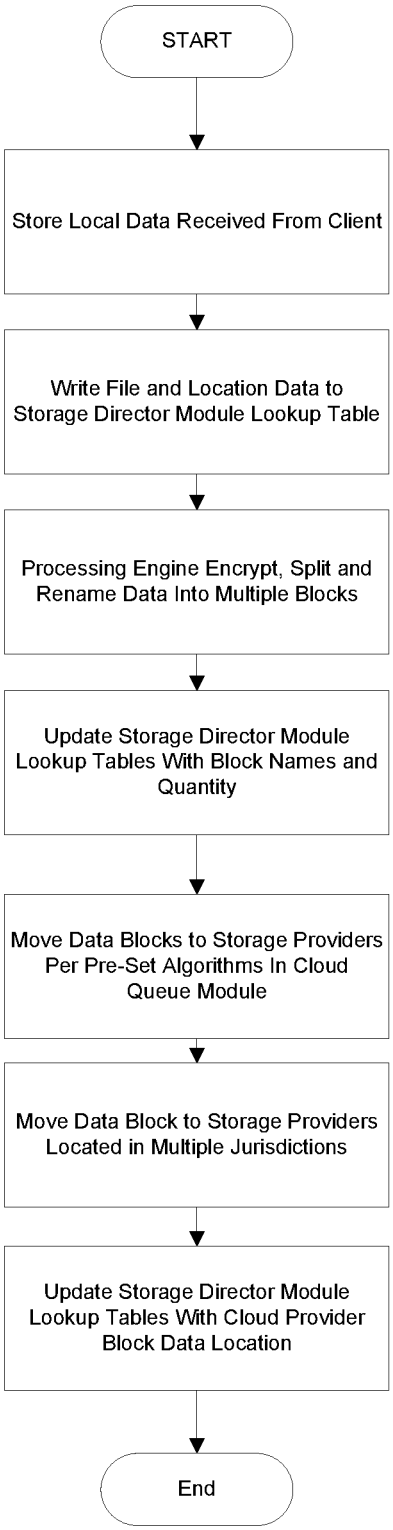
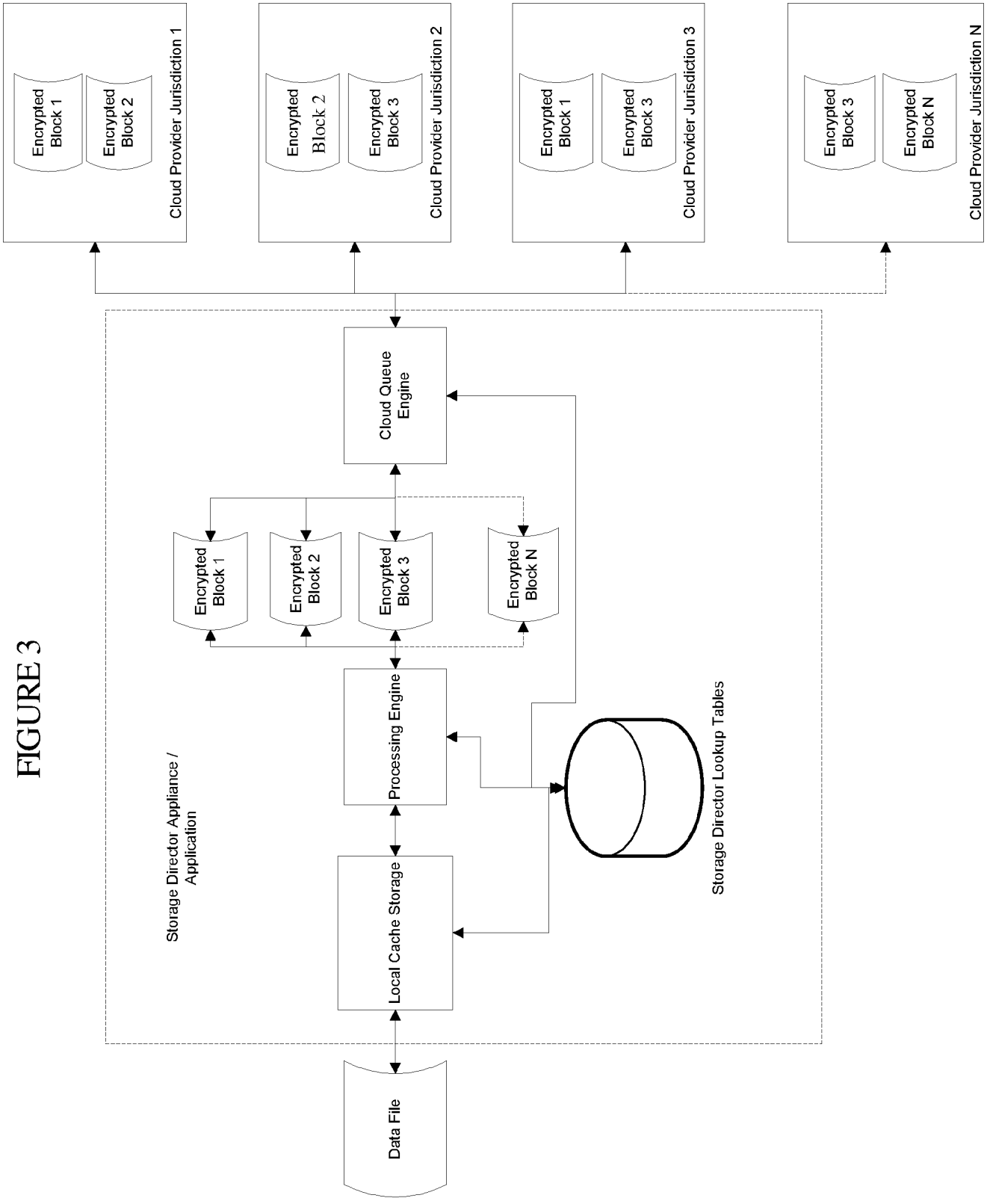

START
Store Local Data Received From Client
Write File and Location Data to Storage Director Module Lookup Table
Processing Engine Encrypt, Split and Rename Data Into Multiple Blocks
Update Storage Director Module Lookup Tables With Block Names and Quantity
Move Data Blocks to Storage Providers Per Pre-Set Algorithms In Cloud Queue Module
Move Data Block to Storage Providers Located in Multiple Jurisdictions
Update Storage Director Module Lookup Tables With Cloud Provider Block Data Location
End

FIGURE 3


Cloud Provider Jurisdiction 1
Encrypted Block 1
Encrypted Block 2
Cloud Provider Jurisdiction 2
Encrypted Block 2
Encrypted Block 3
Cloud Provider Jurisdiction 3
Encrypted Block 1
Encrypted Block 3
Cloud Provider Jurisdiction N
Encrypted Block 3
Encrypted Block N
Cloud Queue Engine
Encrypted Block 1
Encrypted Block 2
Encrypted Block 3
Encrypted Block N
Processing Engine
Storage Director Lookup Tables
Storage Director Appliance / Application
Local Cache Storage
Data File

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2017/045149

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60 *(2013.01)*
G06F 17/30 *(2006.01)*
H04L 9/08 *(2006.01)*
G06F 15/173 *(2006.01)*

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)

G06F 21/00, 21/60-21/64, 7/00, 12/00, 12/14, 15/00, 15/16, 15/163, 15/173, 17/00, 17/30, H04L 9/00, 9/08, 9/14

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)

PatSearch (RUPTO internal), USPTO, PAJ, K-PION, Esp@cenet, Information Retrieval System of FIPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/0084020 A1 (LI SHU) 01.05.2003, paragraphs [0002], [0017], [0019], [0051], [0066], [0090], [0097], [0100], [0105], [0113], claims 1, 5, fig. 11	1-13
Y	US 2011/0107103 A1 (MICHAEL PAUL DEHAAN et al.) 05.05.2011, paragraphs [0030], [0033], claims 1, 8	1-13
Y	US 2008/0183975 A1 (LYNN FOSTER et al.) 31.07.2008, paragraph [0071]	1-13
Y	WO 2013/101085 A1 (INTEL CORPORATION) 04.07.2013, abstract	3, 10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 December 2017 (06.12.2017)	07 December 2017 (07.12.2017)

Name and mailing address of the ISA/RU:
Federal Institute of Industrial Property,
Berezhkovskaya nab., 30-1, Moscow, G-59,
GSP-3, Russia, 125993
Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37

Authorized officer

T. Kiseleva

Telephone No. (499) 240-25-91