

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

Inventor:

DAVID A. REDBERG, residing at:
1059 Merrimac Dr.
Sunnyvale, CA 94087

Assignee: **FORTINET, INC.**
A Delaware Corporation

Entity: Regular Undiscounted

SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

COPYRIGHT NOTICE

[0001] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever. Copyright © 2013, Fortinet, Inc.

BACKGROUND

Field

[0002] Embodiments of the present invention generally relate to cloud based data storage. In particular, embodiments of the present invention relate to systems and methods for use of vendor independent secure cloud storage distribution and aggregation.

Description of the Related Art

[0003] Computing devices have traditionally executed applications and data services locally on respective devices, in which, as the data is accessed, processed, stored, cached, etc., it may travel within the devices over local buses, interfaces and other data pathways. As a result, users of such devices did not have to worry about interference or exposure of user data unless the device itself was lost or stolen. However, with the growing amount of data that is generated and with the evolution of online/Internet based services and cloud storage platforms, applications, content, and services are increasingly being moved to network providers who perform some or all of a given service on behalf of a user's devices. In such cases, a user may become concerned with who can access, or potentially worse, interfere with, the user's data while it is uploaded to a service, while it is stored by the service, or while it is retrieved from the service.

[0004] It has been recognized that while existing cloud storage providers offer a virtually infinite storage capacity, data owners seek geographical and provider diversity in data placement so that they are not tied to a particular service provider and have the flexibility to switch to

another provider without losing data or making significant efforts in data transition. Moreover, with the increasing criticality of data being stored, expectations of users to have more reliable mechanisms in place to ensure availability and durability of the content are also on the rise. On similar lines, instead of storing data within a single cloud, it may also be desired by users to store data across multiple cloud platforms to ensure more security, redundancy, and reduction in potential threat of data compromise.

[0005] Furthermore, storage of data in an unencrypted format is always at the risk of a network attack that may lead to the data being compromised. Storage of encrypted data, on the other hand, using existing technologies, makes the files, folders, filenames, and content thereof unsearchable and hence unfriendly for user access. Existing encryption techniques also expose the encrypted content to frequency analysis attacks. Moreover, since the cloud providers control the encryption keys, the data in the cloud can be exposed to attack within the cloud, insider jobs and subpoena – all without the knowledge or consent of the data owner.

[0006] Existing techniques for managing distribution and aggregation of content stored by a cloud provider also necessitate service provider and/or vendor specific application programming interfaces (APIs) to be incorporated for storage, access, and processing of the content, making present systems rigid and non-flexible to implementation of policies that allow storage of data across different service providers, allow different cloud storage access rights across users and computing devices, allow searching of downloaded encrypted data across cloud service vendors, among other desired activities.

SUMMARY

[0007] Methods and systems are described for vendor independent and secure cloud storage distribution and aggregation. According to one embodiment, a generalized application programming interface (API) is provided by a cloud storage gateway device that is logically interposed between one or more third-party cloud storage platforms and users of an enterprise. The API facilitates storing of files, issuing of search requests against the files and retrieval of content of the files. A file storage policy is assigned by the cloud storage gateway device to each user. The assigned file storage policy defines access rights, storage diversity requirements and a type of encryption to be applied to files for the corresponding user. Responsive to receiving, via the generalized API, a request to store a file, (i) creating, by the cloud storage gateway device, searchable encrypted data corresponding to content of the file and/or metadata associated with the file based on the assigned file storage policy; and (ii) distributing, by the cloud storage gateway device, the searchable encrypted data among one or more third-party cloud storage platforms based on the storage diversity requirements defined by the assigned file storage policy.

[0008] Other features of embodiments of the present disclosure will be apparent from accompanying drawings and from detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0010] **FIG. 1** illustrates an exemplary network architecture in accordance with an embodiment of the present invention.in accordance with an embodiment of the present invention.

[0011] **FIG. 2** illustrates exemplary functional modules of the proposed policy-based framework for secure cloud storage distribution and aggregation in accordance with an embodiment of the present invention.

[0012] **FIG. 3A** illustrates an exemplary flow diagram for generating searchable encrypted files in accordance with an embodiment of the present invention.

[0013] **FIG. 3B** illustrates an exemplary flow diagram for processing search queries for searching encrypted files in accordance with an embodiment of the present invention.

[0014] **FIGS. 4A-C** illustrate an example showing generation of searchable indices from search queries in order to execute search queries on encrypted files in accordance with an embodiment of the present invention.

[0015] **FIG. 5** illustrates a flow diagram for uploading one or more files onto multiple containers provided by one or more cloud storage providers in accordance with an embodiment of the present invention.

[0016] **FIG. 6** illustrates a flow diagram for executing search queries on encrypted files stored as one or more containers provided by cloud storage providers in accordance with an embodiment of the present invention.

[0017] **FIG. 7** illustrates a flow diagram for downloading files from cloud-based storage containers in accordance with an embodiment of the present invention.

[0018] **FIG. 8** illustrates a sequence diagram for uploading files to cloud-based storage containers in accordance with an embodiment of the present invention.

[0019] **FIG. 9** illustrates a sequence diagram for searching searchable encrypted files that are stored in cloud-based storage containers in accordance with an embodiment of the present invention.

[0020] **FIG. 10** illustrates a sequence diagram for downloading files from cloud-based storage containers onto local drives/discs in accordance with an embodiment of the present invention.

[0021] **FIG. 11** is an example of a computer system with which embodiments of the present invention may be utilized.

DETAILED DESCRIPTION

[0022] Systems and methods for a policy-based framework for secure cloud storage distribution and aggregation are described. Methods and systems are also provided for implementing a policy based framework for encrypting, storing, accessing, querying and managing data across one or more cloud platforms. According to one embodiment, a searchable encryption gateway framework provides assignment of a policy from a group of policies stored in a policy database to one or more users such that the policy not only defines the manner in which the users can access and process content stored on the cloud, but can also configure the mode in which the data is encrypted, stored, searched, and accessed to ensure secure and vendor independent cloud management. Embodiments of the system of the present invention can include a policy assignment module, an encryption module, a storage module, and a management module, each of which can be implemented across one or more network devices such as gateway devices, proxy devices, network controllers, among other like devices.

[0023] According to one embodiment, the policy assignment module is configured to assign a policy to one or more users, where the policy is selected from a group of policies that are stored in a database. The selected policy can be used for defining the manner in which a file or metadata related thereto is to be uploaded, stored, searched, downloaded, and/or processed in the context of one or more cloud platforms. The selected policy can further be used to configure access rights of the one or more users such that the access rights dictate the manner in which the users can process the uploaded encrypted files. In an instance, a policy can allow a user to download a searchable encrypted file stored in the cloud to a local device such as a mobile phone and search the downloaded encrypted file on the local device for further processing. The policy can further implement key management policies across cloud providers and local devices such that no vendor lock-in is required and a user is given flexibility to transfer content across cloud providers and perform other desired functions that otherwise require vendor specific Application Programming Interface (API). According to one embodiment, a selected policy can be applied to a group of users across one or more organizations such that the policy not only controls the manner in which the content is uploaded, stored, and accessed in the cloud but also manages the rights of a user and the manner in which the user can retrieve and process the files.

[0024] According to one embodiment, an encryption module is configured to encrypt one or more files to be uploaded/stored across one or more cloud platforms based on a policy defined by the policy assignment module. In an implementation, a selected policy can be used to define encryption keys, decryption keys, and encryption type, among other attributes for carrying out the encryption of data. According to another embodiment, the encryption module can encrypt each file and/or content thereof using cryptographic key information such that the encrypted content is searchable across cloud platforms, making the encryption architecture independent of the vendor/service provider of the cloud platforms. According to one embodiment, based on the policy defined by the policy assignment module, encrypted files can also be downloaded by one or a group of authenticated users onto a local device such that the downloaded encrypted files are available to offline applications, and hence can be searched, controlled, and managed using the keys generated by the encryption module based on the policy.

[0025] According to an embodiment, a storage module is configured to store the searchable encrypted file within the one or more cloud platforms based on policy selected by the policy assignment module. In an implementation, the selected policy can be used to define the manner in which and/or the location at which the file is to be stored (e.g., whether the file is to be stored within a single container or spread across multiple containers and/or whether a copy of the file is to be stored on a local device for offline usage). As the storage module can be implemented independent of the cloud service providers without using application programming interfaces (APIs) exposed by the vendors, the encrypted files can be moved to any cloud platform, thereby avoiding vendor lock-in.

[0026] According to another embodiment, a management module is configured to control and manage encryption, storage, access, and processing of cloud storage based on the policy defined by the policy assignment module. In an embodiment, based on user attributes such as the role of the user, a project assigned to the user, the user's need to access the data at issue, among other such attributes, and further based on organization level changes and requirements, a policy identified by the policy assignment module can be dynamically changed or modified at run-time in order to comply with the organization requirements and configure the cloud storage for compliance.

[0027] According to another embodiment, the system may further include a mediation module that is operatively coupled with other modules and is configured to mediate vendor specific protocol/APIs thereby facilitating geographical and provider diversity in data placement, making the system agnostic with respect to specific cloud vendor APIs and increasing availability and durability of the stored data. In another embodiment, system of the present disclosure can further include a generalized API module that is operatively coupled with the mediation module and configured to provide a generalized API that can be called by any content/data intensive user application to access content from containers of cloud storage. Generalized API module can allow a single standard thread to multiple users to connect any of their applications with the proposed system and to perform any of storage, upload, retrieval, download, modify, search, and other allied functions at multiple cloud stores of different cloud service providers.

[0028] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present disclosure. It will be apparent, however, to one skilled in the art that embodiments of the present disclosure may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0029] Embodiments of the present disclosure include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps.

[0030] Alternatively, the steps may be performed by a combination of hardware, software, firmware and/or by human operators.

[0031] Embodiments of the present invention may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, but is not limited to, fixed (hard) drives, magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs),

electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware). Moreover, embodiments of the present disclosure may also be downloaded as one or more computer program products, wherein the program may be transferred from a remote computer to a requesting computer by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection).

[0032] In various embodiments, the article(s) of manufacture (e.g., the computer program products) containing the computer programming code may be used by executing the code directly from the machine-readable storage medium or by copying the code from the machine-readable storage medium into another machine-readable storage medium (e.g., a hard disk, RAM, etc.) or by transmitting the code on a network for remote execution. Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the present disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0033] Notably, while embodiments of the present invention may be described using modular programming terminology, the code implementing various embodiments of the present invention are not so limited. For example, the code may reflect other programming paradigms and/or styles, including, but not limited to object-oriented programming (OOP), agent oriented programming, aspect-oriented programming, attribute-oriented programming (@OP), automatic programming, dataflow programming, declarative programming, functional programming, event-driven programming, feature oriented programming, imperative programming, semantic-oriented programming, functional programming, genetic programming, logic programming, pattern matching programming and the like.

Terminology

[0034] Brief definitions of terms, abbreviations, and phrases used throughout this application are given below.

[0035] The phrases “cloud storage service” and “cloud storage platform” generally refer to computer storage space and/or related management provided by a cloud storage service provider.

[0036] The phrases “cloud storage service provider” and “cloud service provider” generally refer to a company that provides computer storage space and/or related management to other companies. Examples of cloud service providers include, but are not limited to, Dropbox, Google Drive and Amazon Web Services.

[0037] The terms “connected” or “coupled” and related terms are used in an operational sense and are not necessarily limited to a direct physical connection or coupling. Thus, for example, two devices may be couple directly, or via one or more intermediary media or devices. As another example, devices may be coupled in such a way that information can be passed therebetween, while not sharing any physical connection on with another. Based on the disclosure provided herein, one of ordinary skill in the art will appreciate a variety of ways in which connection or coupling exists in accordance with the aforementioned definition.

[0038] The phrases “in one embodiment,” “according to one embodiment,” and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one embodiment of the present invention, and may be included in more than one embodiment of the present invention. Importantly, such phases do not necessarily refer to the same embodiment.

[0039] If the specification states a component or feature “may”, “can”, “could”, or “might” be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[0040] The term “responsive” includes completely or partially responsive.

[0041] The phrase “storage container” generally refers to a file system and/or a user interface concept/metaphor that is used to store, organize or catalogue electronic data and/or electronic files. Some storage containers, such as directories and folders, may include references

to other storage containers, such as other directories, folders and/or files. Examples of storage containers include, but are not limited to, directories, directory structures, web directories, folders, smart folders, files and namespaces of same.

[0042] Folder - to In computing, a directory is a file system cataloging structure in which references to other computer files, and possibly other directories, are kept.

[0043] **FIG. 1** illustrates an exemplary network architecture 100 in accordance with an embodiment of the present invention. System architecture 100 illustrates a plurality of clients 102a, 102b..102n, collectively referred to clients 102 hereinafter, operatively and communicatively coupled to each other through a local area network (LAN) 104. Clients 102, as part of their function, may utilize data, which includes files, directories, metadata (e.g., access control list (ACL) creation/edit dates associated with the data, etc.), and other data objects. Clients 102 may also upload files, search for files or content therein, or even download files as and when desired, wherein during a copy, backup, archive or other storage operation, clients 102 may send a copy of some data objects to a secondary storage computing device by utilizing one or more data agents. A data agent may be a software module or part of a software module that is generally responsible for storage operations, such as copying, uploading, archiving, migrating, download, and recovering data from a data store or other memory location. Each client 102 may have at least one data agent, and system architecture 100 can support multiple clients 102.

[0044] According to one embodiment, clients 102 through LAN 104 can be operatively coupled with one or more cloud stores 114a, 114b...114n, collectively referred to as cloud stores 114 hereinafter, through a cloud gateway 108 using Internet 112. Cloud gateway device 108 typically acts as an interface between the clients 102 and stores 114, wherein different file/data read/write requests received from clients 102 can be handled by the gateway device 108 to identify the appropriate set of stores 114 that need to be accessed for processing the requests. Could gateway device 108 can be selected from one or a combination of access management devices, proxy devices, gateway devices, and network controllers, which basically have the intelligence to act as an interface between the clients and cloud service providers. In an embodiment, gateway 108 can be configured with a network attached storage (NAS), wherein NAS provides a way to satisfy incoming data writes from clients 102 quickly, and to buffer or

spool data before it is transferred to cloud stores 114. Cloud gateway 108 may further be configured to de-duplicate locally stored data before being written up to cloud stores 114. Clients 102 and applications used thereby can also specify parameters (e.g., under a storage policy) that dictate to the cloud gateway 108 the manner in which their content is to be handled, e.g., how long it is to be retained, whether it be encrypted/compressed, should it be deduplicated, should it be indexed and searchable, should it to be replicated and if so, how many copies and to where, etc. Cloud gateway device 108 may facilitate and/or configure the cloud stores 114 by allowing for metadata to be specified on a per file/object basis or on a data container or bucket basis. Further, the system 100 permits data to be replicated on demand to selected geographies based on access usage patterns, etc. Cloud gateway 108 can also be configured with the intelligence of automatically determining the most optimal cloud store 114 for a given client 102 and then route all files/content from the client 102 to the identified store 114.

[0045] Clients 102 may store one or more files, directories, metadata, or parts thereof across one or more cloud stores 114. Clients may also store such content across two or more stores 114 such that the content is divided into multiple chunks and each chunk is stored on a different cloud store 114. According to one embodiment, system 100 of the present invention proposes a vendor independent cloud management architecture such that file chunks are stored across cloud stores 114 that are managed by different cloud service providers. This allows geographical and provider diversity in data placement and avoids any vendor lock-in, leading to increased flexibility and availability.

[0046] According to one embodiment, as can be seen in **FIG. 1**, LAN 104 can be operatively coupled with cloud gateway 108 by means of a proxy 106 that can support multiple protocols such as Hypertext Transfer Protocol Secure (HTTPS), Simple Mail Transfer Protocol (SMTP), Simple Object Access Protocol (SOAP) and File Transfer Protocol (FTP). Proxy 106 can be configured to establish and terminate sessions between clients 102 and cloud stores 114. In an embodiment, proxy 106 can also be configured within cloud gateway 108. In addition to the proxy 106, cloud gateway device 108 can also be operatively coupled with a policy database 110, wherein the policy database 110 can include multiple administrator-configurable policies such that each client 102 is assigned a policy, which is configured to define the rights of the client 102. Such rights not only control the manner in which the respective client 102 encrypts,

stores, accesses, and manages files and metadata related thereto, but also the mode in which multiple cloud providers in general interact with the client 102 across one or more cloud platforms. According to one embodiment, a policy can be implemented for a client 102 or a group of clients 102, also interchangeably referred to as users 102 hereinafter, based on their role and responsibility in the organization including other factors relating to the projects they work in, experience they carry, among other attributes. The selected policy can then be used for defining the manner in which the client 102 interacts with multiple cloud storage providers and the access rights he/she possesses to create, upload, store, search, download, and/or process in the context of one or more cloud platforms. In an instance, a policy stored in the policy database 110 can allow a client 102 to download a searchable encrypted file from a cloud store such as store 114a onto a local device, such as client's mobile phone, and then search the downloaded encrypted file on the local device for further processing. According to one embodiment, policies can be used to enforce endpoint protection by, for example, allowing/blocking decryption of downloaded data based on characteristics of the device. For example, an administrator may define a policy for a user that only allows download of decrypted data to company-approved devices or devices that provide a secure container in which to place the downloaded data.

[0047] **FIG. 2** illustrates exemplary functional modules of a policy-based framework 200 for secure cloud storage distribution and aggregation in accordance with an embodiment of the present invention. Framework 200 of **FIG. 2** also illustrates an environment showing interactions between enterprise users and cloud service providers for storage, retrieval, and searching of data and content stored by the providers in their respective cloud stores. According to one embodiment, enterprise 202 can include multiple users 202a, 202b, and 202c, collectively referred to as users 202 hereinafter, who, in an embodiment, may be structurally similar to the clients 102 of **FIG. 1**. Each user 202 of an enterprise may have a different role and responsibility and hence needs to be given different access rights and privileges to access data and content for evaluation and processing. In an instance, a project manager would need to have access to project related costs, billings, and manpower allocation details, which a project engineer may not need. Enterprise users 202 can be operatively coupled to one or more cloud service providers 206a, 206b, 206c, collectively referred to as cloud service providers 206 hereinafter. According to one embodiment, users 202a-c may be remote users (e.g., connecting to

the enterprise network over the Internet or over a private network using some type of remote access connection) or local users.

[0048] Cloud service providers 206 may offer free, personal and/or business accounts providing hundreds or more of gigabytes of online storage. Cloud service providers 206 typically provide many distributed storage resources acting as one, provide high fault tolerance via redundancy and/or distribution of data and provide high durability through the creation of versioned copies. Examples of cloud service providers include, but are not limited to, Dropbox, Google Drive and Amazon Web Services.

[0049] According to one embodiment, enterprise users 202 can be operatively coupled with the cloud service provider 206 through a gateway 204, which is configured to interface transactions and execute instructions for read/write/search of content between the users 202 and the containers provided by the cloud service providers 206. According to one embodiment, gateway 204 can incorporate multiple functional modules to facilitate transactions between the users 202 and the cloud service providers 206, including but not limited to, a policy assignment module 208, an encryption module 210, a storage module 212, a management module 214, a mediation module 216, and a generalized API module 218. Gateway 204 can further be operatively coupled with a policy database 218, wherein the policy database 218 comprises one or more policies that define the rights and privileges of the users 202 with respect to their interactions with multiple cloud service providers 206 and may further enforce endpoint protection, as described above.

[0050] According to one embodiment, policy assignment module 208 is configured to facilitate assignment of a policy selected from the policy database 218 to one or a group of users 202, where the policy to be assigned can be selected, by an administrator, for example, based on the role, responsibility, enterprise practices, among other attributes and can be configured to define the manner in which data, metadata, or any other content, can be accessed and processed by the user or the group of users 202. In one embodiment, a policy not only defines the manner in which files can be uploaded, stored, downloaded, searched, and/or processed in the context of one or more cloud platforms, but also includes any other configurable aspect of the mode in which the user 202 accesses data stored or to be stored in the namespaces, directories, folders, files or other storage containers of one or more cloud platforms. The selected policy can further

be used to configure access rights of the one or more users such that the rights dictate the manner in which the users process the files, whether encrypted or unencrypted, for instance.

[0051] According to one embodiment, cloud based storage containers can be configured to store the content and/or metadata of encrypted files, wherein gateway 204 can be configured for key management to allow encryption and decryption of content stored on the containers. Policy assigned to a user 202 can also be configured to manage access rights relating to encryption and decryption of content, such that, for instance, one user is allowed to download a searchable encrypted file stored in the cloud onto a local device and search the downloaded encrypted file on the local device for further processing, and another user is not. User-assigned policy can further include key management sub-policies across cloud providers and local devices such that no vendor lock-in is required and a user is given the flexibility to transfer content across varied cloud providers and perform other desired functions that otherwise require vendor specific Application Programming Interfaces (APIs). According to one embodiment, a selected policy can be applied to a group of users across one or more organizations such that the policy not only controls the manner in which the content is uploaded, stored, and accessed in the cloud but also manages the rights of the group of users and the manner in which the users can retrieve and process the files.

[0052] According to one embodiment, encryption module 210 is configured to encrypt one or more files to be uploaded/stored across one or more cloud platforms based on the policies assigned by the policy assignment module 208. As the gateway device 204 acts as an interface between the enterprise users 202 and the cloud service providers 206, the gateway 204 can be configured to define and manage encryption keys, decryption keys, and encryption type, among other attributes for carrying out the encryption of content. In an implementation, the gateway 204 can share encryption/decryption keys based on the policy assigned to the user, wherein, for instance, in case a policy does not authorize a user to encrypt files for storage on cloud-based containers, gateway 204 would not share any key details (private/secret and/or public keys) with the user 202.

[0053] According to one embodiment, the encryption module 210 can encrypt each file and/or part thereof using cryptographic key information such that the encrypted content is searchable across and within cloud platforms, making the encryption architecture independent of

the vendor/service provider of the cloud platforms. Encryption module 210 can further allow a user 202, based on his/her assigned policy, to download searchable encrypted files onto a local device such that the downloaded encrypted files are then available to offline applications and can be searched/managed using the keys generated and processed locally and/or by the gateway 204. As can be seen in **FIG. 2**, one or more containers (e.g., directories, folders, files and their associated namespaces) of cloud service providers 206 can store metadata and/or content associated with searchable encrypted files, which can be accessed by one or more users, based on the assigned policies. Access to such searchable encrypted files can allow the users to search through the content of the files within the context of the cloud service providers 206 or can also allow the users to download the encrypted files onto their local devices such as laptops, PCs, mobile device, smart phones, tablet PCs, portable computing devices, among other like devices, as has been done by user 202b of **FIG. 2**, wherein the user 202b has downloaded the searchable encrypted files on respective local device, which would then allow the user 202b to search metadata and/or content associated with the searchable encrypted files even in offline mode when cloud service providers 206 are inaccessible via a network connection, for example.

[0054] For purposes of brevity, examples of searchable encrypted files are described in which the encrypted version of the name of the original file requested to be stored in the cloud is used as all or a portion of the name of a folder containing one or more files having stored therein the encrypted textual content of the original file. Hashes of one or more search terms may be used to form the file names to provide searchable indices. In other embodiments, the files may be zero-sized files and the file names themselves may represent all or a portion of the cipher text (e.g., encrypted content of the original file).

[0055] In yet another embodiment, full text and/or regular expression search capabilities may be provided. For example, full text search-aware encryption may be supported in a cloud storage service provider-agnostic manner by automatically processing, by the cloud gateway (e.g., cloud gateway 108 or 204), data associated with a file requested to be stored in the cloud and creating desired meta-data to enable search before distributing the data among one or more cloud service providers. The cloud gateway may store an additional small amount of meta-data for multi-user access control and sharing purposes and send the encrypted data and meta-data to the cloud for permanent storage. In this manner, end-users may later search for any keyword,

term, or expression in the uploaded files effectively with no information leakage to the cloud providers. Further improvements to the remote processing ability can be provided by handling complex regular expressions and/or Boolean logic-based formulas. For example, in the case of Health Insurance Portability and Accountability Act (HIPAA) data storage applications, a hospital doctor may be interested in patient data records where a patient's age is between 10 and 30 and their records contain the term "diabetes." Additionally, it is desirable to allow users to perform searches using the full power of regular expressions, allowing fuzzy matching, and searching records in multiple formats automatically.

[0056] Empirical data suggests with about five percent overhead the cloud gateway can create an ordered index that is fully searchable to support both regular expression and full text search capabilities. In connection with testing of a prototype system implementing an embodiment of the present invention, "Programming Python," by Mark Lutz was analyzed and found to contain a total of 542,259 words of which 51,842 were unique words (including numbers and symbols). This rough count includes many duplicates, so it can be viewed as an upper bound. Regardless, indexing of such a document is easy. A full accounting (in clear text) of all words and their counts is 994KB for a 27MB PDF.

[0057] Most words deduplicate well. Therefore, in one embodiment, a finer representation of a text file may be created based on a deduplicated document for regular expression and n-gram based searches. For example, if each word were represented by a hash of n-bits, and assuming ~50k unique words in a book, it is estimated that no more than 5,000,000 hashes would be needed to prevent collision over an average document or set of documents, so 3-bytes per word is more than sufficient.

[0058] In one embodiment, to run a regular expression on a document, both the encrypted document and the ordered index are downloaded from the cloud. Then, the cloud gateway determines if any combination of words satisfies the regular expression. Finally, the search run on the deduplicated hash document, by hashing the words. This is the same basis for full text search capability. A simplified example of how searchable encrypted files may be created and processed by a searchable encryption engine for executing search queries is described further below with reference to **FIGs. 3A-B**.

[0059] FIG. 3A illustrates a flow diagram for generating searchable encrypted files in accordance with an embodiment of the present invention. According to one embodiment, the security engine used by the searchable encryption framework is based on encryption of file names and file obscurity in the cloud as described in Appendix A, whereby each file in the user space is chunked and each chunk corresponds to an individual file in the encrypted cloud space. Encrypted files may be spread evenly or otherwise over arbitrary file name sets, to further obfuscate the search space, with the option for file padding, or the random creation of empty files in the sequence to further prevent data leakage. Chunks from a single file can be distributed across separate cloud storage service providers. The methods described herein further allow the data to be searchable despite being encrypted, thereby not breaking existing application functionality. In one embodiment, the searchable encryption framework also offers a generalized API to upload files, and search for files by name and no additional provider-specific functionality is needed to provide searchable encryption, deduplication, and tokenization.

[0060] At step 302, a file to be encrypted can be received by gateway device 204 from an enterprise user 202. Such a file can be received based on policy assigned to the user and rights defined in the policy. At step 304, the file can be partitioned into one or more chunks, wherein chunk size can be pre-defined or dynamically determined by the encryption module 210 or any other module of the gateway 204. Chunk sizes can also be different for each user/file/enterprise such that a file can be partitioned into multiple chunks of varied sizes based on one or a combination of file contents, characteristics of the file content, policy assigned to the user, attributes of cloud stores in which chunks are intended to be stored, among other parameters. For instance, a chunk can be as small as a record in the file and as large as the whole file itself.

[0061] At step 306, each chunk can be encrypted based on public and private/secret keys defined by the encryption module 210. In an exemplary implementation, each chunk R can be encrypted based on a public key P using a function Encrypt (P, R) to generate cipher text, C, by the following equation:

$$C \leftarrow \text{Encrypt}(P, R), \text{ if predicate} = 1$$

$$C \leftarrow \text{Encrypt}(P, 0), \text{ Otherwise}$$

According to one embodiment, the cipher text, C, can be decrypted using an appropriate secret/private key, S, defined by the encryption module 210.

[0062] At step 308, indices, also referred to as keywords hereinafter, which would typically be used as search terms in the form of search queries are stored as filenames of the chunks. For instance, in a medical record that states, “Peter is an Asian having Diabetes”, possible search keywords can be “Peter”, “Asian”, and “Diabetes” and therefore indexing can be done on these three keywords such that they are stored in an searchable yet ciphered format. For instance, searchable index for “Peter” can be generated by the encryption module 210 as “uetywo”. Likewise, “Diabetes” can be indexed as “hdweuf”, which is again searchable after the keywords are generated as searchable indices by the encryption module 210.

[0063] At step 310, further obfuscation can be processed on the encrypted file chunks by options such as file padding or random creation of empty files, which can further prevent data leakage. Any other known technique for enhancing encryption of file chunks can also be implemented and is well covered within the scope of the present disclosure. At step 312, the encrypted chunks are finally stored across one or more cloud-based containers. In an implementation, gateway 204 can be configured to store file chunks such that contiguous chunks are not stored together, and instead, are stored on containers provided by different cloud service providers.

[0064] **FIG. 3B** illustrates an flow diagram for processing search queries for searching encrypted files in accordance with an embodiment of the present invention. At step 350, the gateway device 204 receives a search query, wherein the search query can define elements and keywords to be searched based on defined constraints. For instance, a search query can be defined as “Select Details based on Name, wherein the Name is “Ronn” OR “Eric”. At step 352, keywords being searched are evaluated and extracted. For instance, for the above mentioned search query, the keywords may include “Ronn” OR “Eric”. Other attributes of the search query, including but not limited to the constraints defined in the query can also be evaluated. At step 354, each extracted keyword can be converted into searchable indices by the encryption module 210. Searchable indices, as mentioned with reference to **FIG. 3A** can be stored within file names of multiple file chunks. For instance, search keyword “Ronn” can be indexed as “uevbwq” and Eric can be indexed as “uastyb”.

[0065] At step 356, the modified search query can be executed based on the searchable indexed formed from the search keywords. In an instance, instead of “Ronn” OR “Eric”, the modified search query can be “uevbwq” OR “uastyb”, which once formed can then be run on one or more containers of the cloud service providers 406, which store the file chunks. At step 358, chunks having matching indices can be returned as the result set. As multiple file chunks can have the same searchable index, multiple chunks can be returned as results from different containers.

[0066] **FIGs. 4A-C** conceptually illustrate the generation of searchable indices from search queries in order to execute search queries in encrypted files in accordance with an embodiment of the present invention. **FIG. 4A** shows multiple containers (1-4), which may stored within a single cloud service provider or across multiple cloud service providers. Each container can include multiple encrypted file chunks, which may be named by means of searchable indices as mentioned in connection with the description of **FIGs. 3A-B**. For instance, container 1 can include four file chunks having their names (adfbhlbewfuwed, ewuiyrt, hdweuf, and uetywo). In the present example, the top-most portion of each container may represent a folder within which the other portions are included in the form of files. The name of the folder may be the encrypted version of the original file name and the names of the files may include one or more searchable indices.

[0067] Size of each file chunk and/or each container can be varied and stored such that optimal processing can be done on the file chunks with minimum latency. In an instance, while allocating file chunks to containers, each chunk can be assigned a weight based on the content it represents, importance of the chunk, among other parameters, and then be allocated, based on its weight, to the least weighted container, which may allow minimal latency in access of the chunk.

[0068] The second portion of **FIG. 4** shows the same set of four containers, each having four file chunks that may be named using searchable indices. The figure further represents a search query, “Ronn” or “Eric”, wherein Ronn and Eric form part of the keywords to be looked out for from the one or more containers. As is illustrated in the third and final portion of **FIG. 4**, keywords “Ronn” and “Eric” are converted, by the encryption module 210, into searchable indices (uetywo) OR (pigeou), which are then executed as part of the search query on the one or more containers. As can also be seen in **FIG. 4**, two file chunks, one in container 1 and the other

in container 4, match the search indices and can therefore be returned as part of the result set. In an implementation, the searchable indices can be defined in the gateway device 204 and then sent to one or more relevant set of containers in the form of a query. Alternatively, in cases of downloaded encrypted files on local devices, search keywords can also be indexed within the local device itself by using key management implemented by the policy assigned to the user, and the indexed terms can then be searched on the local database itself.

[0069] Referring back to **FIG. 2**, according to one embodiment, storage module 212 is configured to store the files and/or other content, including but not limited to searchable encrypted files, within the one or more cloud platforms and/or containers of the cloud service providers 206 by one or more users 202 based on their respective policies. In an implementation, a policy can be used to define the manner in which and/or the location at which a file is to be stored (e.g., whether the file is to be stored within a single container, or divided into chunks and stored across multiple containers and/or whether a copy of the file is to be stored on a local device for offline usage). Gateway 204, through the storage module 212, can also dynamically change the configuration of file storage so as to store the content optimally at any given instant. As the gateway 204 can automatically change the storage pattern across one or more containers of cloud service providers 206, enterprise users 202 do not have to worry about changing their providers in order to find a more optimal solution, from a cost, bandwidth, latency, and other allied standpoints. As the storage module 212 can be implemented independent of the cloud service providers without using application programming interfaces (APIs) exposed by the vendors, files stored by such vendors can be moved to any cloud platform at any moment, thereby avoiding vendor lock-in.

[0070] According to another embodiment, management module 214 is configured to control and manage encryption, storage, access, and processing of cloud storage based on the policy defined by the policy assignment module 208. As management module 214 is configured to manage all functions relating to storage, transfer, access, processing, and search, among other functions, the module 214 may be operatively coupled with all other functional modules of the system 200. As roles, responsibilities, and other user attributes keep changing periodically, the management module 214 can be configured to factor all such parameters including service quality of cloud service providers 206, storage capacity anticipated, and change in policies,

among others and modify the cloud-based content storage and access patterns at run-time in order to comply with the organization requirements and desired performance levels.

[0071] According to another embodiment, mediation module 216 is operatively coupled with other functional modules and is configured to mediate vendor specific protocols/APIs with gateway 204 so as to allow the gateway 204 to facilitate a vendor lock-in free environment for users 202, thereby facilitating geographical and provider diversity in content placement, making the system agnostic with respect to specific cloud vendor APIs and increasing availability and durability of the stored data. Mediation module 216 can be configured to dynamically detect changes in vendor specific protocols/APIs and change configurations in the gateway 204 so as to allow the gateway 204 to optimally process user transactions for data storage, transfer, and retrieval at any time.

[0072] According to another embodiment, gateway 204 can include a generalized API module 218 that is operatively coupled with the mediation module 216 and configured to provide a generalized API that can be called by any content/data intensive user application. For instance, user applications relating to database, project management, finance, and strategy development are typically content centric and can accordingly be operatively coupled with the gateway 204 by means of the generalized API module 218 so as to enable the gateway 204 to, based on the mediation module 216, enable the content from such applications to be efficiently stored across cloud-based containers. In sum, the generalized API module 218 allows a single standard thread to multiple users to connect any of their applications with the gateway 204 to perform any of storage, upload, retrieval, download, modify, search, and other allied functions at the cloud stores.

[0073] **FIG. 5** illustrates a flow diagram 500 for uploading one or more files to a plurality of containers provided by cloud storage providers in accordance with an embodiment of the present invention. At step 510, a file to be uploaded by a user can be received at a gateway device. At step 520, the gateway device can check whether a policy exists for the concerned user, which if present, is assigned to the user. In case no policy exists for the user, an appropriate policy can be identified for the respective user and accordingly assigned, based on which the file uploading process is carried out. At step 530, the received file can be divided into multiple chunks of same or varying sizes, wherein in an implementation, the complete file is

taken as a single chunk and uploaded onto a container provided by a cloud-based providers, and in another implementation, the file is broken into numerous chunks, which are then stored across one or more containers.

[0074] At step 540, each file chunk is encrypted based on the policy assigned to the user. It would be appreciated that it is not necessary to encrypt a file before storing it on the cloud storage, but the same may be preferred. It also to be appreciated that storing of files and/or metadata related thereto based on the user assigned policy, without encryption, is also covered within the scope of the present invention. Furthermore, in an implementation, files can be encrypted such that they are searchable by a user having the appropriate rights to do so. In yet another embodiment, only a partial set of file chunks can be encrypted, while the other set may not be encrypted. At step 550, encrypted file chunks can be stored on a single or a combination of containers of multiple cloud service providers. As mediation takes place between the APIs of multiple cloud service providers and cloud gateway of the present disclosure, any file chunk can be uploaded to any container that is accessible by the gateway. A gateway can also categorize or assign weights to cloud service providers based on their priority, response time, feedback, performance, and other evaluation parameters and accordingly upload chunks by choosing the most optimal set of containers. For instance, file chunks having higher weights/priority can be allocated to more secured containers. It should be appreciated that any other change in parameters based on which allocation of files to containers takes place is within the scope of the present disclosure.

[0075] **FIG. 6** illustrates a flow diagram 600 for executing search queries on encrypted files stored on one or more containers provided by cloud storage providers in accordance with an embodiment of the present invention. At step 610, a search query is received from a user, wherein the search query defines one or more elements along with constraints, which need to be matched with data stored on cloud-based containers. At step 620, policy associated with the user is evaluated to assess whether the user has the rights to execute a search on the containers. As such access rights may be partial, a user, based on the assigned policy, may be allowed to search in a partial set of containers. In case a user is not assigned a policy, gateway may be configured to check the profile of the user and accordingly assign an appropriate policy to define access rights and privileges of the user while interacting with multiple cloud-based platforms. At step

630, the received search query can be divided into multiple query elements and subsequently converted into searchable indices. An exemplary conversion of search keywords/elements to searchable indices has been explained previously with reference to **FIG. 3B**.

[0076] At step 640, the searchable indices can be executed by the gateway device so as to retrieve matching file chunks stored in containers of cloud storage. At step 650, the matching file chunks can be retrieved and presented to the user. It should be appreciated that the above flow diagram is completely exemplary in nature and any change in configuration and structure of the file being searched, or policy based on which the search is conducted is within the scope of the present disclosure. For instance, in case the user assigned policy does not allow retrieval of the complete file chunk but only a part therefore, the step 650 may be configured accordingly to extract only the authorized file chunk portion for subsequent presentation.

[0077] **FIG. 7** illustrates a flow diagram 700 for downloading files from cloud-based storage containers in accordance with an embodiment of the present invention. At step 710, a request for file(s) to be downloaded is received by gateway device from a user. At step 720, policy details of the user that has requested for file download are retrieved to evaluate whether user has the required authorization and rights to make such a request and download the requested set of files. In case, for instance, from the requested set of files, only a partial set has been authorized to the user, the gateway device accordingly processes the request and negates the remaining set of files. At step 730, it is checked for whether the user policy allows downloading of requested set of files, wherein in case the policy does not allow, the method ends. At step 740, in case the user policy allows downloading of files, the gateway processes the request by checking the location at which each file is stored and accordingly retrieves the files from the identified locations. In case one or more of the requested files are stored as chunks, the gateway can be configured to extract each file chunk of the relevant file from one or more containers and combine them to form the desired file. At step 750, the files and/or chunks thereof can be saved onto the local drive.

[0078] According to one embodiment, files requested for downloading may include one or more searchable encrypted files, in which case, the gateway, upon receiving such a request, identifies location of the encrypted files and downloads the searchable encrypted files onto the

local drive, in order to enable the user to search the encrypted file offline without being connected to cloud based containers or even the gateway device, for instance.

[0079] **FIG. 8** illustrates a sequence diagram 800 for uploading files to cloud-based storage containers in accordance with an embodiment of the present invention. As can be seen, multiple structural elements including client application/browser, proxy, policy database, searchable encryption engine, cloud provider API mediation, and a plurality of containers are present in the architecture of the proposed system. As the function of each structural element has been explained in detail above, the same is not being repeated for brevity of the disclosure. It would also be appreciated that multiple structural features may form part of a single network device. For instance, gateway device of the present disclosure can include the searchable encryption engine and the cloud provider API mediation within itself. Furthermore, although policy database can also be incorporated within the gateway device, the database can also be an external database and operatively coupled with the gateway device. As can be seen in the sequence diagram, upload sequence flow can be initiated by a user, through his/her client application, by sending a file upload request to a gateway, which is operatively coupled with the policy database of the proposed architecture. The gateway device can be accessible to the client by use of a proxy, such as a HTTP proxy, which sets up and terminates sessions between client applications and gateway interface.

[0080] As a next step, upon receiving the request, the gateway device, through the policy database checks for whether a policy exists for the user and assigns the appropriate policy to the user based on parameters including but not limited to, role and responsibility of user in the enterprise and years of experience. The user can then, through the HTTPS proxy, submit the assigned policy to the gateway and, using the searchable encryption engine of the gateway, partition the file to be uploaded into chunks. It would be appreciated that partitioning the file into multiple parts/chunks is not compulsory and is shown only as an exemplary embodiment of the present system. A file can therefore always be directly uploaded onto a container provided by a cloud service provider without being partitioned into chunks.

[0081] As illustrated in **FIG. 8**, searchable encryption engine can be configured to divide the file to be uploaded into multiple chunks, and then encrypt each chunk such that the chunk is searchable. Once the client, through the HTTP proxy, receives the encrypted file chunks, the

same can be sent the cloud provider API mediation, which mediates with the vendor specific APIs of one or more cloud service providers to allow the user access a vendor lock-in free environment to upload and process files. Once the mediation process with the desired set of cloud providers is complete, the gateway can be configured to upload each file, whether in chunks or not and whether encrypted or not, onto one or more containers. Confirmation of the successful upload of the files on the containers can then be given back to the user along with details of the containers on which the files are stored.

[0082] **FIG. 9** illustrates a sequence diagram 900 for searching in searchable encrypted files that are stored in cloud-based storage containers in accordance with an embodiment of the present invention. As can be seen, a user initiates the sequence flow by indicating, through a HTTP proxy, a file or content therein to be searched for. In response to the above search request, the gateway device determines whether the user has a policy associated thereto and whether the assigned policy allows the user to search for the intended content. In case the user-assigned policy allows a user to execute search for the desired content, the searchable encryption engine enables the user to create a search query, and then process the created query that comprises multiple keywords and constraints so as to generate a set of searchable indices (an example of which has been described with reference to **FIG. 3B**). The gateway device can then, upon generation of the searchable indices, run the query based on such indices on one or more containers and extract files or chunks thereof that match the queries. In an embodiment, as the gateway device may be aware of the containers on which the content/files would be stored, it need not execute the index-based search queries on all the containers but rather only on a set of containers that are known to contain relevant content. Results obtained from one or more containers after executing the index-based queries can then be processed using Boolean operations to result in a final set of results that can then be reported back to the user.

[0083] **FIG. 10** illustrates a sequence diagram 1000 for downloading files from cloud-based storage containers onto local drives/discs in accordance with an embodiment of the present invention. As can be seen, a user initiates the sequence flow by indicating a file or a part thereof to be downloaded onto the local drive. After receiving a file download request, the gateway device can be configured to evaluate whether the policy assigned to the enterprise user allows or gives him/her the right to download the requested file. Once the policy is evaluated and it is confirmed

that the user is authorized to download the file, the download request can be forwarded by the gateway device to the mediation module so as to allow the module to assess the container(s) on which the file resides, map the APIs of the cloud service providers of the respective container(s), and then send the request for downloading to the container(s). In case the file requested for downloading has been divided into multiple file chunks, with each chunk being stored on a different container, multiple file chunk download requests can be sent by the gateway device to the respective set of containers. Results from the containers can then be evaluated to confirm that they relate to the intended file, and then subsequently returned back to the client.

[0084] According to one embodiment, systems and methods of the present disclosure provide a cloud storage gateway device that is logically interposed and operatively coupled with one or more third-party cloud storage platforms on one side and a plurality of users of an enterprise on the other side. Systems and methods further provide a generalized application programming interface (API), by means of a generalized API module 218, through which the plurality of users can store files to the one or more third-party cloud storage platforms, issue search requests against the files, and retrieve content of the files.

[0085] According to another embodiment, the gateway device can be configured to assign a file storage policy from a plurality of file storage policies that are stored in a policy database to each user of the plurality of users, wherein the plurality of file storage policies define the access rights, storage diversity requirements, and type of encryption to be applied onto the files. In an exemplary implementation of the present system and method, the gateway device can be configured to receive, through the generalized API, a request to store/upload a file from a user and create searchable encrypted data corresponding to one or more of (i) content of the file and (ii) metadata associated with the file, wherein the upload request is associated with a first user of the plurality of users and the searchable encrypted data is, based on the type of encryption defined by the file storage policy, assigned to the first user. Gateway device can further be configured to distribute the searchable encrypted data among the one or more third-party cloud storage platforms based on the storage diversity requirements defined by the assigned file storage policy by uploading a subset of the searchable encrypted data to the one or more third-party cloud storage platforms.

[0086] According to another embodiment of the present disclosure, gateway device can also be configured to receive, through the generalized API, a request to search content of a file or metadata associated with the file. In order to implement the same, gateway device can be configured to check whether the search request is authorized based on the access rights defined by the file storage policy assigned to a user of the plurality of users with which the search request is associated, wherein, in case the search request is authorized, the gateway device executes the request on one or more third-party cloud storage platforms in order to apply the search (through searchable indices) onto the searchable encrypted data and return results of the search request to a source of the search request.

[0087] According to another embodiment of the present disclosure, gateway device, through the generalized API, can be configured to receive a request to access/download a file. For implementing the same, the gateway device, also interchangeably referred to as cloud storage gateway device in the present disclosure, first determines whether the access request is authorized based on the access rights defined by the file storage policy (or simply referred to as policy above) assigned to a user of the plurality of users with which the access request is associated. Once it is determines that the access request is authorized, the gateway device can be configured to gather content of the file by downloading a subset of the distributed searchable encrypted data from each of the one or more third-party cloud storage platforms and decrypt the searchable encrypted data. Decrypted data can then be returned to the user that requested for the file.

[0088] **FIG. 11** is an example of a computer system with which embodiments of the present invention may be utilized. Embodiments of the present invention include various steps, which have been described above. A variety of these steps may be performed by hardware components or may be tangibly embodied on a computer-readable storage medium in the form of machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with instructions to perform these steps. Alternatively, the steps may be performed by a combination of hardware, software, and/or firmware. As such, **FIG. 11** is an example of a computer system 1100, such as a cloud gateway, a client or server, upon which or with which embodiments of the present invention may be employed.

[0089] According to the present example, the computer system includes a bus 1130, one or more processors 1105, one or more communication ports 1110, a main memory 1115, a removable storage media 1140, a read only memory 1120 and a mass storage 1125.

[0090] Processor(s) 1105 can be any future or existing processor, including, but not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), or Motorola® lines of processors. Communication port(s) 1110 can be any of an RS-232 port for use with a modem based dialup connection, a 10/100 Ethernet port, a Gigabit port using copper or fiber or other existing or future ports. Communication port(s) 1110 may be chosen depending on a network, such as a Local Area Network (LAN), Wide Area Network (WAN), or any other network to which the computer system 1100 connects. For example, in the context of a PBX, communication port(s) 1110 may include communication cards supporting Ethernet or DS1/DS3 types of connections and in the context of a fax server, such as one of fax servers 341a-n, communication port(s) 1110 may include Ethernet, DS0, T1/DS1 (such as ISDN PRI) or fractional T1/DS1 or digital DS0 (such as ISDN BRI).

[0091] Main memory 1115 can be Random Access Memory (RAM), or any other dynamic storage device(s) commonly known in the art. Read only memory 1120 can be any static storage device(s) such as Programmable Read Only Memory (PROM) chips for storing static information such as start-up or BIOS instructions for processor 1105.

[0092] Mass storage 1125 may be any current or future mass storage solution, which can be used to store information and/or instructions. Exemplary mass storage solutions include, but are not limited to, Parallel Advanced Technology Attachment (PATA) or Serial Advanced Technology Attachment (SATA) hard disk drives or solid-state drives (internal or external, e.g., having Universal Serial Bus (USB) and/or Firewire interfaces), such as those available from Seagate (e.g., the Seagate Barracuda 7200 family) or Hitachi (e.g., the Hitachi Deskstar 7K1000), one or more optical discs, Redundant Array of Independent Disks (RAID) storage, such as an array of disks (e.g., SATA arrays), available from various vendors including Dot Hill Systems Corp., LaCie, Nexsan Technologies, Inc. and Enhance Technology, Inc.

[0093] Bus 1130 communicatively couples processor(s) 1105 with the other memory, storage and communication blocks. Bus 1130 can include a bus, such as a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X), Small Computer System Interface (SCSI), USB or

the like, for connecting expansion cards, drives and other subsystems as well as other buses, such as front side bus (FSB), which connects the processor(s) 1105 to system memory.

[0094] Optionally, operator and administrative interfaces, such as a display, keyboard, and a cursor control device, may also be coupled to bus 1130 to support direct operator interaction with computer system 1100. Other operator and administrative interfaces can be provided through network connections connected through communication ports 1110.

[0095] Removable storage media 1140 can be any kind of external hard-drives, floppy drives, IOMEGA® Zip Drives, Compact Disc – Read Only Memory (CD-ROM), Compact Disc – Re-Writable (CD-RW), Digital Video Disk – Read Only Memory (DVD-ROM). In no way should the aforementioned exemplary computer system limit the scope of the invention.

[0096] While embodiments of the present invention have been illustrated and described, it will be clear that the present invention is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the present invention. Therefore, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims.

CLAIMS

What is claimed is:

1. A method comprising:

providing, by a cloud storage gateway device logically interposed between one or more third-party cloud storage platforms and a plurality of users of an enterprise, a generalized application programming interface (API) through which the plurality of users can store files to the one or more third-party cloud storage platforms, issue search requests against the files and retrieve content of the files;

assigning, by the cloud storage gateway device, a file storage policy of a plurality of file storage policies to each user of the plurality of users, the plurality of file storage policies defining access rights, storage diversity requirements and a type of encryption to be applied to the files; and

responsive to receiving, via the generalized API, a request to store a file:

creating, by the cloud storage gateway device, searchable encrypted data corresponding to one or more of (i) content of the file and (ii) metadata associated with the file, wherein the storage request is associated with a first user of the plurality of users and the searchable encrypted data is based on the type of encryption defined by the file storage policy assigned to the first user; and

distributing, by the cloud storage gateway device, the searchable encrypted data among the one or more third-party cloud storage platforms based on the storage diversity requirements defined by the assigned file storage policy by uploading a subset of the searchable encrypted data to each of the one or more third-party cloud storage platforms.

2. The method of claim 1, further comprising:

responsive to receiving, via the generalized API, a request to search content of the file or metadata associated with the file:

determining, by the cloud storage gateway device, whether the search request is authorized based on the access rights defined by the file storage policy

assigned to a user of the plurality of users with which the search request is associated; and

when the search request is authorized, causing, by the cloud storage gateway device, the one or more third-party cloud storage platforms to apply the search request to the searchable encrypted data and returning results of the search request to a source of the search request.

3. The method of claim 1, further comprising:

responsive to receiving, via the generalized API, a request to access the file:

determining, by the cloud storage gateway device, whether the access request is authorized based on the access rights defined by the file storage policy assigned to a user of the plurality of users with which the access request is associated; and

when the access request is authorized, gathering the content of the file, by the cloud storage gateway device, by downloading a subset of the distributed searchable encrypted data from each of the one or more third-party cloud storage platforms and decrypting the searchable encrypted data; and

returning the file to a source of the access request.

4. A method comprising:

assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms, wherein the policy defines access rights of the one or more users;

encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file;

storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and

managing access to the searchable encrypted file by the one or more users based on the policy.

5. The method of claim 4, wherein the step of managing comprises allowing the one or more users to download the searchable encrypted file to a local device.

6. The method of claim 5, wherein the local device comprises a mobile computing device.
7. The method of claim 5, wherein the downloaded encrypted file is searchable by the one or more users using the cryptographic key information.
8. The method of claim 4, wherein the step of encrypting further comprises:
 - dividing the file into a plurality of chunks;
 - creating namespaces for one or more of the plurality of chunks; and
 - configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.
9. The method of claim 8, wherein a set of chunks from the plurality of chunks is searchable.
10. The method of claim 8, wherein the step of configuring the namespaces comprises storing content of the file as filenames.
11. The method of claim 4, wherein the step of encrypting further comprises the step of randomly creating empty files.
12. The method of claim 4, wherein the step of encrypting the file is carried out independent of the service provider of the one or more cloud platforms.
13. The method of claim 4, wherein the policy is implemented for a group of users.
14. The method of claim 4, wherein the policy defines the manner in which the file is stored, accessed, and processed.
15. The method of claim 4, wherein the file is stored across two or more cloud platforms.
16. The method of claim 4, wherein said storing the searchable encrypted file on the one or more cloud platforms is carried out independent of the service provider of the one or more cloud platforms.
17. The method of claim 4, wherein the policy is selected from a plurality of policies stored in a database, wherein the database is operatively coupled with the gateway device.

18. The method of claim 4, wherein the policy defines one or more of a set of encryption keys, a set of decryption keys, search indices, a type of encryption and one or more authorized locations to which the file may be stored.
19. The method of claim 4, wherein said encrypting further comprises encrypting one or more of filename and search indices.
20. A secure cloud storage system comprising:
 - one or more processors;
 - a communication interface mechanism;
 - one or more internal data storage devices operatively coupled to the one or more processors and storing:
 - a policy assignment module configured to implement a policy selected from a group of policies for a user, wherein the policy defines and manages access to and processing of a file to be uploaded on a cloud, wherein the policy defines access rights of the user;
 - an encryption module configured to, using cryptographic key information defined by the policy, produce a searchable encrypted file by encrypting content of the file to be stored across one or more cloud platforms;
 - a storage module configured to store the searchable encrypted file on the one or more cloud platforms based on the policy; and
 - a management module configured to manage and control access to the searchable encrypted file by the user based on the policy.
21. The system of claim 20, wherein the management module is further configured to allow the user to download the searchable encrypted file to a local device.
22. The system of claim 21, wherein the downloaded encrypted file is searchable by the user using the cryptographic key information defined by the policy.
23. The system of claim 20, wherein the encryption module is further configured to:
 - divide the file into a plurality of chunks;
 - create namespaces for one or more of the plurality of chunks; and

configure the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.

24. The system of claim 23, wherein a set of chunks from the plurality of chunks is searchable.
25. The system of claim 23, wherein the encryption module is further configured to randomly create empty files.
26. The system of claim 20, wherein one or more of the policy assignment module, the encryption module, the storage module, and the management module are implemented on different devices, wherein the devices are selected from one or more of access management devices, proxy devices, gateway devices, and network controllers.
27. The system of claim 20, further comprising a mediation module configured to make implementation of one or more of the policy assignment module, the encryption module, the storage module, and the policy management module independent of the service provider of the one or more cloud platforms.
28. The system of claim 20, wherein the policy is implemented for a group of users.
29. The system of claim 20, wherein the policy defines the manner in which the file is stored and processed.
30. The system of claim 20, wherein the file is stored across two or more cloud storage platforms.
31. The system of claim 20, wherein the group of policies are stored in a database operatively coupled with the system.
32. The system of claim 20, wherein the policy defines and manages one or more of encryption keys, decryption keys, search indices, type of encryption, and location of the file.

ABSTRACT

[0097] Methods and systems for vendor independent and secure cloud storage distribution and aggregation are provided. According to one embodiment, an application programming interface (API) is provided by a cloud storage gateway device logically interposed between third-party cloud storage platforms and users of an enterprise. The API facilitates storing of files, issuing of search requests against the files and retrieval of content of the files. A file storage policy is assigned to each user, which defines access rights, storage diversity requirements and a type of encryption to be applied to files. Responsive to receiving a request to store a file, (i) searchable encrypted data is created relating to content and/or metadata of the file based on the assigned file storage policy; and (ii) the searchable encrypted data is distributed among the third-party cloud storage platforms based on the storage diversity requirements defined by the assigned file storage policy.

Dragonfruit: Cloud Provider-Agnostic Trustworthy Cloud Data Storage and Remote Processing

Eric W. D. Rozier and Saman Zonouz
Electrical and Computer Engineering
University of Miami
{e.rozier, s.zonouz}@miami.edu

David Redberg
Fortinet Inc.
Sunnyvale, California 94086
dredberg@fortinet.com

Abstract—Trustworthy cloud services require practical secure storage and data processing techniques that enable end-users to upload sensitive data and perform computations remotely without having to first download the data. In this paper, we present Dragonfruit, a cloud provider-agnostic searchable cloud data storage solution, that allows the utilization of several existing cloud providers, and the execution of search queries over encrypted data by customers, using unmodified cloud infrastructures. In particular, Dragonfruit makes use of filename search capabilities that most existing cloud providers support to embed searchable data within the cloud. Dragonfruit supports queries using complex Boolean expressions on structured data formats such as JSON. Our evaluation on a real-world test-bed show that Dragonfruit is able to work with several cloud providers such as Google-Drive and Dropbox simultaneously and is able to respond to search requests within a few seconds proving a reasonable performance overhead for practical usage.

I. INTRODUCTION

With the proliferation of cloud computing, outsourcing storage is becoming easier and more cost effective. Users are willing to pay for services which give them access to their data from any location, without requiring them to carry devices with large amounts of memory. Additionally the cloud offers users scalable storage without the burden of large-scale data center management. Despite the advantages provided by current cloud technologies, there is a need to ensure that the privacy of the data stored by a client remains intact even when using cloud infrastructure managed by a third party.

Recent revelations about the National Security Agency's PRISM program [1], and the collusion of many cloud providers such as Facebook, Microsoft, and Dropbox [2], [3] with secret government programs, makes the privacy of customer data when stored on the cloud suspect. In addition to programs such as PRISM which violates the security and confidentiality of user data, governments have also directed companies to turn over master encryption keys used to secure data [4], [5], further exposing confidential customer data, and increasing the risk that it will be compromised. Even if one trusts government programs with their data, government employees can accidentally or maliciously expose data they acquire (as has happened in the past, e.g. [6], [7]).

The risk posed to customers who wish to keep their data safe from competitors, and to comply with privacy restrictions placed on them by an increasingly complex space of local, state, federal, and international legislation (e.g. HIPPA [8], [9], state regulations [10], international law [11]), has manifested to cloud providers in the US in a very tangible form. In the short

time since PRISM was revealed, 10% of officials at non-US companies had already canceled their contracts with US cloud providers, and 56% of non-US businesses surveyed by the Cloud Security Alliance reported that they are now hesitant to work with US-based cloud operators [12]. Many companies are now seeking to do business with competitors in Europe, with some Swiss cloud hosting companies seeing a 45% growth [13].

In order to prevent further damage to US-based cloud operations, and to restore faith in the solutions available here, and elsewhere, new technologies must be developed which provide better than end-to-end encryption. We must develop technologies that are resistant to the attack vectors presented by cloud collusion. Our objective in this study is to design and evaluate a practical and scalable framework for high-performance and security-aware electronic search on large-scale databases of customer records. In this paper we describe algorithms and systems for securing cloud-based storage and providing search over these encrypted records enabling the use of remote untrusted cloud-servers while reducing information leakage. We believe that the proposed methods have the potential to significantly contribute to national security, industrial confidentiality, confidence in US-based cloud resources, and compliance with new federally mandated privacy standards.

In our solution, Project: Dragonfruit, individual customers encrypt their data before sending it to the cloud. Afterwards the cloud-resident encrypted data records can be processed (queried) remotely by the customers. This processing occurs in a way which minimizes the loss of data confidentiality. Traditional encryption schemes do not allow for search to be performed over encrypted data meaning that the data owner has to download the whole data set each time it needs a small part of the data. Given the current rates of data growth, and the growing expense of bandwidth and local storage this is not a practical solution.

In summary, the contributions of this paper are as follows.

- The implementation of a novel cloud-storage platform which minimizes information leakage by limiting trust to a local trusted domain under which the user has full physical control.
- The implementation of a searchable encryption scheme which allows a user to perform searches over encrypted data stored on the cloud, while preserving confidentiality.
- Performance testings of our implemented system com-

paring various approaches to the storing of searchable cypher-text on the cloud.

- Providing a holistic solution in a cloud-agnostic manner, which allows users to fight emergent threats to cloud-security, and provides existing cloud-providers with a way to reestablish trust from foreign markets.

II. RELATED WORK

The security challenges span several areas of research in the domain of cloud security. We briefly go over the related literature, and discuss their main contributions and shortfalls in typical large-scale practical usage scenarios.

Making use of encryption techniques ensures that user privacy is not compromised by a data center [14]. But the problem then becomes, how can an encrypted database be queried without explicitly decrypting the records to be searched? At a high level, a searchable encryption scheme [15] provides a way to encrypt a search index so that its contents are hidden except to a party that is given appropriate tokens. The Public Key Encryption with keyword search primitive was introduced by Boneh et al. [16], and indexes encrypted documents using keywords. In particular, public-key systems that support equality ($q = a$), comparison queries ($q > a$) as well as more general queries such as subset queries ($q \in S$) have been designed. Song et al. [17] presented a symmetric cryptography setting for searchable encryption architectures for equality tests. Equality tests in the public-key setting are closely related to Anonymous Identity Based Encryption and were developed in [18] by Boneh et al. In [19], Boneh et al. introduce a new primitive called Hidden Vector Encryption that can be used for performing more general conjunctive queries such as conjunction of equality tests, conjunction of comparison queries and subset queries. This system can also be used to support arbitrary conjunctive queries without revealing any information on the individual conjuncts.

Additionally, there are several previous efforts that have focused on exact keyword search; however, in the case of electronic medical records, a match between a query and a data point, does not necessarily mean that the two values are equal. Instead, a match indicates a high enough resemblance between the query and a data point. By using the above mentioned encryption schemes however, two objects, close in value, may be encrypted to very different cipher values. Although error-tolerant search over plain data has also been explored by several past papers [20], it does not satisfy our data privacy requirement as it does not support encrypted data search. Bringer et al. [21] present an error-tolerant searchable encryption scheme which permits one to make searches on encrypted data with only an approximation of some keyword. The main problem with their solution is that the associated construction algorithm is computationally expensive, and hence is not scalable to large databases with large number of queries processed daily. Therefore, a significant problem in this setting is to design efficient and scalable encryption algorithms that enables this type of fuzzy matching.

III. THE CHALLENGES OF SECURING THE CLOUD

Cloud services today offer businesses very attractive economic [22] advantages over conventional in-house data center services, but present several critical challenges when it comes

to protecting the data that is sent to the cloud. This is because sensitive, proprietary, confidential and private data is stored in the cloud when implementing strategies utilizing cloud storage or Software-as-a-Service applications. Key management is a critical factor in securing cloud data. Today, most cloud service providers take measures to secure customers data by the use of encryption. However, the cloud service providers also hold the encryption keys, making key management the weak link in the cloud data security chain. The fact is that if the customer is not always in control of the encryption key, the data in the cloud is at risk. Further, many cloud providers employ data deduplication and other optimization techniques that actually open side-channel attacks on the data.

For regulatory and compliance needs, organizations require knowledge of how their data is protected, where the data is stored geographically, and by what means the cloud service providers maintain the integrity and availability of data in the event of a disaster [23]. Given that it is impossible to know whether today's trusted cloud provider will be there tomorrow, it is incumbent on the organization that owns the data to make sure that data is available should the cloud provider vanish. This implies that the organization takes the responsibility for cloud data to be replicated across multiple cloud storage services.

One approach to securing cloud data while keeping encryption keys in the hands of the customer is to provide a gateway that simply encrypts all data sent to the cloud and decrypts the data coming back from the cloud using a proven encryption technique such as AES 256. But one of the main reasons that encryption has not been put into widespread use is that the data encryption process has a performance impact. Encryption is costly in terms of compute time. Therefore, any solution that uses encryption to protect data before sending it to the cloud must do so in a way that minimizes the impact on performance.

The aforementioned gateway encryption approach protects the data adequately but will prohibit search and sort operations on the cloud data and will break functions in applications like Salesforce, Google Apps or SAP, thereby negating some of the advantages of using the cloud services in the first place. New technology to encrypt cloud data while preserving useful operations that cloud-based applications perform on that data is needed. Further, operations-preserving and format-preserving encryptions only add to the performance impacts already challenging cloud data encryption from a user productivity perspective.

IV. ENCODING SEARCHABLE INDICES

We present how Dragonfruit makes use of search-aware encryption [24], [25] to prevent attackers from gaining unauthorized confidentiality-sensitive data and records. Generally, owners of confidentiality-sensitive data, such as electronic medical records, can not trust (even well-known) cloud providers for storing their data in plain form, due both to internal security policies, and federal or state laws and requirements [8], [10]. Therefore, data must be encrypted before storing it on a remote server. While this prevents unauthorized access and helps ensure the confidentiality of customer data, regular encryption prevents one from searching over encrypted data. As a result, the whole data set must be returned for any query, even if the user is only interested in records with a certain

property. This method is not efficient in terms of bandwidth or the computational power requirements on the client side because the client still has to decrypt all received data to be able to extract those which are actually needed.

Let us assume that the trusted gateway intends to encrypt and send some data record R to the cloud for permanent storage and that the encryption should be such that it preserves the capability to be searchable by specific queries. The algorithm consists of four major steps, namely *Setup*, *Encryption*, *Token*, and *Query*. In the following paragraphs, we describe each step in more detail.

Setup: In this step we initiate all the cryptographic parameters, i.e., public P and private (secret) S keys:

$$P \leftarrow (P_1, P_2, \dots, P_t), \quad (1)$$

and

$$S \leftarrow (S_1, S_2, \dots, S_t), \quad (2)$$

where random public and private keys are generated. The variable t denotes the possible number of predicates (queries) that the customer can ask for in the future. For instance, in medical records if *race* is chosen to be the searchable feature in a patient record database, the possible queries can be formulated as $\{\text{Asian}, \text{White}, \text{African American}, \text{Hispanic}\}$ or all the integer values between 0 and 100 for the *age* feature. An important point is that all searchable features need to first be quantified before they are encrypted.

Encryption: The encryption phase does the main offline step of the whole scheme by encrypting each record one by one. It is important to note that this step will be completed locally by the trusted gateways so that the cloud provider will have access to cipher texts only, and not the encryption keys themselves. In particular, the encryption step is carried as using the following assignments for $0 < j < t + 1$

$$C_j \leftarrow \begin{cases} \text{Encrypt}(P_j, R) & \text{if } \text{Predicate}_j(I) = 1, \\ \text{Encrypt}(P_j, 0) & \text{Otherwise.} \end{cases} \quad (3)$$

Once completed, this step will give us a cipher text vector

$$C \leftarrow (C_1, C_2, \dots, C_t), \quad (4)$$

whose length is the number of possible predicates t .

Token: This step prepares the framework to process a given query. In particular, for a given query that is represented as a logical predicate, as discussed above, e.g., *Select records whose race is Asian*, the framework generates the corresponding *token* to be sent to the cloud provider. Clearly, this step must also be accomplished locally by the trusted gateway, with the cloud provider only given permission to see the encrypted token. In particular, to complete this step, the trusted gateway chooses a single private key from S that corresponds to the selected query predicate¹. Let us assume that the predicate is the i -th element in our list of all possible queries.

Query: The final step of the searchable encryption scheme is processing the received query by the cloud provider that has access to the encrypted records, and the single private key that the trusted gateway has sent. Finally, the cloud provider decrypts the corresponding cipher text C_i for individual patient

record. It is easy to follow that the cloud provider will retrieve and correctly decrypt only the records which match the received query, and will get 0 as the result of all other decryptions (see equation (IV)). The retrieved records are then sent back to the trusted gateway. It is important to mention that for absolute data disclosure prevention, the trusted gateway should encrypt the records using a symmetric key and unique salt such that R is already encrypted and the cloud provider is not allowed to see the actual record.

Using the above mentioned algorithm, our framework makes sure that the cloud provider can perform and accomplish the search over the encrypted data, and in the meanwhile, cannot get access to any confidential data.

A. Cloud Provider-Agnostic Searchable Encryption

It is crucial that Dragonfruit performs its searchable encryption in a cloud provider-agnostic manner such that it is usable regardless of the cloud provider's infrastructural specifications. Consequently, end users can use Dragonfruit to store and search for their data remotely in the cloud without any Dragonfruit-specific support by the cloud provider. To this end, Dragonfruit makes use of the most basic functionality that almost all of the existing cloud providers provide. In particular, Dragonfruit employs the file-name search functionality, and therefore, stores the relevant information in the file-names while storing customer data in the cloud. Once the data is stored, when a user queries for a given search term, Dragonfruit calls the cloud provider's API functions to check for the existence of valid cypher-text.

To implement the above mentioned solution, Dragonfruit requires a global policy file where all the searchable fields, their value ranges, and the discretization granularity are determined. For instance, *age* may be assigned as a searchable field with the $[0, 120]$ range, and 5 year granularity.² In this *age* example, the individual data point values are discretized into 5-year buckets, e.g., ages between $[0, 5)$, $[5, 10)$, $[10, 15)$, ... It is important to mention that the policy design is a one-time effort that is done initially before the data are sent by the end users. When an *Encryption* request is issued by the end-user for a particular sensitive file (see Section IV), Dragonfruit creates a folder in the cloud where the directory name is assigned with the AES-512 encrypted version of the original file name. Encrypted strings contain non-ASCII characters and therefore cannot be assigned as file names; therefore, before the directory creation step, Dragonfruit performs a one-to-one reversible mapping from the encrypted string and a usually-long file name of ASCII characters. Dragonfruit stores the encrypted version of the original file within the created directory. Dragonfruit then creates several zero-size files each assigned with a name equal to one of the computed cipher texts C_j as described in Section IV. For additional security, Dragonfruit can stripe the contents of the file over these files, further obfuscating which names relate to the file vs. cypher-text.

During the query phase, Dragonfruit receives the plain-text query request from the end-user sites and crafts the corresponding encrypted queries (Section IV) and calls the cloud's file-name search API function to search for the target files. Upon the returned list of files which matched the file-name search,

¹Remember that S includes a private key for each possible predicate/query.

²The granularity amount effects the the chance for false positives.

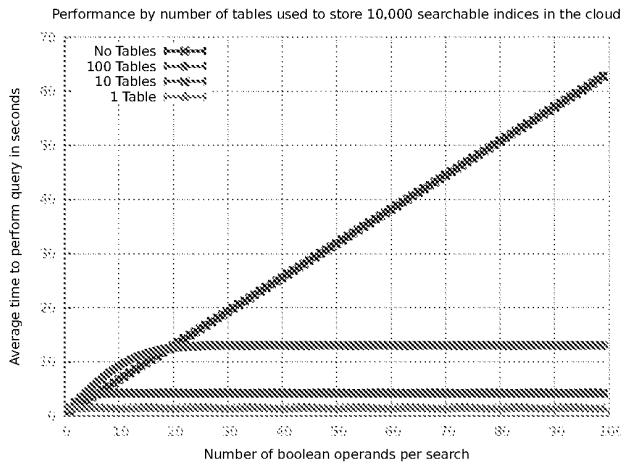


Fig. 1. Performance comparison of query algorithms involving direct look up of each cypher-text on the cloud, and downloading tables of cypher-text on the cloud, using differing number of tables. All tests were executed over files with 10,000 searchable indices, and searches involving from one to 99 boolean operands.

Dragonfruit browses the directory of each directory in which a cypher-text file was found and locates those files which contain the encrypted data and downloads them. Dragonfruit decrypts the downloaded file and returns to the user.

V. PERFORMABILITY AND THE CLOUD

Given that we are storing the searchable indices on the cloud the performability of our solution is a large concern. We implemented and tested two methods for retrieving searchable terms from the cloud and tested them experimentally with Dragonfruit. The first method involves simply storing the indices individually on the cloud-provider's system. When a query for a given term is used, the index is generated and each is searched in turn. For large boolean queries, however, this method can prove costly given that cloud providers throttle requests and limit the rate at which queries can be performed.

The second method we tested involves a hierarchy of indices generated using a variable-bit SHA-3 hashing algorithm [26] (we used the keccak sponge function for our tests [27]). In this case, we hash all cypher-texts as usual, but then generate a second hash for each cypher-text which indicates the key for a table in which many cypher-texts are aggregated.

In this case, when a user wants to perform a search using a some cypher-text as a boolean operand (e.g. records where $(Race = Asian) \wedge (Age > 35)$), the cypher-text is hashed using SHA-3 to find the table hash which represents the path of the table on the cloud if present. The cloud provider is queried for the table, which is then downloaded, loaded into memory, and then searched for the original cypher-text.

The results of our experiment are shown in Figure 1 for setups involving no tables, 100 tables, 10 tables, and a single table, each dividing a total of 10,000 searchable indices, and plots the time required to process the query as a function of the number of boolean operands used. With no tables, the performance scales linearly with the number of operands. Additional search terms each incur the cost of sending and receiving the request to the cloud, along with the throttling delay imposed by the cloud-provider. Response time

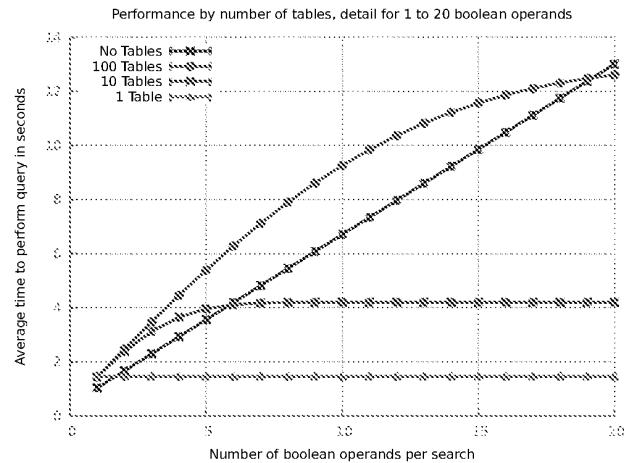


Fig. 2. Performance comparison of query algorithms involving direct look up of each cypher-text on the cloud, and downloading tables of cypher-text on the cloud, using differing number of tables. All tests were executed over files with 10,000 searchable indices, and searches involving from one to 20 boolean operands.

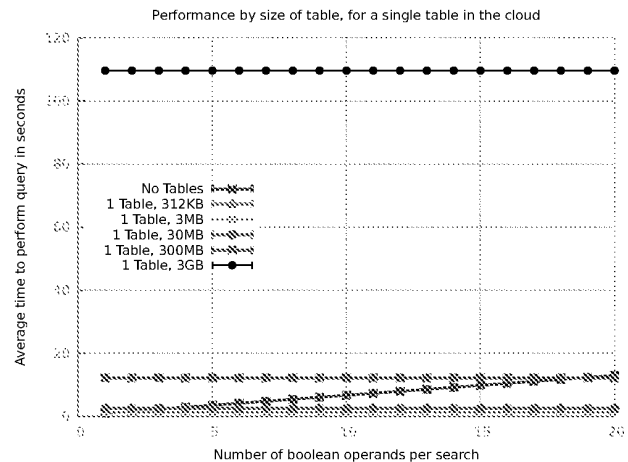


Fig. 3. Performance comparison of query algorithms involving direct look up of each cypher-text on the cloud, and downloading a single table of cypher-text of varying sizes, from 312KB to 3GB.

of the algorithm quickly becomes unmanageable for complex searches.

Using 100 tables, the overhead penalties to download the table, store it in memory, and perform the search locally dominates performance until around 19 search terms, at which point (largely in thanks to the birthday paradox [28]) we have loaded sufficient tables to account for most search terms, and the table approach outperforms the no-table approach. Using 10 tables, this effect kicks in much earlier, outperforming the no table approach for 6 or more boolean search terms, and always outperforming the 100 table approach. With a single table, containing all entries (and utilizing 312KB of RAM), performance is better for all searches involving two or more terms, losing to the no table approach only for a single search term. In all of the table approaches, once sufficient tables have been loaded to account for most search terms, performance is roughly static (local searches for keys in the tables resident in memory can be performed so quickly, the performance is

Appendix A

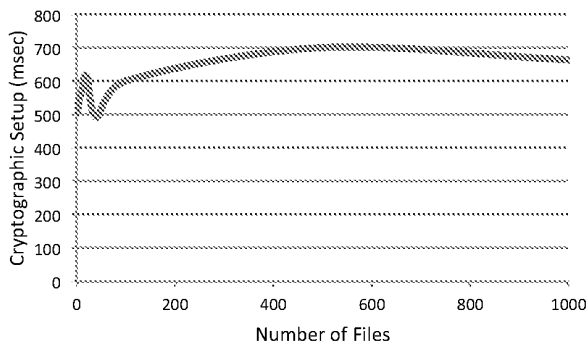


Fig. 4. The Cryptographic Setup Time Requirement

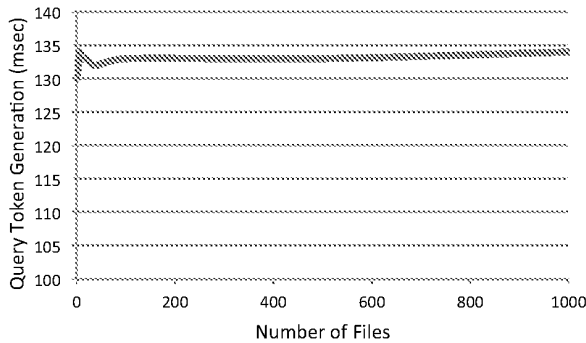


Fig. 5. The Cryptographic Token Generation Time Requirement

dominated by the setup time). Additional detail is provided in Figure 2, which shows the behavior of these methods for one to 20 boolean operands.

To explore the setup costs for larger tables, we also performed tests on searches involving one to 99 boolean operands on tables containing 10,000; 100,000; 1,000,000; 10,000,000; and 100,000,000 searchable terms, these required 312KB, 3MB, 30MB, 300MB, and 3GB of RAM respectively. The results of these experiments are shown in Figure 3. For tables up to 1,000,000 terms in size, the table approach clearly beats the no-table approach for a single table. When 10,000,000 entries are stored in the table, the no-table approach is faster for 19 or fewer boolean operands, at which point the setup cost of the table equals the cost to search each operand. For larger tables, however, the setup costs dominate the performance.

These results favor the use a hierarchical table based approach, with the size and number of tables depending on the expected complexity of searches run by users. In general, tables should be fairly large, given the high cost of a single query, and the low setup costs for most tables once downloaded. Larger tables accounting for more possible search terms minimizes the number of queries performed, which tends to be the largest portion of setup costs for tables containing 1,000,000 terms or fewer.

VI. EXPERIMENTAL RESULTS

After implementing Dragonfruit, we measured the time requirements of its different steps for customers silos of different sizes, i.e., different number of records. In particular, Figure 4 illustrates the length of the initial setup phase for the cryptographic algorithms, e.g., key generation. As shown on

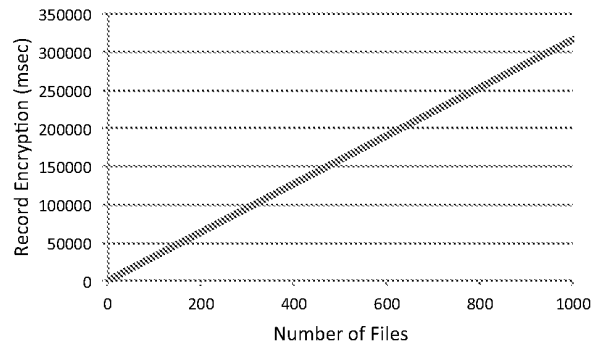


Fig. 6. The Cryptographic Encryption Time Requirement

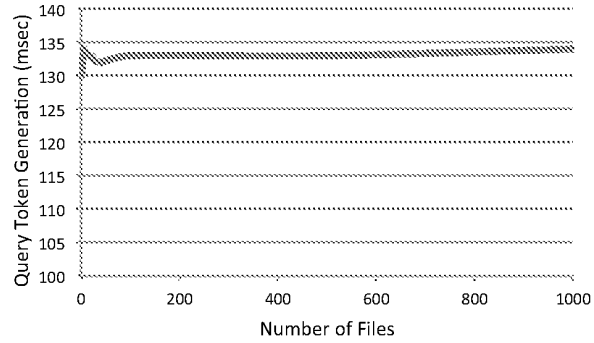


Fig. 7. The Cryptographic Query Processing Time Requirement

the graph, the time that the setup phase takes to complete stays almost the same regardless of amount of customer data. Figure 5 shows the amount of overhead that the token generation causes on the system for each individual query. It is important to note that the token generation is an online procedure that needs to be done every time a user sends the cloud provider a query to search over the data base. Furthermore, because the token generation is accomplished on the client side the online computation required to process simultaneous queries from users are distributed among the trusted gateways Dragonfruit is installed on, allowing better performance than if run on a single resource.

Figure 6 shows the performance overhead on the infrastructure caused by encryption of customer data by the trusted gateway before they are sent for permanent storage on the cloud. Although the processing time does not guarantee a real-time data encryption (approximately 5 minutes are required to encrypt 1000 example records [?], [?]), the trusted gateway can perform this computation step during an offline phase for the available records once, and on a per record basis from then on. Finally, Figure 7 shows the final step in our process, i.e., remote encrypted query processing. The algorithm requires the cloud provider to go over individual database records to guarantee zero information leakage at the end of the procedure, unlike in traditional databases, the records cannot be stored in a particular data structure within the cloud provider since it provides the cloud owner with extra information about the inter-record semantic proximity.

VII. CONCLUSION

In this paper we have presented Dragonfruit, a cloud provider-agnostic searchable cloud data storage solution, that

allows the use of several existing cloud providers to store and execute queries upon customer data using only currently existing cloud functionality. In particular, Dragonfruit makes use of the filename search capability that most of the existing cloud providers provide to store the searchable data point key values. Dragonfruit supports complex Boolean query expressions on structured data formats such as JSON. Our evaluation on a real-world test-bed showed that Dragonfruit is able to work with several cloud providers such as Google-Drive and Dropbox simultaneously and respond to data search requests within few seconds proving a reasonable performance overhead for practical usages.

VIII. FUTURE WORK

We are working to extend our implementation of Dragonfruit to provide more sophisticated methods of cypher-text storage and retrieval to improve performance, and to extend the types of queries that can be executed. In particular we are working to implement large query sets to implement full-text search on large documents with minimal overhead using a variant on the SHA-3 hierarchical hashing mentioned in Section V. We are also working to leverage our cloud-agnostic solution to allow users to load-balance their data sets across multiple clouds, and to allow for higher reliability by employing a multi-cloud solution.

ACKNOWLEDGMENT

The authors would like to thank Fortinet Inc. for the grant which funded this research project as well as our research collaborators at the company who have contributed to the work with their valuable technical comments and expertise.

REFERENCES

- [1] G. Mezzofiore, "Nsa whistleblower edward snowden: Washington snoopers are criminals," <http://www.ibtimes.co.uk/articles/479709/20130617/nsa-whistleblower-edward-snowden.htm>, International Business Times, June 2013.
- [2] S. Braun, A. Flaherty, J. Gillum, and M. Apuzzo, "Secret to prism program: Even bigger data seizure," <http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure>, June 2013.
- [3] D. Rushe, "How microsoft handed the nsa access to encrypted messages," <http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data>, The Guardian, July 2013.
- [4] D. McCullagh, "Feds put heat on web firms for master encryption keys," July 2013.
- [5] ———, "Feds tell web firms to turn over user account passwords," http://news.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/, July 2013.
- [6] T. Friedman, "VA will pay \$20 million to settle lawsuit over stolen laptop's data," <http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/>, CNN, January 2009.
- [7] J. Vijayan, "Nasa breach update: Stolen laptop had data on 10,000 users," http://www.computerworld.com/s/article/9233701/NASA_breach_update_Stolen_laptop_had_data_on_10_000_users, Computer World, November 2012.
- [8] "Public law 104-191, "health insurance portability and accountability act of 1996," [Online]. Available: <http://aspe.hhs.gov/admsimp/pli04191.htm>
- [9] "Standards for electronic transactions," 2000. [Online]. Available: <http://aspe.hhs.gov/admsimp/final/efin00.htm>
- [10] U. of California Corporate Compliance Policies and Procedures, "Legal medical record standards, policy no. 9420," <http://policy.ucop.edu/doc/1100168/LegalMedicalRecord>, May 2008.
- [11] "Datenschutzkonferenz: Geheimdienste gefährden massiv den datenverkehr zwischen deutschland und aussereuropäischen staaten," Press Release of the Conference of Data Protection Commissioners of the Federation and the Lander, Data Protection Commissioners of the Federation and the Lander of Germany, July 2013.
- [12] A. Peterson, "Nsa snooping is hurting u.s tech companies' bottom line," <http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/25/nsa-snooping-is-hurting-u-s-tech-companies-bottom-line/>, The Washington Post, July 2013.
- [13] M. Meier, "Prism expose boosts swiss data center revenues," <http://www.dailyhostnews.com/prism-expose-boosts-swiss-data-center-revenues>, Daily Host News, July 2013.
- [14] S. Kamara and K. Lauter, "Cryptographic Cloud Storage Financial Cryptography and Data Security," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. Miret, K. Sako, and F. Sebé, Eds. Springer Berlin / Heidelberg, 2010, vol. 6054, ch. 13, pp. 136–149. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14992-4_13
- [15] D. Hofheinz and E. Weinreb, "Searchable encryption with decryption in the standard model," *Cryptology ePrint Archive*, Report 2008/423, 2008, <http://eprint.iacr.org/>.
- [16] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, (2004) Public Key Encryption with Keyword Search. [Online]. Available: <http://crypto.stanford.edu/~dabo/abstracts/encsearch.html>
- [17] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of the 2000 IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 2000, pp. 44–. [Online]. Available: <http://dl.acm.org/citation.cfm?id=882494.884426>
- [18] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.
- [19] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proceedings of the 4th conference on Theory of cryptography*, ser. TCC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 535–554. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1760749.1760788>
- [20] A. Hinneburg, C. C. Aggarwal, and D. A. Keim, "What is the nearest neighbor in high dimensional spaces?" in *Proceedings of the 26th International Conference on Very Large Data Bases*, ser. VLDB '00. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2000, pp. 506–515. [Online]. Available: <http://dl.acm.org/citation.cfm?id=645926.671675>
- [21] J. Bringer, H. Chabanne, and B. Kindarji, "Error-tolerant searchable encryption," in *Proceedings of the 2009 IEEE international conference on Communications*, ser. ICC'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 768–773. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1817271.1817415>
- [22] T. Alford and G. Morton, "The economics of cloud computing," Booz Allen Hamilton, 2009.
- [23] D. Vaile, K. Kalinich, P. Fair, and A. Lawrence, "Data sovereignty and the cloud," Cyberspace Law and Policy Centre and the University of New South Wales Faculty of Law, July 2013.
- [24] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *IEEE Symposium on Security and Privacy*, 2000, pp. 44–55.
- [25] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology-Eurocrypt 2004*. Springer, 2004, pp. 506–522.
- [26] R. L. Rivest, B. Agre, D. V. Bailey, C. Crutchfield, Y. Dodis, K. E. Fleming, A. Khan, J. Krishnamurthy, Y. Lin, L. Reyzin et al., "The md6 hash function—a proposal to nist for sha-3," *Submission to NIST*, vol. 2, p. 3, 2008.
- [27] K. Gaj, E. Homsirikamol, and M. Rogawski, "Fair and comprehensive methodology for comparing hardware performance of fourteen round two sha-3 candidates using fpgas," in *Cryptographic Hardware and Embedded Systems, CHES 2010*. Springer, 2010, pp. 264–278.
- [28] P. Flajolet, D. Gardy, and L. Thimonier, "Birthday paradox, coupon collectors, caching algorithms and self-organizing search," *Discrete Applied Mathematics*, vol. 39, no. 3, pp. 207–229, 1992.

+ 100 ↗

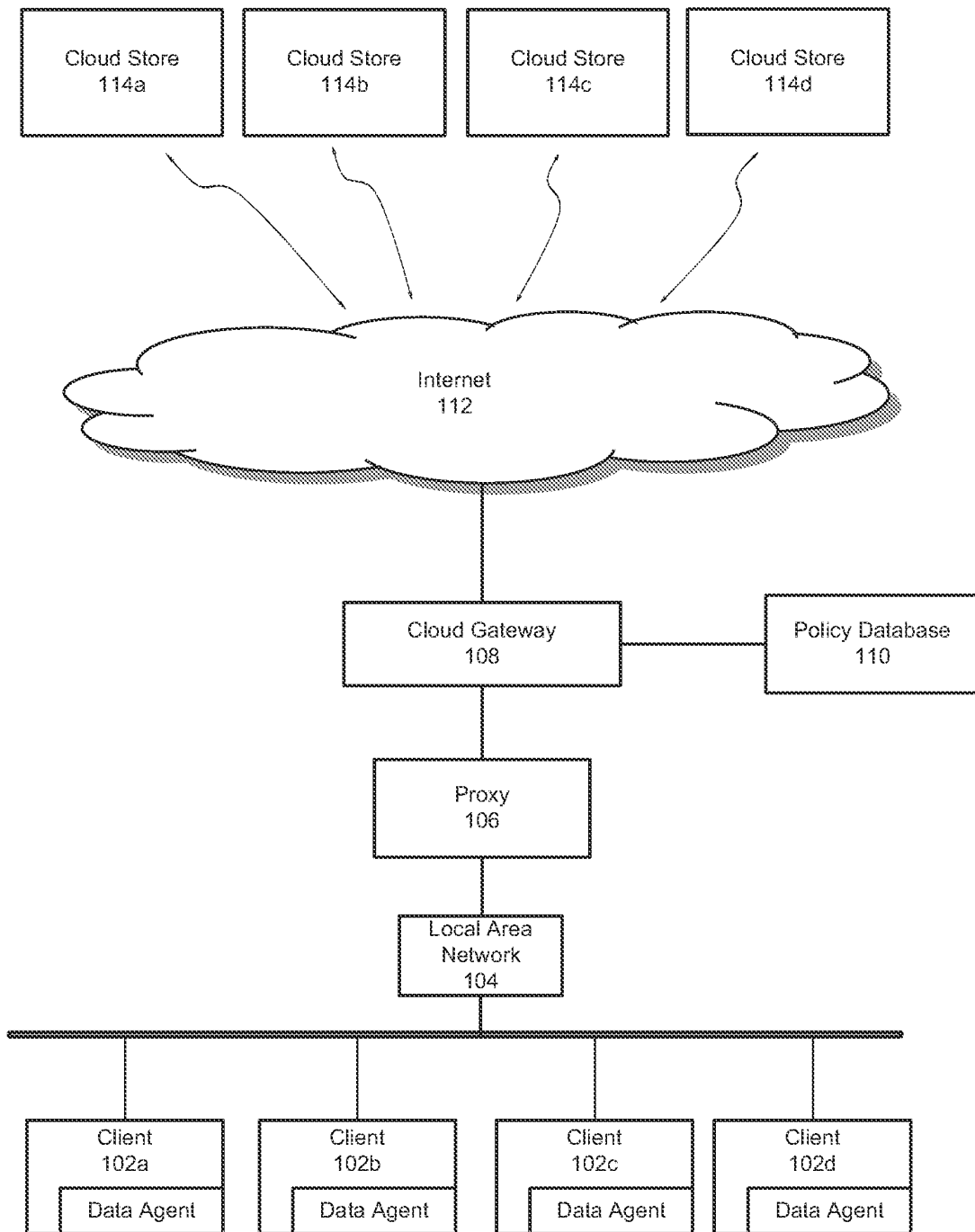


Fig. 1

+

200

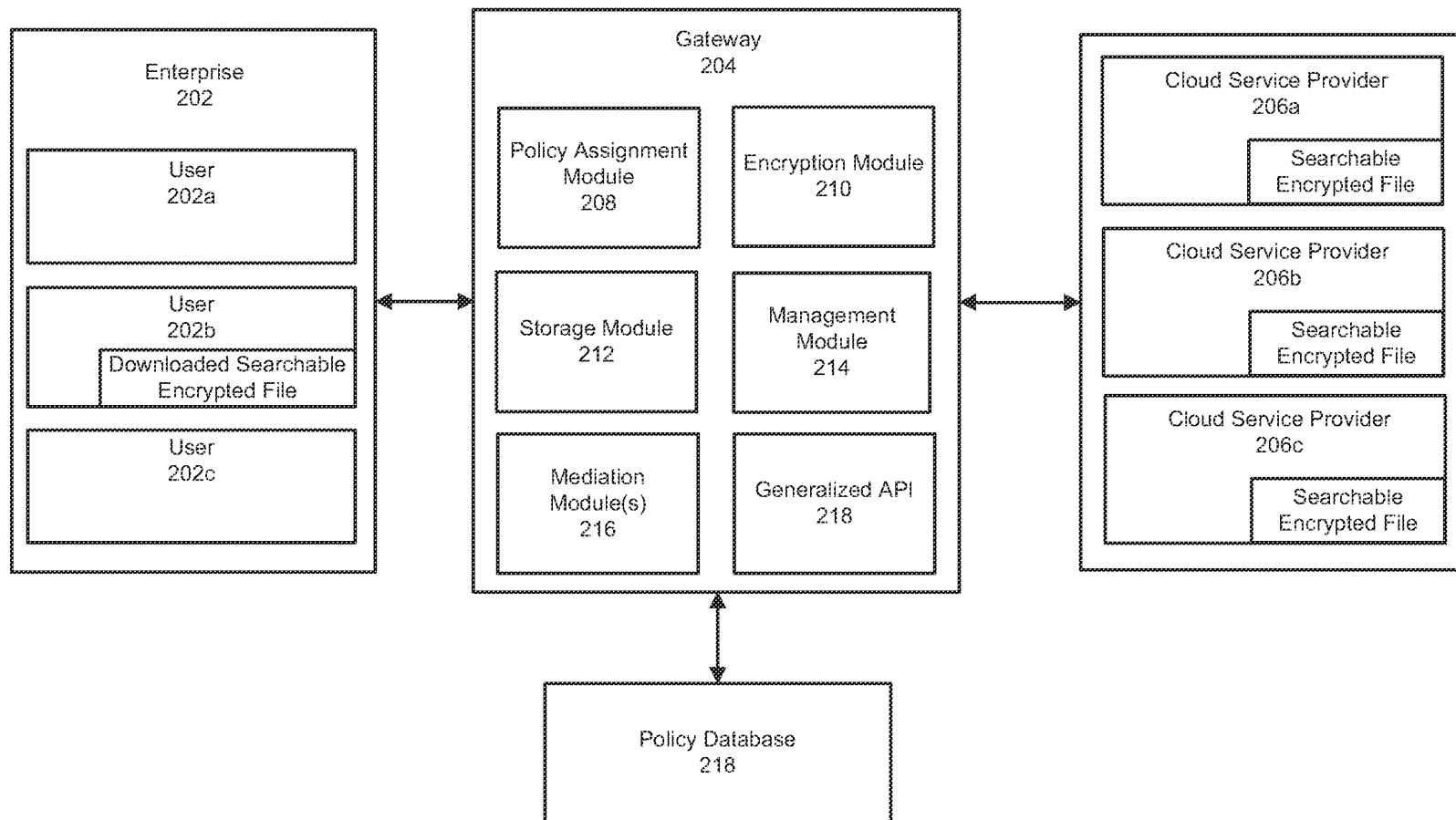


Fig. 2

+

+ 300 ↘

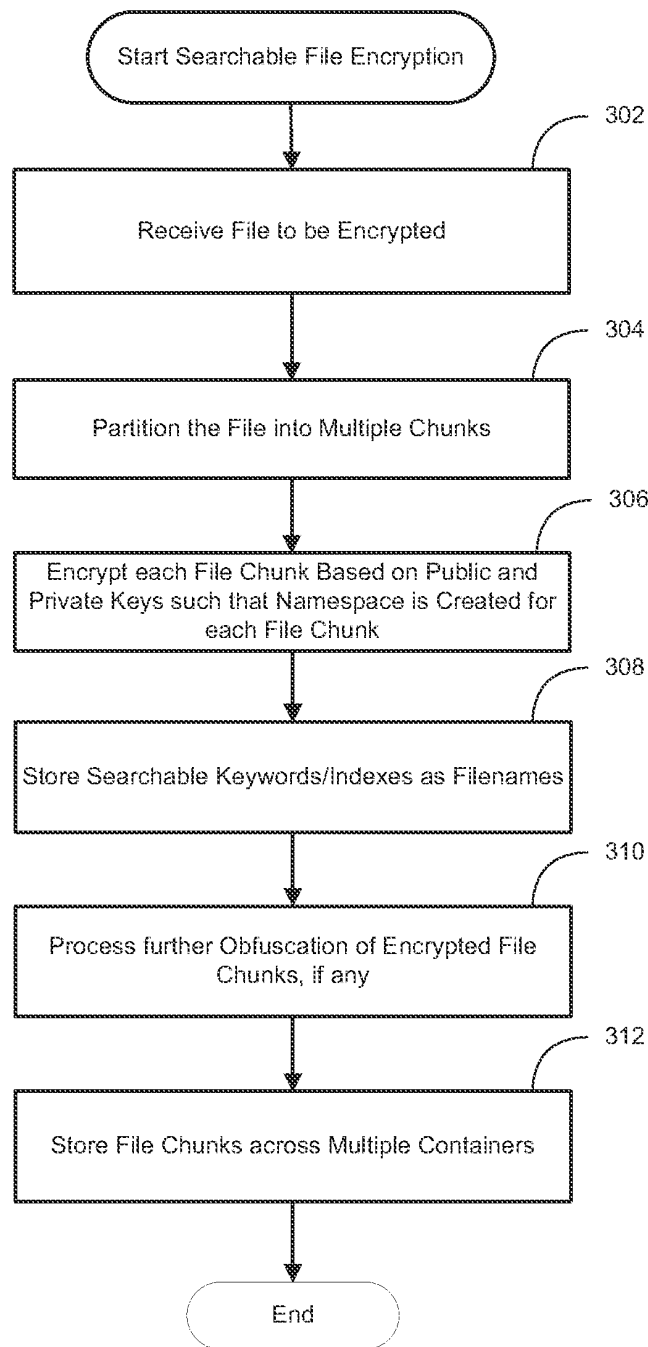


Fig. 3A

+

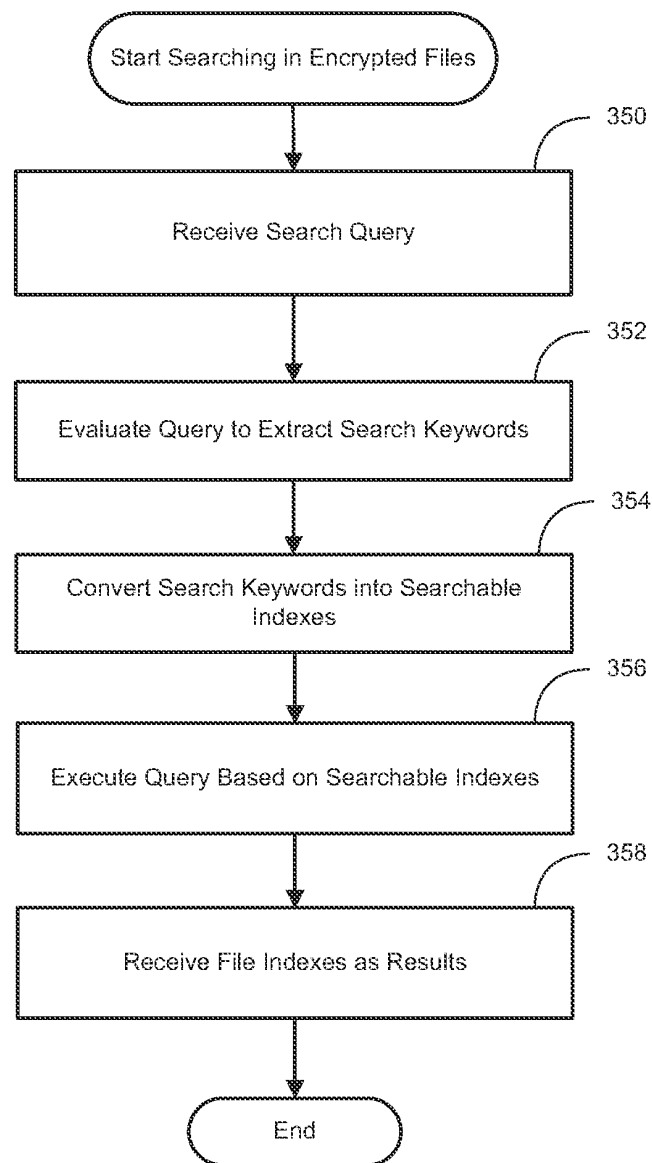
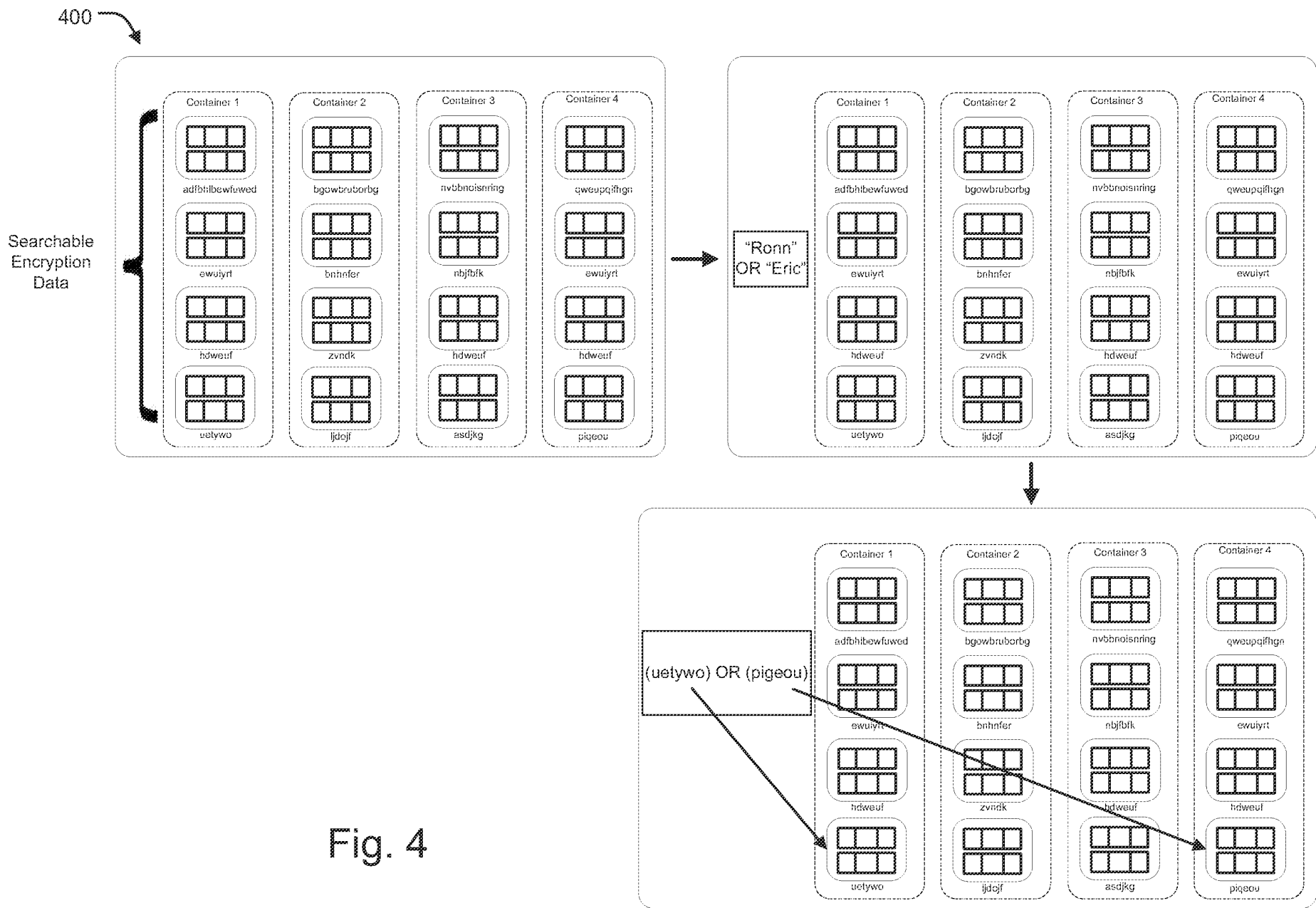


Fig. 3B



+ 500 ↘

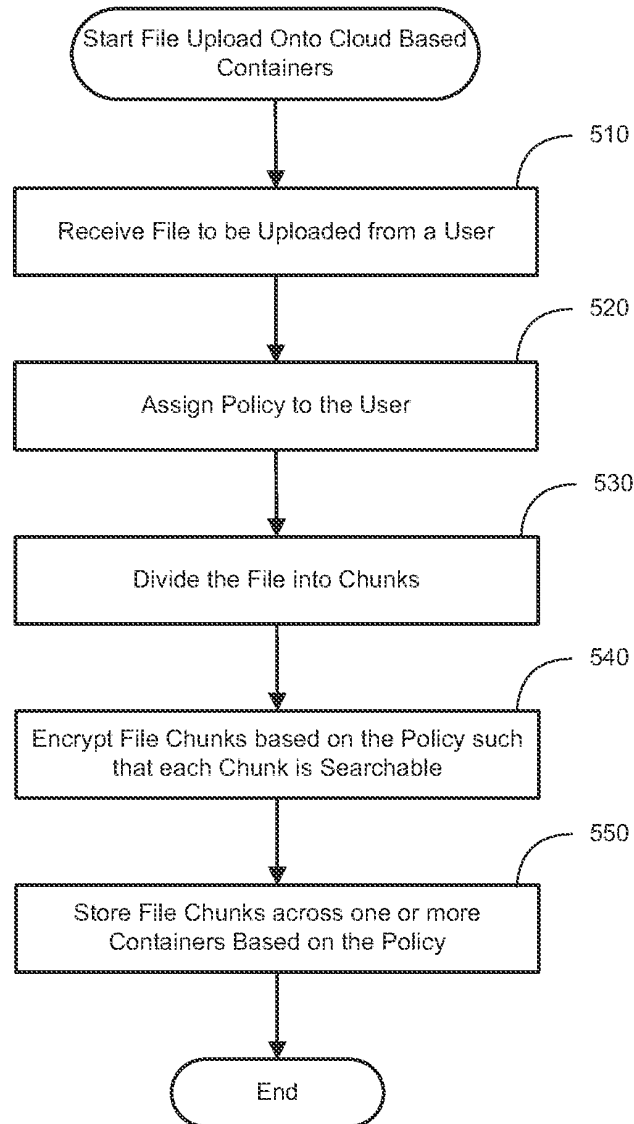


Fig. 5

+

600

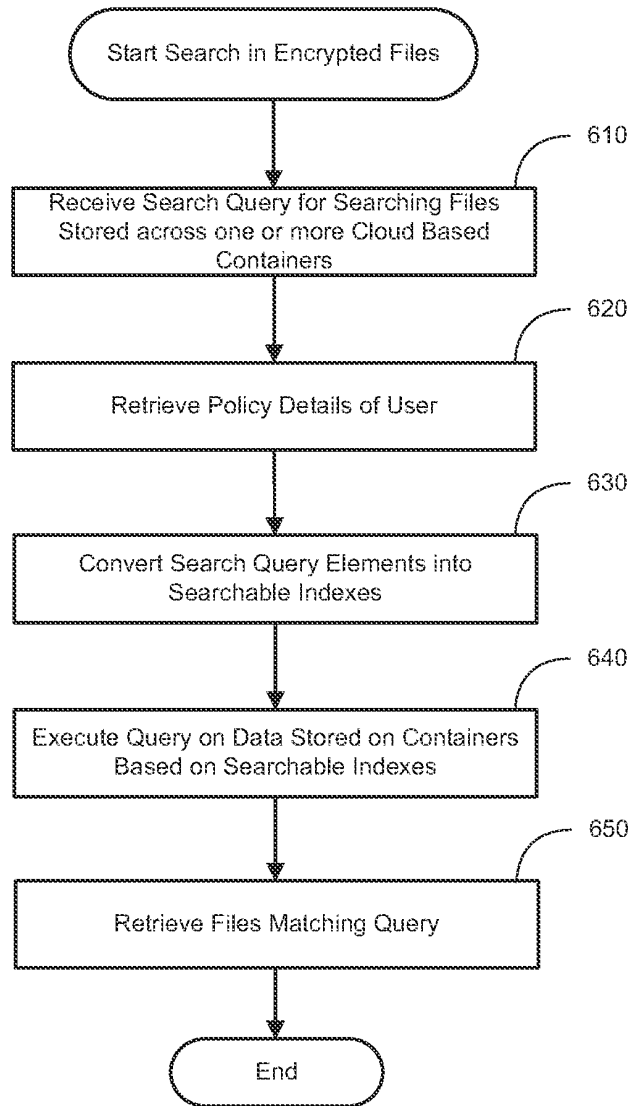


Fig. 6

700 ↗

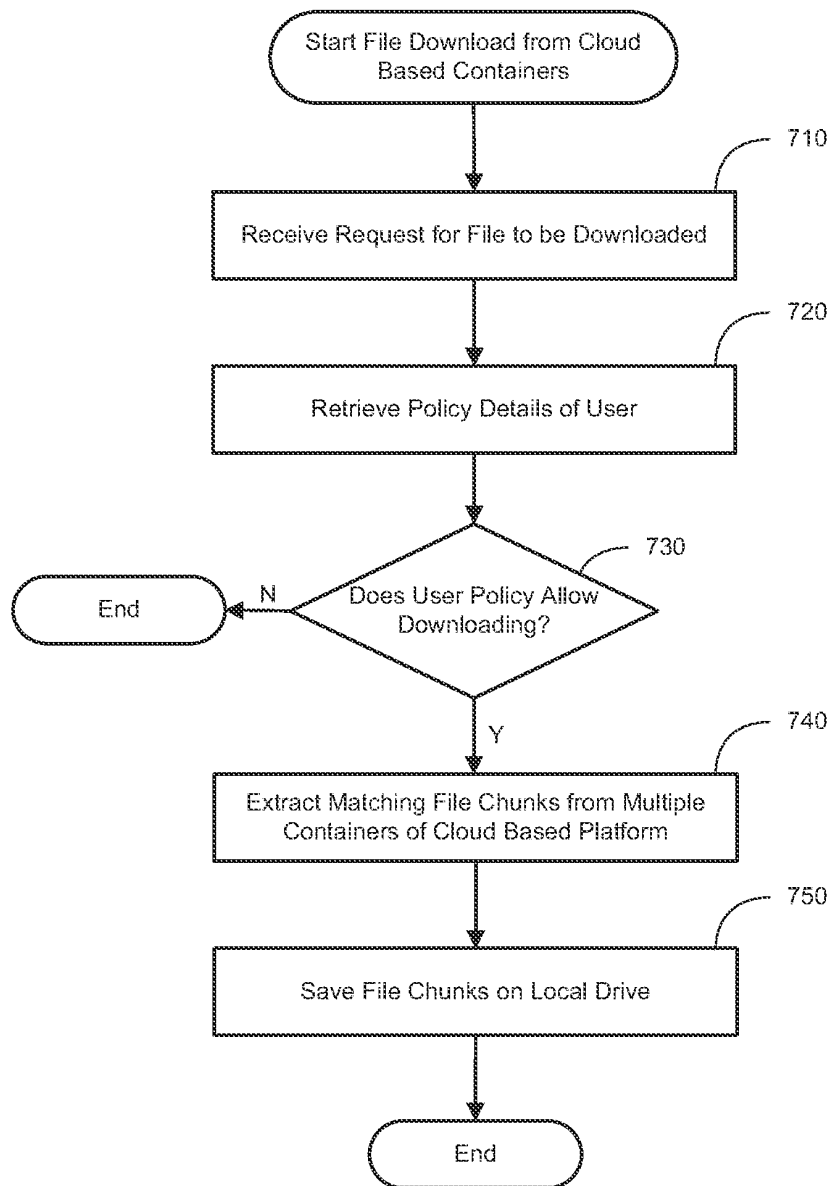


Fig. 7

800

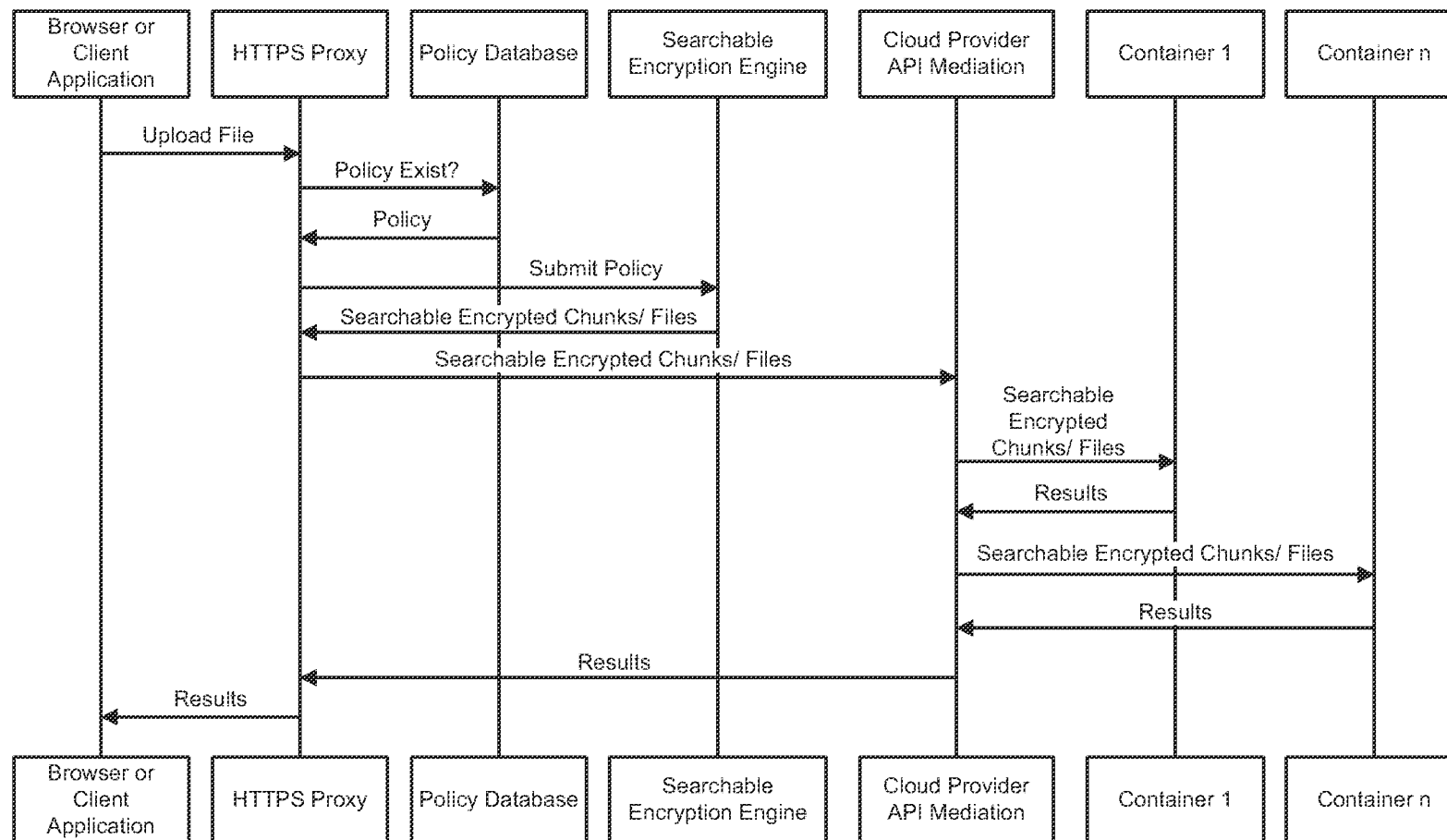


Fig. 8

+

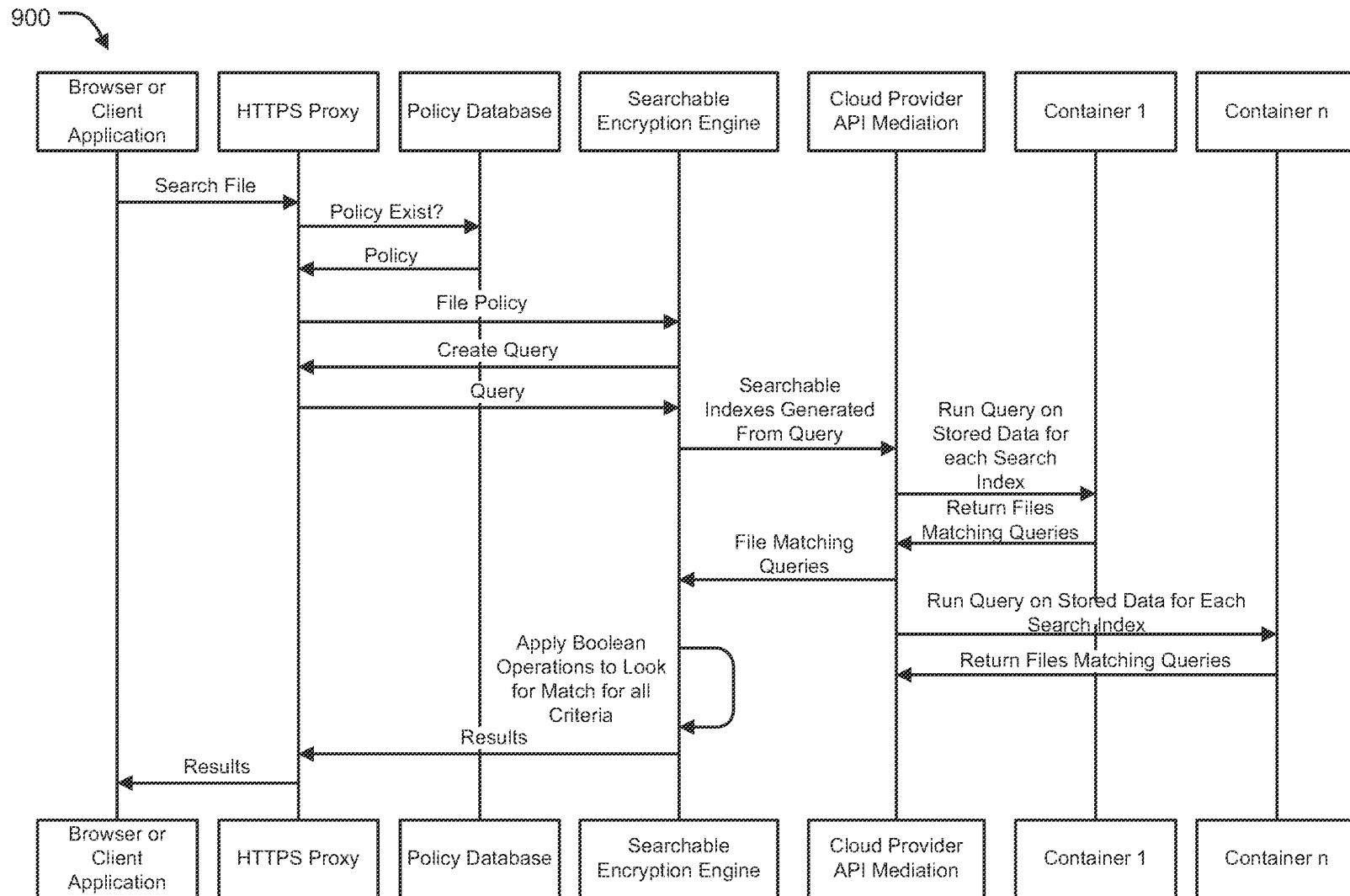


Fig. 9

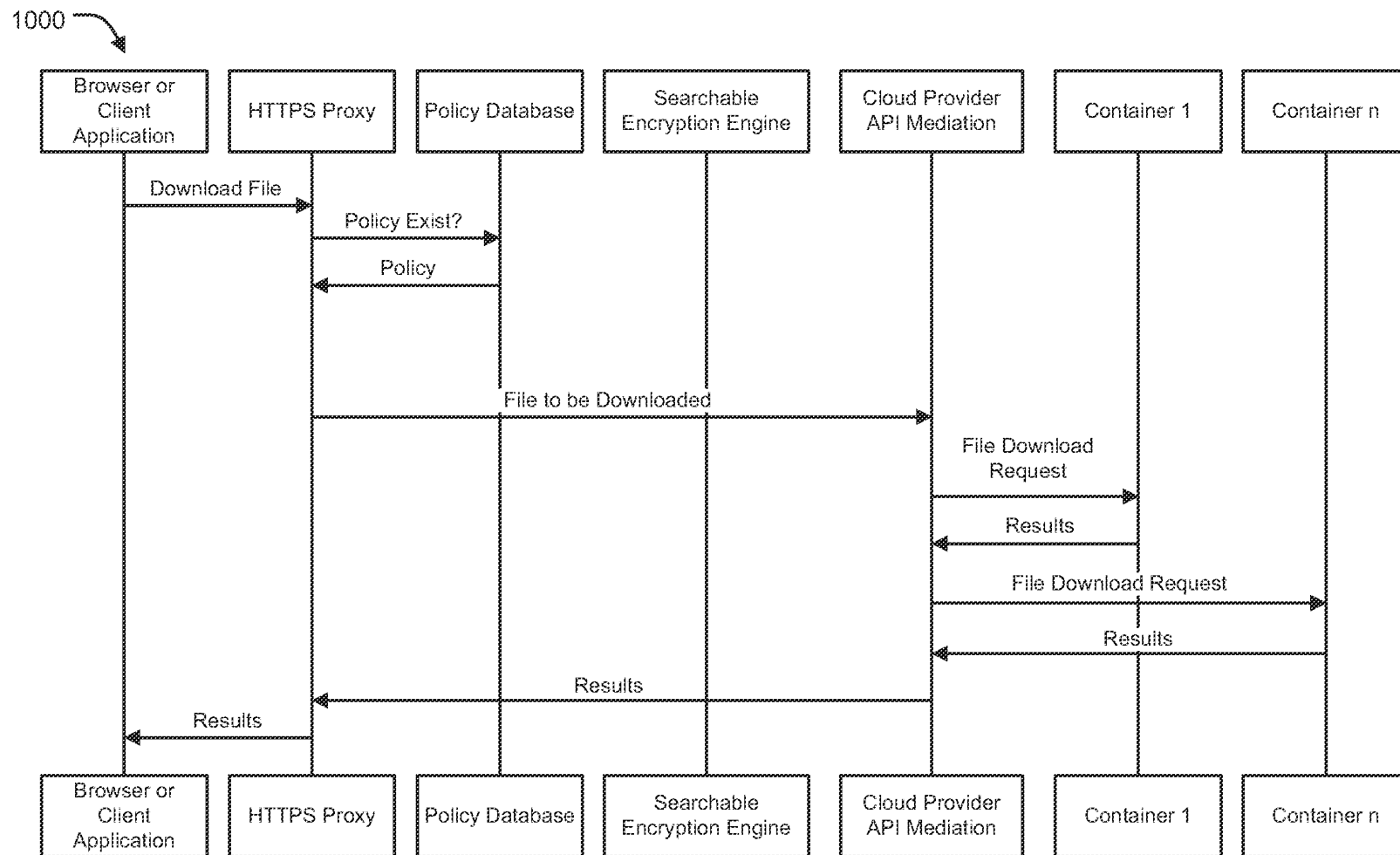


Fig. 10

+
1100 ↘

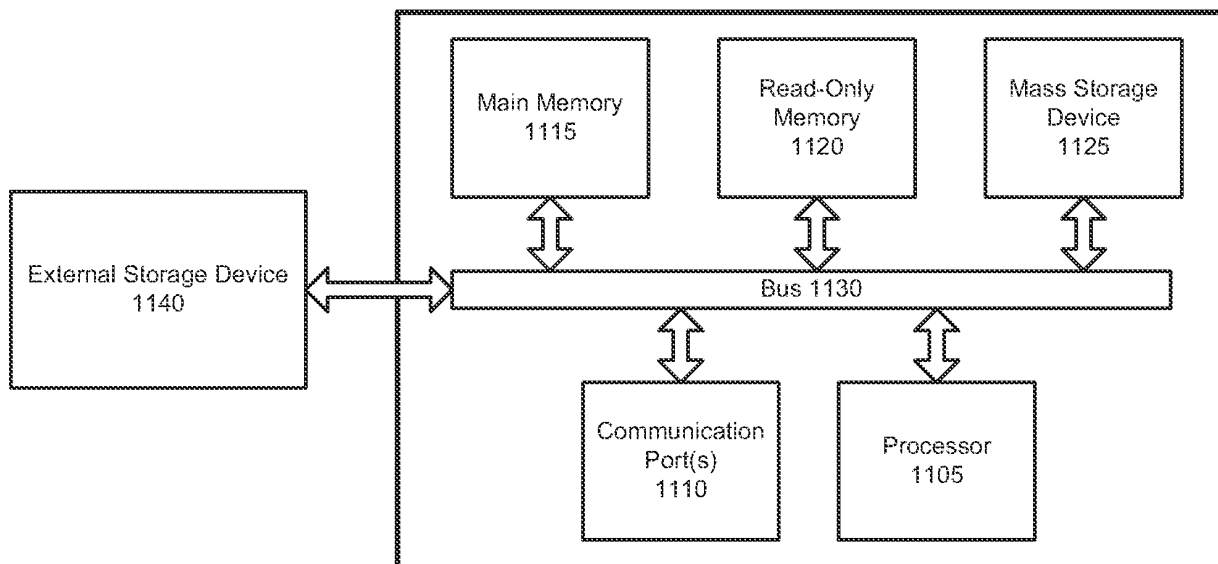


Fig. 11

+

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-011700
		Application Number	
Title of Invention	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--

Inventor Information:

Inventor 1					Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	David	A.	Redberg			
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service						
City	Sunnyvale	State/Province	CA	Country of Residence i	US	
Mailing Address of Inventor:						
Address 1		1059 Merrimac Dr.				
Address 2						
City	Sunnyvale	State/Province	CA			
Postal Code	94087	Country i	US			
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						
Add						

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	64128		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
Attorney Docket Number	FORT-011700	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	12	Suggested Figure for Publication (if any)	8

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-011700
		Application Number	
Title of Invention	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		

Publication Information:
☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	64128		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the application number blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ^j (if applicable)

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-011700
		Application Number	
Title of Invention	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			
			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.
--

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices
If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application. In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application. In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.
--

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-011700
		Application Number	
Title of Invention	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		

Applicant 1				Remove
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.				
Clear				
☒ Assignee		☐ Legal Representative under 35 U.S.C. 117		☐ Joint Inventor
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:				
Name of the Deceased or Legally Incapacitated Inventor :				
If the Applicant is an Organization check here. ☒				
Organization Name	Fortinet, Inc.			
Mailing Address Information:				
Address 1	1090 Kifer Rd.			
Address 2				
City	Sunnyvale	State/Province	CA	
Country ⁱ	US	Postal Code	94086	
Phone Number		Fax Number		
Email Address				
Additional Applicant Data may be generated within this form by selecting the Add button. Add				

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.	
Assignee 1	
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.	
Remove	
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-011700
		Application Number	
Title of Invention	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		

Organization Name	Fortinet, Inc.
-------------------	----------------

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	1090 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country i	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Michael A DeSanctis/			Date (YYYY-MM-DD)	2013-12-02
First Name	Michael A.	Last Name	DeSanctis	Registration Number	39957
Additional Signature may be generated within this form by selecting the Add button.					Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
First Named Inventor/Applicant Name:		David A. Redberg		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-011700		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Pages:				
Claims:				
Claims in Excess of 20	1202	12	80	960
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2560

Electronic Acknowledgement Receipt

EFS ID:	17544599
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	02-DEC-2013
Filing Date:	
Time Stamp:	18:31:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2560
RAM confirmation Number	6667
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1		Patent_Application.pdf	287727	yes	37
			bd11e1570e4a0cad807cd5e730e48cd321312b5		
	Multipart Description/PDF files in .zip description				
	Document Description	Start	End		
	Specification	1	31		
	Claims	32	36		
	Abstract	37	37		
Warnings:					
Information:					
2	Appendix to the Specification	appendix_a.pdf	120676	no	6
			58b3d109a5e4a9f924a2f61d206760d2ca9e2ac1		
Warnings:					
Information:					
3	Drawings-only black and white line drawings	drawings.pdf	92659	no	12
			10cbb6a2ec446d90ac47463e1b8f6ff757d772e3		
Warnings:					
Information:					
4	Application Data Sheet	ads.pdf	1265052	no	6
			a2fc9d9634d268bbbedf0124ac2b05345da24db56		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36501	no	2
			3edfb60b838bfadc94296004e4e516b2d614aa29		
Warnings:					
Information:					
Total Files Size (in bytes):			1802615		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SCORE Placeholder Sheet for IFW Content

Application Number: 14094484

Document Date: 12/02/2013

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://Score.uspto.gov/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO.	TOT CLAIMS	IND CLAIMS
14/094,484	12/02/2013	2161	2560	FORT-011700	32	3

CONFIRMATION NO. 4264

64128

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

FILING RECEIPT



OC000000065505738

Date Mailed: 12/19/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

David A. Redberg, Sunnyvale, CA;

Applicant(s)

Fortinet, Inc., Sunnyvale, CA

Assignment For Published Patent Application

Fortinet, Inc., Sunnyvale, CA

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 12/12/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/094,484**

Projected Publication Date: To Be Determined - pending completion of Corrected Papers

Non-Publication Request: No

Early Publication Request: No

page 1 of 3

Title

SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

Preliminary Class

707

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/094,484	12/02/2013	David A. Redberg	FORT-011700

CONFIRMATION NO. 4264

64128

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

FORMALITIES LETTER



Date Mailed: 12/19/2013

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
 - More than one figure is present and each figure is not labeled "Fig." with a consecutive Arabic numeral (1, 2, etc.) or an Arabic numeral and capital letter in the English alphabet (A, B, etc.)(see 37 CFR 1.84(u)(1)). See Figure(s) 4A,4B,4C. A brief description of the several views of the drawings (see 37 CFR 1.74) should be added or amended to correspond to the corrected numbering of the figures. See also 37 CFR 1.77(b)(9).

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge as set forth in 37 CFR 1.16(f) was not received.
The surcharge is due for any one of:
 - late submission of the basic filing fee, search fee, or examination fee,
 - late submission of inventor's oath or declaration,
 - filing an application that does not contain at least one claim on filing, or
 - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are:

- \$ 140 surcharge.
- \$(.00) Previous Payment Amount.
- \$ 140 TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
David A. Redberg

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice".
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/nhassani/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/094,484			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	600		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720		
TOTAL CLAIMS (37 CFR 1.16(i))	32 minus 20 =	*				x 80 =	960		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
			TOTAL			TOTAL	2560		
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
			TOTAL ADD'L FEE				TOTAL ADD'L FEE		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
			TOTAL ADD'L FEE				TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of: David A. Redberg Serial No.: 14/094,484 Filed: December 2, 2013 Atty. File No.: FORT-011700 Entitled: "SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION"	Group Art Unit: 2161 Confirmation No.: 4264 Examiner: <u>RESPONSE TO THE NOTICE TO FILE CORRECTED PAPERS</u> Electronically Submitted
---	---

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notice to File Corrected Papers mailed December 19, 2013, in connection with the above-identified application, attached is a Replacement Drawing Sheet (Fig. 4A-C). Payment in the amount of \$140 is being submitted via EFS-Web concurrently with the filing of this paper.

Respectfully submitted,

Hamilton, DeSanctis & Cha LLP

By: /Michael A. DeSanctis/
Michael A. DeSanctis
Registration No. 39957
Customer No. 64128
(303) 856-7155

Date: December 22, 2013

Fig. 4B

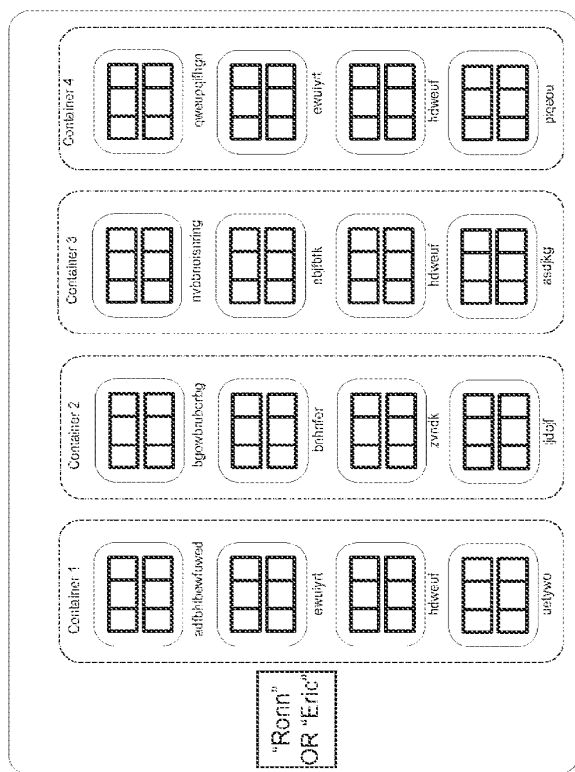
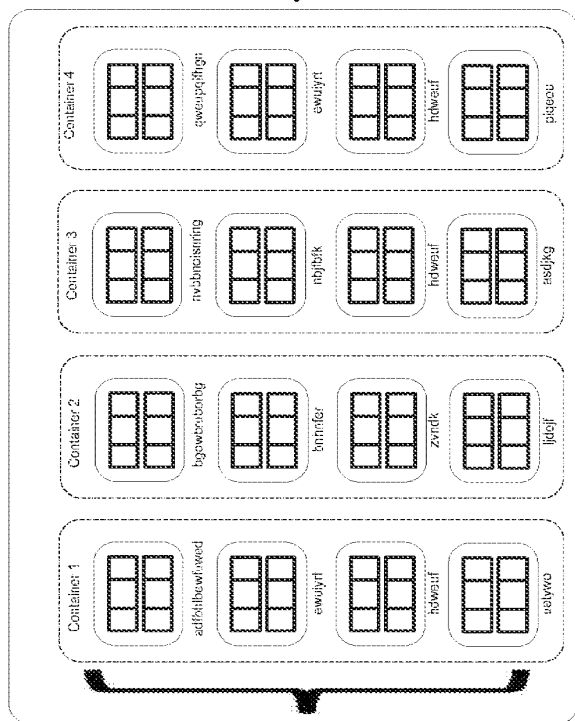


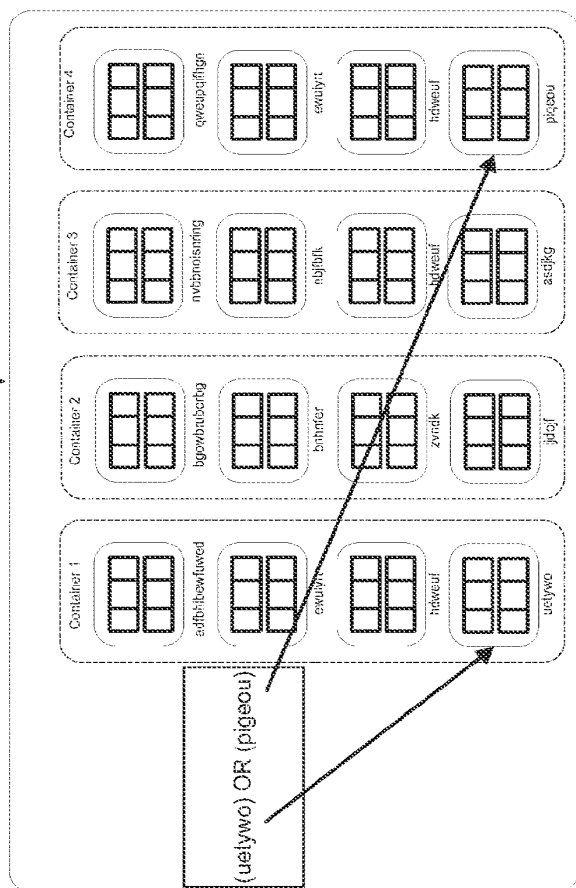
Fig. 4A

400



Searchable
Encryption
Data

Fig. 4C



Electronic Patent Application Fee Transmittal				
Application Number:		14094484		
Filing Date:		02-Dec-2013		
Title of Invention:		SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
First Named Inventor/Applicant Name:		David A. Redberg		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-011700		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	1051	1	140	140
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				140

Electronic Acknowledgement Receipt

EFS ID:	17806216
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	04-JAN-2014
Filing Date:	02-DEC-2013
Time Stamp:	13:10:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 140
RAM confirmation Number	6394
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Applicant Response to Pre-Exam Formalities Notice	Response_CorrectedPapers_11700.pdf	14087 d3a20e407fb645e62ef74aa4a565813f72d36b15	no	1
Warnings:					
Information:					
2	Drawings-only black and white line drawings	Replcaement_Fig4.pdf	537567 8d800fd24b3724d37781af014d4290579e73dd71	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	29917 3720b41e3380facaa034dfd0ccff70151f57c200	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			581571		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/094,484			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280		
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720		
TOTAL CLAIMS (37 CFR 1.16(i))	32 minus 20 =	*				x 80 =	960		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	2560		
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
				TOTAL ADD'L FEE			TOTAL ADD'L FEE		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
				TOTAL ADD'L FEE			TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
14/094,484	12/02/2013	2161	2700	FORT-011700	32	3

CONFIRMATION NO. 4264

UPDATED FILING RECEIPT



OC000000065921478

64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

Date Mailed: 01/09/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

David A. Redberg, Sunnyvale, CA;

Applicant(s)

Fortinet, Inc., Sunnyvale, CA

Assignment For Published Patent Application

Fortinet, Inc., Sunnyvale, CA

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 12/12/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/094,484**

Projected Publication Date: 06/04/2015

Non-Publication Request: No

Early Publication Request: No

page 1 of 3

Title

SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

Preliminary Class

707

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/094,484	12/02/2013	David A. Redberg	FORT-011700

CONFIRMATION NO. 4264

64128

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

NOTICE



Date Mailed: 01/09/2014

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
David A. Redberg



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/094,484	12/02/2013	David A. Redberg	FORT-011700

CONFIRMATION NO. 4264

PUBLICATION NOTICE



64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

Title: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

Publication No. US-2015-0154418-A1

Publication Date: 06/04/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	12/02/2013	David A. Redberg	FORT-011700	4264
64128 7590 06/15/2015 MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP FINANCIAL PLAZA AT UNION SQUARE 225 UNION BOULEVARD, SUITE 150 LAKEWOOD, CO 80228			EXAMINER LEWIS, LISA C	
			ART UNIT 2495	PAPER NUMBER
			NOTIFICATION DATE 06/15/2015	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesantis@hdciplaw.com
docket@hdciplaw.com

Office Action Summary	Application No. 14/094,484	Applicant(s) REDBERG, DAVID A.	
	Examiner Lisa Lewis	Art Unit 2495	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 12/02/2013.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2a) ☐ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☒ Claim(s) 1-32 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☐ Claim(s) ____ is/are rejected.

8) ☐ Claim(s) ____ is/are objected to.

9) ☒ Claim(s) 1-32 are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some** c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.

4) ☐ Other: ____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-3, drawn to a method comprising: providing a cloud storage device and an API, assigning a file storage policy, receiving a request to store a file, creating a searchable encrypted data corresponding to content or metadata, distributing the searchable encrypted data based on storage diversity requirements, classified in G06F21/6218, for example.

II. Claims 4-32, drawn to a method and system comprising: assigning a policy to one or more users, encrypted cryptographic key information, storing the encrypted information, and managing access to the file, classified in H04L9/08, for example.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I and II are directed to related processes. The related inventions are distinct if: (1) the inventions as claimed are either not capable of use together or can have a materially different design, mode of operation, function, or effect; (2) the inventions do not overlap in scope, i.e., are mutually exclusive; and (3) the inventions as claimed are not obvious variants. See MPEP § 806.05(j). In the instant case, the inventions as claimed have materially different mode of operation. For example, Invention I requires storage diversity requirements which are not required of Invention II, and Invention II requires cryptographic key information which is not required of Invention I. Furthermore, the inventions as claimed do not encompass overlapping subject matter and there is nothing of record to show them to be obvious variants.

Art Unit: 2495

3. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and/or examination burden if restriction were not required because one or more of the following reasons apply:

There would be a significant burden on the examiner to search both sets together.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of an invention to be examined even though the requirement may be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103 or pre-AIA 35 U.S.C. 103(a) of the other invention.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lisa Lewis whose telephone number is (571)270-7724. The examiner can normally be reached on Monday - Friday, 6:30 a.m. - 3:30 p.m.

Art Unit: 2495

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on (571) 272-3739. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Lisa Lewis/
Primary Examiner, Art Unit 2495

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:



Practitioners associated with Customer Number:

64128

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:



The address associated with Customer Number:

64128

OR

☐	Firm or Individual Name			
	Address			
	City	State	Zip	
	Country			
	Telephone	Email		

Assignee Name and Address: Fortinet, Inc.
899 Kifer Rd.
Sunnyvale, CA 94086

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date
Name	Todd A. Nelson	Telephone (408) 486-7803
Title	Vice President Legal	

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	22656282
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	17-JUN-2015
Filing Date:	02-DEC-2013
Time Stamp:	12:48:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	declaration.pdf	231141 f1a4983b86c5b6d32354f0fe7eb16c2930a87f2a	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73	statement.pdf	117342	no	3
			94431533ad6654ee5c9f69c1eb8e3556e42ade51		
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	Assignment.pdf	349531	no	2
			352866cfe48a4569b5d00f3a1b7a14e3b88f0c27		
Warnings:					
Information:					
4	Power of Attorney	Executed_POA_3_73_c_2.pdf	76400	no	1
			f4ad760f71d7becdc33b00b6c2c4b21776d380d1		
Warnings:					
Information:					
Total Files Size (in bytes):			774414		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)Title of
Invention**SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION**

As the below named inventor, I hereby declare that:

This declaration
is directed to:☐

The attached application, or

☒United States application or PCT international application number 14/094,484filed on December 2, 2013

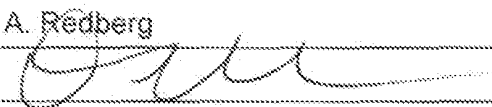
The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identify theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTORInventor: David A. RedbergDate (Optional) 6/16/2015Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 118 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-8199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)Applicant/Patent Owner: Fortinet, Inc.Application No./Patent No.: 14/094,484Filed/Issue Date: December 2, 2013Titled: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATIONFortinet, Inc., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Michael A DeSanctis/

June 17, 2015

Signature

Date

Michael A. DeSanctis/

39957

Printed or Typed Name

Title or Registration Number

[Page 2 of 2]

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ASSIGNMENT

WHEREAS, I, **David A. Redberg**, have invented certain new and useful improvements for which an application entitled

"SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION"

is about to be made for Letters Patent of the United States, the application having been executed on even date herewith, and which may be identified in the United States Patent and Trademark Office by Application No. 14/094,484, filed on December 2, 2013 and further identified as Atty. Docket No. FORT-0117000.

WHEREAS, **Fortinet, Inc.**, a Corporation of the State of Delaware, and having its principal offices at 899 Kifer Rd., Sunnyvale, CA 94086 (hereafter "Assignee"), is desirous of acquiring the entire right, title and interest in and to the application, any inventions or discoveries described therein and in, to and under any and all Letters Patents to be obtained therefor;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I have sold, assigned and transferred, and by these presents do hereby sell, assign and transfer unto the Assignee, its successors and assigns:

1. the entire right, title and interest in and to the application, any inventions or discoveries described therein and the Letters Patent(s), both foreign and domestic, that may or shall issue, including all rights under the International Convention, and
2. all proceeds of the application, any inventions or discoveries described therein and the Letters Patent(s) (including but not limited to, damages for pre-patent grant infringement, all license royalties and proceeds of infringement suits); and in and to any and all causes of action (excepting claims upon the United States of America) for past, present, and future infringement of any of the Letters Patent(s), or relating to any inventions or discoveries described therein, including the right to collect royalties and seek injunctive relief, for all such infringements and the right to sue on all such causes of action for their own use and benefit and the use and benefit of their successors, assigns and legal representatives,

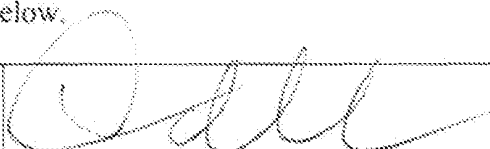
I do hereby authorize and request the Commissioner of Patents to issue the Letters Patent(s) to the Assignee in accordance herewith.

I further authorize the Assignee, its successors and assigns, or anyone it may properly designate, to apply for Letters Patent, in its own name, if desired, in any and all

foreign countries, and additionally to claim the filing date of the United States application and/or otherwise take advantage of the provisions of the International Convention.

I do hereby covenant and agree with the Assignee, its successors and assigns, that I will not execute any writing or do any act whatsoever conflicting with these presents, and that I or my executor(s) or administrator(s) will, at any time upon request, without further or additional consideration, but at the expense of the Assignee, its successors and assigns, execute such additional writings and do such additional acts as the Assignee, its successors and assigns, may deem necessary or desirable to perfect the Assignee's enjoyment of this grant, and render all necessary assistance in making application for and obtaining original, continuation, divisional, reissued, reexamined, substitute or extended Letters Patent(s) of the United States, or of any and all foreign countries on the invention, and in enforcing any rights, occurring as a result of such applications or patents, by giving testimony in any proceedings or transactions involving such applications or patents.

IN WITNESS WHEREOF, I have executed this Assignment on the date indicated below.

Signature:	
Date:	June 16, 2015
Full Name:	David A. Redberg
Address:	~~1050 Merrimac Dr.~~ 1969 E. 28 th St
	~~Sunnyvale, CA 94087~~ BROOKLYN, NY 11229
	UNITED STATES



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/094,484	12/02/2013	David A. Redberg	FORT-011700

CONFIRMATION NO. 4264

POA ACCEPTANCE LETTER



64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

Date Mailed: 06/23/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/17/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/sleutchit/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: Lewis, Lisa C.
Inventor: David A. Redberg	Group Art Unit: 2495
App. No.: 14/094,484	Conf. No.: 4264
Filed: December 2, 2013	Docket No.: FORT-011700
For: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO RESTRICTION REQUIREMENT

Sir:

Responsive to the Office action having a notification date of June 15, 2015 (the "Office Action"), the undersigned respectfully requests the Examiner to enter the following Amendment and to consider the following remarks:

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks begin on page 7 of this paper.

Amendment

Amendments to the Claims

Please cancel claims 1-3, without prejudice.

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

- 1-3. **(Cancelled)**
4. **(Original)** A method comprising:
 - assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms, wherein the policy defines access rights of the one or more users;
 - encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file;
 - storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and
 - managing access to the searchable encrypted file by the one or more users based on the policy.
5. **(Original)** The method of claim 4, wherein the step of managing comprises allowing the one or more users to download the searchable encrypted file to a local device.
6. **(Original)** The method of claim 5, wherein the local device comprises a mobile computing device.
7. **(Original)** The method of claim 5, wherein the downloaded encrypted file is searchable by the one or more users using the cryptographic key information.

8. **(Original)** The method of claim 4, wherein the step of encrypting further comprises:
 - dividing the file into a plurality of chunks;
 - creating namespaces for one or more of the plurality of chunks; and
 - configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.
9. **(Original)** The method of claim 8, wherein a set of chunks from the plurality of chunks is searchable.
10. **(Original)** The method of claim 8, wherein the step of configuring the namespaces comprises storing content of the file as filenames.
11. **(Original)** The method of claim 4, wherein the step of encrypting further comprises the step of randomly creating empty files.
12. **(Original)** The method of claim 4, wherein the step of encrypting the file is carried out independent of the service provider of the one or more cloud platforms.
13. **(Original)** The method of claim 4, wherein the policy is implemented for a group of users.
14. **(Original)** The method of claim 4, wherein the policy defines the manner in which the file is stored, accessed, and processed.
15. **(Original)** The method of claim 4, wherein the file is stored across two or more cloud platforms.
16. **(Original)** The method of claim 4, wherein said storing the searchable encrypted file on the one or more cloud platforms is carried out independent of the service provider of the one or more cloud platforms.

17. **(Original)** The method of claim 4, wherein the policy is selected from a plurality of policies stored in a database, wherein the database is operatively coupled with the gateway device.
18. **(Original)** The method of claim 4, wherein the policy defines one or more of a set of encryption keys, a set of decryption keys, search indices, a type of encryption and one or more authorized locations to which the file may be stored.
19. **(Original)** The method of claim 4, wherein said encrypting further comprises encrypting one or more of filename and search indices.
20. **(Original)** A secure cloud storage system comprising:
 - one or more processors;
 - a communication interface mechanism;
 - one or more internal data storage devices operatively coupled to the one or more processors and storing:
 - a policy assignment module configured to implement a policy selected from a group of policies for a user, wherein the policy defines and manages access to and processing of a file to be uploaded on a cloud, wherein the policy defines access rights of the user;
 - an encryption module configured to, using cryptographic key information defined by the policy, produce a searchable encrypted file by encrypting content of the file to be stored across one or more cloud platforms;
 - a storage module configured to store the searchable encrypted file on the one or more cloud platforms based on the policy; and
 - a management module configured to manage and control access to the searchable encrypted file by the user based on the policy.
21. **(Original)** The system of claim 20, wherein the management module is further configured to allow the user to download the searchable encrypted file to a local device.

22. **(Original)** The system of claim 21, wherein the downloaded encrypted file is searchable by the user using the cryptographic key information defined by the policy.
23. **(Original)** The system of claim 20, wherein the encryption module is further configured to:
 - divide the file into a plurality of chunks;
 - create namespaces for one or more of the plurality of chunks; and
 - configure the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.
24. **(Original)** The system of claim 23, wherein a set of chunks from the plurality of chunks is searchable.
25. **(Original)** The system of claim 23, wherein the encryption module is further configured to randomly create empty files.
26. **(Original)** The system of claim 20, wherein one or more of the policy assignment module, the encryption module, the storage module, and the management module are implemented on different devices, wherein the devices are selected from one or more of access management devices, proxy devices, gateway devices, and network controllers.
27. **(Original)** The system of claim 20, further comprising a mediation module configured to make implementation of one or more of the policy assignment module, the encryption module, the storage module, and the policy management module independent of the service provider of the one or more cloud platforms.
28. **(Original)** The system of claim 20, wherein the policy is implemented for a group of users.
29. **(Original)** The system of claim 20, wherein the policy defines the manner in which the file is stored and processed.

30. **(Original)** The system of claim 20, wherein the file is stored across two or more cloud storage platforms.
31. **(Original)** The system of claim 20, wherein the group of policies are stored in a database operatively coupled with the system.
32. **(Original)** The system of claim 20, wherein the policy defines and manages one or more of encryption keys, decryption keys, search indices, type of encryption, and location of the file.

REMARKS

The undersigned respectfully requests consideration of the above-captioned patent application in view of the above claim amendments and the following remarks. In this Amendment and Response, claims 1-3 have been cancelled, without prejudice. No claims have been amended or added. Hence, upon entry of this Amendment and Response, claims 4-32 are presented for examination. No new matter has been added by way of this Amendment.

Election/Restriction Requirement

In the Office Action, the Examiner indicated restriction to one of Group I (i.e., claims 1-3) and Group II (i.e., claims 4-32) was required under 35 U.S.C. § 121. The undersigned hereby elects without traverse the claims of Group II (i.e., claims 4-32) for examination. The claims directed to the non-elected Group I have been cancelled. Consequently, the undersigned respectfully requests the Examiner to promptly issue a substantive action regarding Group II.

Request for a Telephone Interview

If the Examiner believes a telephone conference would expedite prosecution of this patent application, please telephone the undersigned at 303-856-7155.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date: June 26, 2015

/Michael A DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 064128
Ph: (303) 856-7155

Electronic Acknowledgement Receipt

EFS ID:	22762354
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	26-JUN-2015
Filing Date:	02-DEC-2013
Time Stamp:	20:06:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Amendment_Response.pdf	97798 9e3ece2c968739b0b556bd97f69ab9cbb70d2c7	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	7
Warnings:			
Information:			
Total Files Size (in bytes):		97798	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.			



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	12/02/2013	David A. Redberg	FORT-011700	4264
64128 7590 08/07/2015 MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP FINANCIAL PLAZA AT UNION SQUARE 225 UNION BOULEVARD, SUITE 150 LAKEWOOD, CO 80228			EXAMINER LEWIS, LISA C	
			ART UNIT 2495	PAPER NUMBER
			NOTIFICATION DATE 08/07/2015	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesantis@hdciplaw.com
docket@hdciplaw.com

Office Action Summary	Application No. 14/094,484	Applicant(s) REDBERG, DAVID A.	
	Examiner Lisa Lewis	Art Unit 2495	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 06/26/2015.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☒ Claim(s) 4-32 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☒ Claim(s) 4-32 is/are rejected.

8) ☐ Claim(s) ____ is/are objected to.

9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some** c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.

4) ☐ Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of 35 U.S.C. 112(b):

(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 20-32 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

3. Claim limitation “module configured to” has been interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because it uses a generic placeholder “module” coupled with functional language without reciting sufficient structure to achieve the function. Furthermore, the generic placeholder is not preceded by a structural modifier. Since the claim limitation invokes 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, claims 20-32 has/have been interpreted to cover the corresponding structure described in the specification that achieves the claimed function, and equivalents thereof.

4. Claim element "module configured to" is a limitation that invokes 35 U.S.C. 112, sixth paragraph. However, the written description fails to clearly link or associate the disclosed structure, material, or acts to the claimed function such that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function. Applicant may:

a. Amend the claim so that the claim limitation will no longer be interpreted as a limitation under 35 U.S.C. 112, sixth paragraph; or

Art Unit: 2495

b. Amend the written description of the specification such that it clearly links or associates the corresponding structure, material, or acts to the claimed function without introducing any new matter (35 U.S.C. 132(a)); or

c. State on the record where the corresponding structure, material, or acts are set forth in the written description of the specification and linked or associated to the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181.

5. If applicant wishes to provide further explanation or dispute the examiner's interpretation of the corresponding structure, applicant must identify the corresponding structure with reference to the specification by page and line number, and to the drawing, if any, by reference characters in response to this Office action.

6. If applicant does not intend to have the claim limitation(s) treated under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, applicant may amend the claim(s) so that it/they will clearly not invoke 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, or present a sufficient showing that the claim recites/recite sufficient structure, material, or acts for performing the claimed function to preclude application of 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

For more information, see MPEP § 2173 et seq. and Supplementary Examination Guidelines for Determining Compliance With 35 U.S.C. 112 and for Treatment of Related Issues in Patent Applications, 76 FR 7162, 7167 (Feb. 9, 2011).

Election/Restrictions

Applicant's election without traverse of Group II, claims 4-32, in the reply filed on 06/26/2015 is acknowledged.

Claim Rejections - 35 USC § 103

1. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

2. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 4, 12-20, and 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Prahlad et al. (US 2010/0332401) in view of Guaralnik et al. (US 2013/0207775).**

4. Regarding claims 4 and 20, Prahlad teaches a method comprising:

a. Assigning to one or more users, by a gateway device (internal data storage device), a policy for managing access to and processing a file to be stored on one or more cloud platforms, wherein the policy defines access rights of the one or more users (Cloud gateway may apply storage policies to determine to which cloud storage site the cloud gateway should migrate the data. Users/applications may dictate to the cloud gateway the handling of their content, such as if it should be encrypted (processed) (thus suggesting that the gateway encrypts the data). Cloud gateway may permit data replication on demand to selected geographies based on access usage patterns) - see [0284] and [0272].

Art Unit: 2495

b. Encrypting, by the gateway device, using cryptographic key information defined in the policy, content of the file to produce a searchable encrypted file (Users/applications may dictate, under the storage policy, to the cloud gateway the handling of their content, such as if it should be encrypted and searchable (thus suggesting that the gateway may produce a searchable encrypted file). Data is encrypted with a key) - see [0284] and [0272] and [0122].

c. Storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy (Cloud gateway may apply storage policies to determine to which cloud storage site the cloud gateway should migrate the data) - see [0284].

d. Managing access to the searchable encrypted file by the one or more users based on the policy (Cloud gateway may permit data replication on demand to selected geographies based on access usage patterns and this is under the storage policy) – see [0272].

5. Please note that if Prahlad does not *explicitly* teach that the key is in the policy, for example, although the encryption is handled via the policy by the gateway), the differences between that which is disclosed and that which is claimed are considered to be so slight that that it would have been obvious to the skilled artisan to modify the teachings of Prahlad in order to create the claimed invention.

6. Further, Prahlad suggests that the policy is used to manage access for users (see above), but does not explicitly disclose the “assigning” of policies for users regarding access.

7. Guarlnik teaches a method wherein access policies are assigned for users and access is granted or denied to the user based on that policy - see [0006].

8. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to modify the teachings of Prahlad to specifically assign access policies to users, for the purpose of added security, based upon the beneficial teachings provided by Guarlnik. This would make the system more secure. Both Prahlad and Guarlnik are in the field of computer security and therefore, are in analogous arts.

9. Regarding claim 12, Prahlad teaches that the encrypting of the file is carried out independent of the service provider of the one or more cloud platforms (performed by gateway) - see [0272].
10. Regarding claims 13 and 28, Guarlnik teaches that the policy is implemented for a group of users – see [0007].
11. Regarding claims 14 and 29, Prahlad teaches that the policy defines the manner in which the file is stored, accessed, and processed - see [00272] and [0284].
12. Regarding claims 15 and 30, Prahlad teaches that the file may be stored across two or more cloud platforms (file may be transferred or copied to one more secondary cloud storage sites) - see [0359] and figure 1.
13. Regarding claim 16, Prahlad teaches that storing the searchable encrypted file on the one or more cloud platforms is carried out independent of the service provider of the one or more cloud platforms (gateway performs storage) - see [0272] and [0284].
14. Regarding claims 17 and 31, Prahlad teaches that the policy is selected from a policy of policies stored in a database, wherein the database is operatively coupled with the gateway device – see [0075] and [0284].

Art Unit: 2495

15. Regarding claims 18 and 32, Prahlad teaches that the policy defines one or more of a set of encryption keys, a set of decryption keys, search indices, a type of encryption, and one or more authorized locations to which the file may be stored – see [0272] and [0284].

16. Regarding claim 19, Prahlad teaches that encrypting further comprises encrypting one or more of filename and search indices (parameters are specified such as if its encrypted, indexed, searchable, etc. and therefore, it is suggested that a user/application could specify encrypted index) - see [0272].

17. Regarding claim 26, Prahlad teaches that the functions of the modules are performed on the gateway device (see rejection for claim 20). Prahlad does not teach that these are implemented on different devices. However, MPEP 2144.04 states that making parts separable is an indication of obviousness. It would be obvious to implement the modules on separate gateway devices since it does not affect the function of the modules.

18. Regarding claim 27, Prahlad teaches that the encryption module and storage module are independent of the service provider of the one or more cloud platforms – see [0272] and [0284].

19. Claims 5, 6, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Prahlad et al. (US 2010/0332401) in view of Guaralnik et al. (US 2013/0207775), and further in view of Haeger et al. (US 2014/0122866).

20. The teachings of Prahlad and Guaralnik are relied upon for the reasons set forth above.

21. Regarding claims 5, 6, and 21, Prahlad and Guaralnik do not teach allowing the one or more users to download the searchable encrypted file to a local device (mobile).

Art Unit: 2495

22. Haeger teaches that in cloud systems, the user downloads the encrypted file from the cloud storage server and can decrypt the file using the same secret key at his/her computing device (which can be a phone) - see [0001] and [0002], for example.

23. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to modify the teachings of Prahlad and Guarlnik to download the encrypted file (which Prahlad teaches is searchable) to a local device, based upon the beneficial teachings provided by Haeger, as this is the typical way cloud computing systems are structured.

24. Claims 7 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Prahlad et al. (US 2010/0332401) in view of Guarlnik et al. (US 2013/0207775), and further in view of Aissi et al. (US 2014/0052999).

25. The teachings of Prahlad and Guarlnik are relied upon for the reasons set forth above.

26. Regarding claims 7 and 22, Prahlad and Guarlnik do not teach that the file is searchable using cryptographic key information.

27. Aissi teaches that clients are given access to searchable encrypted database by providing the clients with the database decryption key – see [0031], for example.

28. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to modify the teachings of Prahlad and Guarlnik by making the file searchable via cryptographic key, based upon the beneficial teachings provided by Aissi, in order to provide easy and secure access to the encrypted searchable file.

Allowable Subject Matter

Claims 8-11 and 23-25 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lisa Lewis whose telephone number is (571)270-7724. The examiner can normally be reached on Monday - Friday, 6:30 a.m. - 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on (571) 272-3739. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Lisa Lewis/
Primary Examiner, Art Unit 2495

Notice of References Cited	Application/Control No. 14/094,484	Applicant(s)/Patent Under Reexamination REDBERG, DAVID A.	
	Examiner Lisa Lewis	Art Unit 2495	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2010/0332401 A1	12-2010	Prahlad et al.	705/80
*	B	US-2013/0133023 A1	05-2013	BURSTEIN et al.	726/1
*	C	US-2013/0207775 A1	08-2013	Guralnik et al.	340/5.21
*	D	US-2014/0052999 A1	02-2014	Aissi et al.	713/189
*	E	US-2014/0122866 A1	05-2014	Haeger et al.	713/153
*	F	US-2014/0136675 A1	05-2014	Yao et al.	709/223
*	G	US-8,819,768 B1	08-2014	Koeten et al.	726/1
*	H	US-2015/0046971 A1	02-2015	Huh et al.	726/1
*	I	US-2015/0074398 A1	03-2015	Cullen et al.	713/168
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4264

SERIAL NUMBER 14/094,484	FILING or 371(c) DATE 12/02/2013 RULE	CLASS 713	GROUP ART UNIT 2495	ATTORNEY DOCKET NO. FORT-011700		
APPLICANTS Fortinet, Inc., Sunnyvale, CA; INVENTORS David A. Redberg, Sunnyvale, CA; ** CONTINUING DATA ***** ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 12/12/2013						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☐ No Verified and /LISA C LEWIS/ Acknowledged Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY CA	SHEETS DRAWINGS 12	TOTAL CLAIMS 32	INDEPENDENT CLAIMS 3
ADDRESS MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP FINANCIAL PLAZA AT UNION SQUARE 225 UNION BOULEVARD, SUITE 150 LAKEWOOD, CO 80228 UNITED STATES						
TITLE SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION						
FILING FEE RECEIVED 2700	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees		
				☐ 1.16 Fees (Filing)		
				☐ 1.17 Fees (Processing Ext. of time)		
				☐ 1.18 Fees (Issue)		
				☐ Other _____		
				☐ Credit		

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	22	download\$4 near4 (data or information or file or content) and (data or information or file or content) near5 searchable near5 encrypted	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 08:28
L3	376	cloud with download\$4 near4 file near9 (user or device or local\$4 or mobile or phone)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 08:37
L4	25	cloud with download\$4 near4 file near9 (user or device or local\$4 or mobile or phone) with encrypted	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 08:37
L5	54	encrypted near9 searchable near9 key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 08:44
L6	1	(encrypted near9 searchable).ab,ti. and (chunk or portion or segment or section) near9 (namespace or name space or filename or file name)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:01
L7	23	(encrypted near9 searchable) and (chunk or portion or segment or section) near9 (namespace or name space or filename or file name)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:01
L8	36	(encrypted near9 searchable) and (chunk or portion or segment or section or block) with name	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:39
L9	1	(encrypted near9 searchable) same (chunk or portion or segment or section or block) with name	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:40
L10	34	(encrypted near9 searchable) same (chunk or portion or segment or section or block)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:40
L13	54	(encrypted near9 searchable)with index	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:45

L14	5	(encrypted near9 searchable)with index same (block or section or portion or chunk or divid\$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:46
L15	30	empty file near9 encrypt\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 09:56
L17	55	group access policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 10:01
L18	3	"20140052999"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 10:35
L19	1297	(G06F21/6218).cpc. and cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 10:39
L20	317	(G06F21/6218).cpc. and cloud and gateway	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 10:39
L21	750	((Redberg and david).in. or (fortinet).as.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 10:40
L22	1	((Redberg and david).in. or (fortinet).as.) and cloud and searchable	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/03 10:40
S1	26	gateway with policy with cloud with encrypt\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/21 08:28
S2	41	searchable encrypted	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/21 08:48
S3	14	searchable encrypted same cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/21 08:48
S4	27	searchable encrypted not S3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/21 08:49

S5	42	gateway with policy with cloud with access\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 09:47
S6	23	gateway with policy with cloud same gateway near9 stor\$4 near9 cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 09:50
S7	22	gateway near9 policy near9 cloud same gateway near9 stor\$4 near9 cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 09:50
S9	1	gateway with cloud with assign\$4 with access near4 policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:37
S10	1	gateway with cloud with assign\$4 policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:37
S11	2	police\$4 near9 user near9 assign\$4 with access\$4 with cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:38
S12	684	police\$4 near9 user near9 assign\$4 with access\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:39
S13	349	police\$4 near3 user near9 assign\$4 with access\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:39
S15	154	police\$4 near3 user near3 assign\$4 with access\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:39
S16	101	police\$4 near3 user near3 assign\$4 near9 access\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:40
S17	16	police\$4 near3 user near3 assign\$4 near9 access\$4 and cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/07/30 10:40

EAST Search History (I nterference)

< This search history is empty >

8/ 3/ 2015 10:40:43 AM

C:\ Users\ llewis1\ Documents\ EAST\ Workspaces\ 14094484.wsp

Search Notes 	Application/Control No. 14094484	Applicant(s)/Patent Under Reexamination REDBERG, DAVID A.
	Examiner LISA LEWIS	Art Unit 2495

CPC- SEARCHED		
Symbol	Date	Examiner
(G06F21/6218).cpc.	8/3/2015	LL

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Searched EAST	8/3/2015	LL
Searched NPL	8/3/2015	LL
DP Search	8/3/2015	LL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/LISA LEWIS/ Primary Examiner.Art Unit 2495
--	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14094484	
	Filing Date		2013-12-02	
	First Named Inventor	David A. Redberg		
	Art Unit	2495		
	Examiner Name			
	Attorney Docket Number	FORT-011700		

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		14094484
Filing Date		2013-12-02
First Named Inventor	David A. Redberg	
Art Unit	2495	
Examiner Name		
Attorney Docket Number	FORT-011700	

1	AlephCloud. FAQ. http://www.alephcloud.com/#faq/c1pya . 2 pgs.	☐
2	AlephCloud. "AlephCloud Raises \$7.5M Series B for New Approach to Cloud Content Privacy Management." http://www.alephcloud.com/#lpr-20130522/cbri . 2 pgs.	☐
3	AlephCloud. "Content Canopy." http://www.alephcloud.com/#products/cife . 1 pg.	☐
4	AlephCloud. "It's the Content, not the Container." http://www.alephcloud.com/#solution/c15sb . 1 pg.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	14094484
Filing Date	2013-12-02
First Named Inventor	David A. Redberg
Art Unit	2495
Examiner Name	
Attorney Docket Number	FORT-011700

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael A. DeSanctis/	Date (YYYY-MM-DD)	2015-08-28
Name/Print	Michael A. DeSanctis	Registration Number	39957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:		14094484		
Filing Date:		02-Dec-2013		
Title of Invention:		SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
First Named Inventor/Applicant Name:		David A. Redberg		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-011700		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	23346944
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	01-SEP-2015
Filing Date:	02-DEC-2013
Time Stamp:	12:42:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$180
RAM confirmation Number	10172
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_11700.pdf	612476	no	4
			5be75dc166e57f98f1bd9ef52faac271624acd7e		
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	NPL_11700_1.pdf	90586	no	2
			01e01fb8720e315bab877235204e83a93f363ce6		
Warnings:					
Information:					
3	Non Patent Literature	NPL_11700_2.pdf	57004	no	2
			bafba91a4b882a39528b085b6360258db754fda3		
Warnings:					
Information:					
4	Non Patent Literature	NPL_11700_3.pdf	224013	no	1
			465a904a2a20bc079c91f22aa0c8efd48c2a7155		
Warnings:					
Information:					
5	Non Patent Literature	NPL_11700_4.pdf	130738	no	1
			9422dea714ec22ab9c9d611652e0541dd21c26e0		
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	30472	no	2
			aa9ab4fd568b122812dcac0b2e4d07f37976fb01		
Warnings:					
Information:					
Total Files Size (in bytes):			1145289		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: Lewis, Lisa C.
Inventor: David A. Redberg	Group Art Unit: 2495
App. No.: 14/094,484	Conf. No.: 4264
Filed: December 2, 2013	Docket No.: FORT-011700
For: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir/Madam:

Responsive to the Office action having a notification date of August 7, 2015 (the “Office Action”), the undersigned respectfully requests the Examiner to enter the following Amendment and to consider the following remarks:

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks begin on page 7 of this paper.

Amendment

Amendments to the Claims

Please cancel claims 8 and 23, without prejudice.

Please amend claims 4, 9, 10, 20, 21, 24, 25 and 27.

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1-3. **(Cancelled)**

4. **(Currently Amended)** A method comprising:

assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms, wherein the policy defines access rights of the one or more users;

encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file
by:[;]

dividing the file into a plurality of chunks;

creating namespaces for one or more of the plurality of chunks; and

configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable;

storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and

managing access to the searchable encrypted file by the one or more users based on the policy.

5. **(Original)** The method of claim 4, wherein the step of managing comprises allowing the one or more users to download the searchable encrypted file to a local device.
6. **(Original)** The method of claim 5, wherein the local device comprises a mobile computing device.
7. **(Original)** The method of claim 5, wherein the downloaded encrypted file is searchable by the one or more users using the cryptographic key information.
8. **(Cancelled)**
9. **(Currently Amended)** The method of claim [[8]] 1, wherein a set of chunks from the plurality of chunks is searchable.
10. **(Currently Amended)** The method of claim [[8]] 1, wherein the step of configuring the namespaces comprises storing content of the file as filenames.
11. **(Original)** The method of claim 4, wherein the step of encrypting further comprises the step of randomly creating empty files.
12. **(Original)** The method of claim 4, wherein the step of encrypting the file is carried out independent of the service provider of the one or more cloud platforms.
13. **(Original)** The method of claim 4, wherein the policy is implemented for a group of users.
14. **(Original)** The method of claim 4, wherein the policy defines the manner in which the file is stored, accessed, and processed.
15. **(Original)** The method of claim 4, wherein the file is stored across two or more cloud platforms.

16. **(Original)** The method of claim 4, wherein said storing the searchable encrypted file on the one or more cloud platforms is carried out independent of the service provider of the one or more cloud platforms.
17. **(Original)** The method of claim 4, wherein the policy is selected from a plurality of policies stored in a database, wherein the database is operatively coupled with the gateway device.
18. **(Original)** The method of claim 4, wherein the policy defines one or more of a set of encryption keys, a set of decryption keys, search indices, a type of encryption and one or more authorized locations to which the file may be stored.
19. **(Original)** The method of claim 4, wherein said encrypting further comprises encrypting one or more of filename and search indices.
20. **(Currently Amended)** A secure cloud storage system comprising:
 - one or more processors;
 - a communication interface mechanism;
 - one or more internal data storage devices operatively coupled to the one or more processors and storing:
 - a policy assignment module, **which, when executed by the one or more processors, configured to implement implements** a policy selected from a group of policies for a user, wherein the policy defines and manages access to and processing of a file to be uploaded on a cloud, wherein the policy defines access rights of the user;
 - an encryption module, **which, when executed by the one or more processors: configured to,**
 - using cryptographic key information defined by the policy, **produce produces** a searchable encrypted file by encrypting content of the file to be stored across one or more cloud platforms;
 - divides the file into a plurality of chunks;**

creates namespaces for one or more of the plurality of
chunks; and
configures the namespaces of the one or more chunks
such that content of the file is encrypted in a manner that
makes it searchable;

a storage module, which, when executed by the one or more
processors, ~~configured to store~~ stores the searchable encrypted file on
the one or more cloud platforms based on the policy; and

a management module, which, when executed by the one or
more processors ~~configured to manage~~ manages and ~~control~~ controls
access to the searchable encrypted file by the user based on the policy.

21. **(Currently Amended)** The system of claim 20, wherein the management module
[[is]] further ~~configured to allow~~ allows the user to download the searchable
encrypted file to a local device.
22. **(Original)** The system of claim 21, wherein the downloaded encrypted file is
searchable by the user using the cryptographic key information defined by the
policy.
23. **(Cancelled)**
24. **(Currently Amended)** The system of claim [[23]] 20, wherein a set of chunks
from the plurality of chunks is searchable.
25. **(Currently Amended)** The system of claim [[23]] 20, wherein the encryption
module [[is]] further ~~configured to~~ randomly ~~create~~ creates empty files.
26. **(Original)** The system of claim 20, wherein one or more of the policy
assignment module, the encryption module, the storage module, and the
management module are implemented on different devices, wherein the devices
are selected from one or more of access management devices, proxy devices,
gateway devices, and network controllers.

27. **(Currently Amended)** The system of claim 20, further comprising a mediation module, which, when executed by the one or more processors ~~configured to make~~ makes implementation of one or more of the policy assignment module, the encryption module, the storage module, and the policy management module independent of the service provider of the one or more cloud platforms.
28. **(Original)** The system of claim 20, wherein the policy is implemented for a group of users.
29. **(Original)** The system of claim 20, wherein the policy defines the manner in which the file is stored and processed.
30. **(Original)** The system of claim 20, wherein the file is stored across two or more cloud storage platforms.
31. **(Original)** The system of claim 20, wherein the group of policies are stored in a database operatively coupled with the system.
32. **(Original)** The system of claim 20, wherein the policy defines and manages one or more of encryption keys, decryption keys, search indices, type of encryption, and location of the file.

REMARKS

The undersigned notes with appreciation the Examiner's indication that claims 8-11 and 23-25 would be allowable if rewritten in independent form and to overcome the 112 rejections. The undersigned proposes herein amendments to conform the claims to the form indicated to be allowable.

The undersigned respectfully requests consideration of the above-captioned patent application in view of the above claim amendments and the following remarks. In this Amendment and Response, claims 8 and 23 have been cancelled, without prejudice, claims 4, 9, 10, 20, 21, 24, 25 and 27 have been amended and no new claims have been added. Hence, upon entry of this Amendment and Response, claims 4-7, 9-22 and 24-32 are presented for reconsideration. No new matter has been added by way of this Amendment.

Claim Rejections – 35 U.S.C. § 112

In the Office action, the Examiner rejected claims 20-32 under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AIA), second paragraph, for allegedly being indefinite. The undersigned proposes herein amendments to claims 20, 21, 25 and 27 to remove the “configured to” language so that the claim limitations at issue will no longer be interpreted under 35 U.S.C. §112(f) or 35 U.S.C. §112 (pre-AIA), sixth paragraph.

Claim Rejections – 35 U.S.C. § 103
Prahlad and Guaralnik

In the Office action, the Examiner rejected claims 4, 12-20 and 26-32 under 35 U.S.C. §103(a) for allegedly being unpatentable over US Pub. No. 2010/0332401 of Prahlad et al. (hereafter “**Prahlad**”) in view of US Pub. No. 2013/0207775 of Guaralnik et al. (hereafter “**Guaralnik**”). For the sake of expediting issuance of the above-referenced patent application, the undersigned proposes amendments to the claims to put them in the form indicated to be allowable by the Examiner. However, the undersigned is not in agreement with the Examiner's reasons

for rejection and reserves the right to pursue claims of breadth similar to that of the former claims (prior to this amendment) in one or more continuation applications.

Claim Rejections – 35 U.S.C. § 103
Prahlad, Guarnik and Aissi

In the Office action, the Examiner rejected claims 7 and 22 under 35 U.S.C. §103(a) for allegedly being unpatentable over Prahlad in view of Guarnik and further in view of US Pub. No. 2014/0052999 of Aissi et al. For the sake of expediting issuance of the above-referenced patent application, the undersigned proposes amendments to the claims to put them in the form indicated to be allowable by the Examiner. However, the undersigned is not in agreement with the Examiner's reasons for rejection and reserves the right to pursue claims of breadth similar to that of the former claims (prior to this amendment) in one or more continuation applications.

Conclusion

The undersigned respectfully submits that the amendments and remarks presented herein have overcome the rejections, and that the pending claims are in condition for allowance. Accordingly, the undersigned requests that the rejections be withdrawn and that a Notice of Allowance be promptly issued for claims 4-7, 9-22 and 24-32.

Request for a Telephone Interview

If the Examiner believes a telephone conference would expedite allowance of this patent application, please telephone the undersigned at 303-856-7155.

Appl. No. 14/094,484
Amdt. Dated October 21, 2015
Reply to Office Action of August 7, 2015

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date: October 21, 2015

By: /Michael A DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 064128
Ph: (303) 856-7155

Electronic Acknowledgement Receipt

EFS ID:	23855614
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	21-OCT-2015
Filing Date:	02-DEC-2013
Time Stamp:	19:17:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Amendment_Response_2.pdf	107658 db6509fa94054642f5f81e6eb6a2ae097502 2016	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	9
Warnings:			
Information:			
Total Files Size (in bytes):		107658	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.			



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

64128 7590 01/29/2016
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

EXAMINER

LEWIS, LISA C

ART UNIT

PAPER NUMBER

2495

DATE MAILED: 01/29/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	12/02/2013	David A. Redberg	FORT-011700	4264
TITLE OF INVENTION: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION				

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	04/29/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

64128 7590 01/29/2016
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	12/02/2013	David A. Redberg	FORT-011700	4264

TITLE OF INVENTION: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	04/29/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEWIS, LISA C	2495	713-165000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	12/02/2013	David A. Redberg	FORT-011700	4264
64128 7590 01/29/2016 MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP FINANCIAL PLAZA AT UNION SQUARE 225 UNION BOULEVARD, SUITE 150 LAKEWOOD, CO 80228			EXAMINER LEWIS, LISA C	
			ART UNIT 2495	PAPER NUMBER
DATE MAILED: 01/29/2016				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

<i>Notice Requiring Inventor's Oath or Declaration</i>	Application No. 14/094,484	Applicant(s) David A. Redberg	
	Examiner LEWIS, LISA C	Art Unit 2495	

This notice is an attachment to the Notice of Allowability (PTOL-37), or the Notice of Allowability For A Design Application (PTOL-37D).

An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor has not yet been submitted.

An oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each inventor (for any inventor for which a compliant oath, declaration, or substitute statement has not yet been submitted) **MUST** be filed no later than the date on which the issue fee is paid. See 35 U.S.C. 115(f). Failure to timely comply will result in ABANDONMENT of this application.

A properly executed inventor's oath to declaration has not been received for the following inventor(s):

If applicant previously filed one or more oaths, declarations, or substitute statements, applicant may have received an informational notice regarding deficiencies therein.

The following deficiencies are noted:

INFORMAL ACTION PROBLEMS

- A properly executed inventor's oath or declaration has not been received for the following inventor(s): **David A. Redberg**.

Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

Questions relating to this Notice should be directed to the Application Assistance Unit at 571-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/094,484	Applicant(s) REDBERG, DAVID A.	
	Examiner Lisa Lewis	Art Unit 2495	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the response filed 10/21/2015.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 4-7,9-22 and 24-32. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|--|
| <ol style="list-style-type: none"> 1. ☐ Notice of References Cited (PTO-892) 2. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material 4. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____ | <ol style="list-style-type: none"> 5. ☒ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____ |
|--|--|

/Lisa Lewis/
Primary Examiner, Art Unit 2495

DETAILED ACTION

Allowable Subject Matter

Claims 4-7, 9-22, and 24-32 are allowed.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

IN THE CLAIMS:

In claims 9 and 10, the number "1" has been deleted and replaced with the number -4--.

Reasons for Allowance

This communication warrants No Examiner's Reason for Allowance, applicant's reply make evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule 37 CFR 1.104(e). Specifically, applicant's arguments filed on 10/21/2015 are persuasive, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lisa Lewis whose telephone number is (571) 270-7724. The examiner can normally be reached on Monday - Friday, 6:30 a.m. - 3:30 p.m.

Art Unit: 2495

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on (571) 272-3739. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Lisa Lewis/

Primary Examiner, Art Unit 2495

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number		14094484
Filing Date		2013-12-02
First Named Inventor	David A. Redberg	
Art Unit	2495	
Examiner Name		
Attorney Docket Number	FORT-011700	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		14094484
Filing Date		2013-12-02
First Named Inventor	David A. Redberg	
Art Unit	2495	
Examiner Name		
Attorney Docket Number	FORT-011700	

1	AlephCloud. FAQ. http://www.alephcloud.com/#faq/c1pya . 2 pgs.	☐
2	AlephCloud. "AlephCloud Raises \$7.5M Series B for New Approach to Cloud Content Privacy Management." http://www.alephcloud.com/#pr-20130522/cbri . 2 pgs.	☐
3	AlephCloud. "Content Canopy." http://www.alephcloud.com/#products/cife . 1 pg.	☐
4	AlephCloud. "It's the Content, not the Container." http://www.alephcloud.com/#solution/c15sb . 1 pg.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/LISA C LEWIS/	Date Considered	01/19/2016
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	14094484
Filing Date	2013-12-02
First Named Inventor	David A. Redberg
Art Unit	2495
Examiner Name	
Attorney Docket Number	FORT-011700

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael A. DeSanctis/	Date (YYYY-MM-DD)	2015-08-28
Name/Print	Michael A. DeSanctis	Registration Number	39957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	7	(encrypted near9 searchable)with index same (block or section or portion or chunk or divid\$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/01/19 08:23
L2	61	encrypted near9 searchable near9 key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/01/19 08:23
L3	37	(encrypted near9 searchable) same (chunk or portion or segment or section or block)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/01/19 08:24
L4	33	gateway with policy with cloud with encrypt\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/01/19 08:24

EAST Search History (Interference)

< This search history is empty >

1/ 19/ 2016 8:24:16 AM**C:\ Users\ llewis1\ Documents\ EAST\ Workspaces\ 14094484.wsp**

Issue Classification 	Application/Control No. 14094484	Applicant(s)/Patent Under Reexamination REDBERG, DAVID A.
	Examiner LISA LEWIS	Art Unit 2495

CPC						
Symbol					Type	Version
G06F		21		6218	F	2013-01-01
G06F		21		60	I	2013-01-01
G06F		17		30106	I	2013-01-01
G06F		17		30194	I	2013-01-01
G06F		21		602	I	2013-01-01
H04L		63		20	I	2013-01-01
G06F		21		6227	I	2013-01-01
H04L		63		06	I	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 27	
/LISA LEWIS/ Primary Examiner.Art Unit 2495 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 4	O.G. Print Figure 3A

Issue Classification 	Application/Control No. 14094484	Applicant(s)/Patent Under Reexamination REDBERG, DAVID A.
	Examiner LISA LEWIS	Art Unit 2495

[illegible]

NONE		Total Claims Allowed:	
		27	
(Assistant Examiner)	(Date)		
/LISA LEWIS/ Primary Examiner.Art Unit 2495	01/19/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	4	3A

Search Notes 	Application/Control No. 14094484	Applicant(s)/Patent Under Reexamination REDBERG, DAVID A.
	Examiner LISA LEWIS	Art Unit 2495

CPC- SEARCHED		
Symbol	Date	Examiner
(G06F21/6218).cpc.	8/3/2015	LL

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Searched EAST	8/3/2015	LL
Searched NPL	8/3/2015	LL
DP Search	8/3/2015	LL
Search updated	1/19/2016	LL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	General interference Search	1/19/2016	LL

	/LISA LEWIS/ Primary Examiner.Art Unit 2495
--	--

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

64128 7500 01/29/2016

MICHAEL A DESANCTIS
 HAMILTON DESANCTIS & CHA LLP
 FINANCIAL PLAZA AT UNION SQUARE
 225 UNION BOULEVARD, SUITE 150
 LAKEWOOD, CO 80228

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	12/02/2013	David A. Redberg	PORT-011700	4264

TITLE OF INVENTION: SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION

APPL. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	04/29/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEWIS, LISA C	2495	713-165000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Hamilton, DeSanctis & Cha LLP

2.

3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Fortinet, Inc.

(B) RESIDENCE (CITY AND STATE OR COUNTRY)

Sunnyvale, CA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

☐ A check is enclosed.

☒ Payment by credit card. Form PTO-2028 is attached. (via EFS-Web)

☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Michael A DeSanctis/

Date January 29, 2016

Typed or printed name Michael A. DeSanctis

Registration No. 39957

Electronic Patent Application Fee Transmittal				
Application Number:		14094484		
Filing Date:		02-Dec-2013		
Title of Invention:		SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION		
First Named Inventor/Applicant Name:		David A. Redberg		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-011700		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				960

Electronic Acknowledgement Receipt

EFS ID:	24772254
Application Number:	14094484
International Application Number:	
Confirmation Number:	4264
Title of Invention:	SECURE CLOUD STORAGE DISTRIBUTION AND AGGREGATION
First Named Inventor/Applicant Name:	David A. Redberg
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-011700
Receipt Date:	29-JAN-2016
Filing Date:	02-DEC-2013
Time Stamp:	18:00:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$960
RAM confirmation Number	5008
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	issue_fee.pdf	292150 6b360ec5bd1b7085fa2860c8bc4745cc7a9ca095	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30505 7afded2c6ea5a1d2106ddc2a9ddd29df96324ce9	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			322655		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. New Applications Under 35 U.S.C. 111 If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/094,484	03/08/2016	9280678	FORT-011700	4264

64128 7590 02/17/2016

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 133 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Fortinet, Inc., Sunnyvale, CA;
David A. Redberg, Sunnyvale, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.