Digital Safe

(Subject to Changes)

U.S. Patent 8,140,847 B1

Inventor: Jianqing Wu, Ph.D.

A. Introduction

1. Basics About the Patent:

Title of Invention: Digital Safe

Patent No 8,140,847. Application No: 12/233,575

Priority Date: September 28, 2007

Granted: March 20, 2012 Patent Term Extension: 608 days

Patent Owner: Jianqing Wu

Encumbrance: no. Assignment No.

2. The Main concept:

The core concept is a system and method that allows a user to provide his or her own encryption key(s) to encrypt the file on the server and then save the file in the encrypted from (ciphertext) on the server. This concept is very obvious now, but it was contrary to teaching and culture in 2007. This represented a complete change of a storage model from dominant “trusted system” to one there is no trusted relationship between the user and the server.

In order to embody this concept, an encryption key must be sent to the server where file encryption is performed. The key is deleted (e.g., discarded) by a program or an equivalent system action so long it is not saved. The invention must have two features: the user can provide his own individual encryption key(s) to encrypt file, and encryption is performed on the server.

3. Highly preferred features:

This invention discloses a lot of related features:

(1) A great need to accept a hint for each encrypted key (without it, the system would have a huge risk).

(2) There is a need to verify an encrypted file. Since the user wants to encrypt a file using his own key, the file must be important. There is no tolerance for file structure damages. Second, it is necessary to find human errors in entering encryption key and detect network errors causing file corruption.

(3) A feature for sharing highly confidential files between account holders;

(4) A feature of using “link” to share confidential files with individuals who does not use a safe account;

(5) A feature for tracking access histories for individual stored confidential file;

(6) A feature for controlling access by using different methods;

(7) A feature for issuing a certification to prove the substance of the file (the encrypted file cannot be tempered by anyone, so the true content of each encrypted file can be verified by decrypting and viewing a file in real time. Thus, one can see what it is and the upload time stamp.

(8) A feature for ordering a certification of authenticity by online delivery and optional email delivery.

(9) A feature for ordering a certification of authenticity with file that can delivered by regular mail.

(10) The encryption keys are generally sent to the server while data is encrypted using a SSL layer or equivalent, but is not expressly claimed in the claims.

4. Market demand for using the patented features

Although early file storage systems used FTP clients with graphic use interface, it would be a matter of time before FTP becomes totally obsolete! HTTP is still going to dominate internet protocol. The present invention uses HTTP as an example, but the claims do not specify any protocol. In uploading a file, FTP and HTTP are equivalent, but HTTP is more convenient to users.

This patented method is expected to be essential method in storage industry. First, consumers increasingly demand the option for using personal encryption keys that are not generated by computers, software, and will not be stored on the server. Sharing confidential files by using links is highly desirable. The repeated mass data breaches have forced cloud companies to use this basic claimed method. The patent is in the path to collide with the world in the remaining patent term of 10 years.

The patent started becoming an issue only in the last few years. For years, the cloud companies did not understand consumers' distrust in their existing storage systems. The patent was published in 2012, many companies started using server-side encryption using a customer-provided key one to several years after the publication. Designing around activities are revolving around using different terms and using technical equivalents (even avoiding using some claimed terms would have severely hurt its business).

The HTTP file sharing popularity and consumers' demand for high data security will force more and more companies (potentially more than a hundred) use the patented features now or within a few years. Designing around all claims is nearly impossible if companies want to make their storage systems competitive.

B. Summary of Patent Impact

The acceptability of the cloud data storage is limited by a popular concern with data storage security. To address this concern, many methods such as file system encryption, file encryption by account password, and later third-party administered file encryption have been developed. However, none of them can provide enough assurance to consumers. Digital safe and its improvements are intended to raise the users' confidence in data security because it eliminates insider's threats and risk of disclosure compelled by legal process. It also adds the last line of defense against hackers. Digital safe allows users to encrypt files on a file-by-file basis with different protection levels together with traditional transmission protection, thus dramatically increases “entropy”. The use of original encryption keys (rather than transformed keys) assure the highest portability and compatibility of encrypted files when secured files are expected to be shared among users. The file-logging method, together with data sharing method, allows any person to verify file content for files that were created in the past, thus, providing the most smart method for verifying file contents without examining file contents at the time of uploading files. In all respects, the patented method can achieve the highest data security.

Those methods, in conjunction with existing encryption methods such as data transmission encryption, file system encryption, and third-party administered encryption method create the highest at-rest data security theoretically possible. Digital Safe discloses a new method in data storage and will be essential to businesses and consumers who want to move their personal computing on to cloud computing.

Digital safe can be used for at least four major application models: (1) deploying digital safe as an individual file storage system in any cloud storage system, (2) using the patented method as a site tool of cloud computer for storing confidential files, (3) provision of digital safe accounts like bank physical safes for storing confidential files and legal instruments, and (4) deployment of the digital safe system as a central file storage system for multiple purposes such as preserving evidence, personal vital data, invention disclosure, and sealed contracts. When the invention is used to host evidence, it can lead to a new data storage industry for potentially hundreds of millions of users worldwide.

C. Related Patents

2. Digital Safe and Secure File Drawer (U.S. Pat. No. 9,449,183 B2). A secure file storage system with feature to select encryption machine for the maximum data security.

D. Market Size of Data Storage Industry

Digital safe is an essential tool in the cloud data storage market, future consumer data storage market, consumer cloud computing market, and internal data storage market of all industries. Some industries include law firms, investigative agencies, military, and security department of large corporations fields.

(1) The cloud storage industry: 74.94 billions by 2021. See article: http://www.marketsandmarkets.com/PressReleases/cloud-storage.asp.

(2) Consumer data storage cloud is still a void (currently it is used only for hosting websites): potentially hundred of billions. The main hurdles to consumers' use of public cloud is the cloud industry's inability to create highest data security.

(3). The method will impact many other fields. In particular, it will affect the legal field due to the critical nature of data in the e-discovery field. Its market size is USD 22.62 Billion in e-discovery by 2021. There are thousands of law firms. Medical data security is also the subject of protection at least in a good portion of cases.

(4). Some major players in the cloud data storage business include Amazon.com, Dell, Hewlett Packard Enterprise, Microsoft, IBM and a large number of hosting companies.

E. Flaws of Old Data Security Models

Prior art model was wrong and methods were poor. Prior art does not use individual encryption keys for encrypting files, but use a single account password for encrypting files, do not use file verification methods, and do not implement a method of sharing confidential files among users.

1. Common Prior art data security models

The data storage landscape has been heavily influenced by the early development of the trusted system model based upon trusted business relationship. Influenced by this business model, the server owners have a strong interest in keeping and tracking data. This model was originally developed for situations such as bank accounts and commercial sale transactions that require both sides to share data. However, the trusted system concept was extended to data storage system. The common features of prior art data storage security model are:

(1) Using an account password as encryption key for all files in a user account

so that the server administrator can access everything.

(2) Manipulating password or encryption keys to make it more difficult for employees of the hosting companies to access files.

(3) Using third-party vendors to manage encryption keys (Those methods are developed after the prior date of the patent).

(4) Adding additional twists in how data contents are stored. E.g. files may be broken up into pieces, encrypted by blocks, and stored on different servers or in different data centers….

(5) Even the public key infrastructure is vulnerable to security attacks because they are developed without considering data storage security.

2. Data security risks in prior art data security models

None of prior art methods has gained acceptance by consumers and businesses. Each of the prior art methods has fatal problems in data security, data sharing, data portability, and data compatibility. The continuous use of wrong data security strategy is the main reason that consumers would not move their personal computing onto the cloud and that most businesses would not move their last servers to public cloud.

(1) Password-based file encryption. This method is prone to security breaches by the insiders of data storage systems. Moreover, if the account password for a data storage account is jacked by a thief, all files in the account can be accessed by the thief. It poses a losing-everything risk. Consumers have long rejected this method. Since the user account password is saved on a server password database, a successful hacking of the account password database will allow a hacker to access all files stored on the server. The patented invention can prevent hackers to reach all files.

All companies historically stressed the need to use one single master key. This concept is contrary to real file security requirements. In the most prior art storage arrangements, data sharing is not possible because they use a single master key. For the same reason, file content validation and future verification is impossible. The claimed invention allows content verification in a future time.

(2) Manipulation of account passwords. Transformed passwords by using security tokens or data strings may increase difficulties to crack the passwords, but it cannot prevent insiders who know system designs from cracking the method. It is not immune from subpoena served onto those who know the storage system design. In addition, the manipulation of passwords does not change the risk of losing everything. Consumers have rejected this method.

Such a method does not solve the real problem that the password database can be hacked. The information on additional manipulation can be acquired from collaboration of server insiders. In addition, such security model cannot prevent disclosure compelled by legal process. In addition, while such a measure does

not seriously improve data security, but actually reduces data portability. The encrypted files cannot be ported to other systems for decryption. Lack data portability is a fatal problem if consumers want to store data for a very long period of time. Some wills may be stored for many decades. In comparison, the claimed invention can prevent insider attacks, crack abusive legal process, and provide highest data portability.

(3) Manipulation of file digital content. Some vendors break up a file into pieces and store the pieces on several servers or several data centers. This method does not address the risk of insider collaboration by those who know the system design, and cannot stop compelled disclosure by legal process. It also destroys data portability. If for any reason the company ceases to run its data storage business or if users must move their files way from their servers, it may post serious hardship to future data access and credibility of file content. The patented invention does not need to use any of such manipulation that would destroy data portability.

(4) Third-party management of encryption keys. When the encryption keys are managed by third party vendors. This class of methods do not improve data security meaningfully. It changes hacker's targets from data storage server's employees to key management server's employees. It could not stop legal process from reaching the keys. The claimed invention prevent inside attacks and abusive legal process. The method also poses the risk of losing everything. The third party management methods actually invite more people to know the details of security workings.

(5) Other manipulation methods. All other methods are merely to change the format of encryption keys, further increases the number of people who might know account passwords or encryption keys, and increase or change the storage locations of files…. They all violate the golden rule of data security: the safest method is let nobody know encryption keys, and hiding files in the forest is the best measure to prevent targeting operation. They destroy data portability which must be preserved. The patented invention does not need to manipulate encryption keys.

(6) Wrong advancements. Many new technologies are very bad. Manipulation of passwords or encryption keys will ruin data portability, splitting file storage may impair file portability, and let more parties to manage encryption keys will only add more leads for hackers to use in their targeted hacking operations.

Due to the fundamental flaw in data security models, few consumers would store their personal files on public cloud. Most companies also have to reserve one or more private servers for storing highly confidential files. With the massive data breaches, the industry must fully address data security risks.

F. A Sound Data Security Model

The data security models must meet the highest data security, greatest data portability, and greatest convenience in sharing confidential and secret files.

1. Highest data security

A valid security model must be consistent with the true requirement of data security. The highest data security must be achieved by preventing any persons other than the owner from knowing encryption keys. Data security is further increased when data storage systems kept using a large number of encryption keys. This creates a situation like a few targeted persons are hidden in thousands of people. Data encryption keys should be known by the owners only. It is none of the business of the server storage system companies or any other third parties. The safest method is let nobody know encryption keys.

2. Using different levels of data security

For file storage, file security levels must be based upon files. Some files are not confidential; some are personal; some are highly confidential; and some are of top personal secrets. For a typical consumer, web pages are for the public, the data published on Facebook is also for the public. Many files are of moderate confidential. Some files must be kept as private. A few files cannot be disclosed to others. Thus, encrypting all files in one single encryption key is clearly a poor strategy.

Moreover, confidentiality of files is relative to targeted persons. For example, certain public materials may be protected against unwanted readers; certain information may be protected against government agencies; business information may be protected against competitors, personal top secret files may be protected against the world. Family wills and trusts may be protected against those who might have interest in the legal instruments and those who might be in a position to challenge. The old notion of using one single encryption key for all files is also a wrong strategy.

The biggest problem is “linked loss of data security”. When public files and highly confidential files are encrypted by using the same encryption key, the disclosure of the public files with encryption key would destroy data security of all highly confidential files.

3. High data portability

When data is stored on the public cloud, one must think that data might have the need to be shared with others and there are all kinds of situations to move data from one data storage system to another. This data portability requires that the data encryption method be portable to other systems. If data files encrypted by using transformed encryption keys, such data files cannot be ported to other systems. Similarly, stored data on difference servers and different data centers will destroy data portability. In those cases, encrypted data cannot

be accessed by using other systems in real time. This is like using the worst method to achieve little benefits. Accordingly, consumers demand the use of the original form of encryption keys to encrypt files.

4. High data sharing capability

When data can be stored on the public cloud, it allows the users to share the data in a way the users want. Thus, this feature must be used to gain the widest acceptance.

5. Workable encryption key management

The burden in tracking encryption keys will depend upon whom files are encrypted against. For a company, files are encrypted against the rest of the world but not against the employees, the company can maintain a key file listing all encryption keys for all encryption files. There is no real burden here because the files would be available to all employees if they were not stored on a public cloud. If files are encrypted against internal employees as well as the rest of world, encryption keys must be kept against those who do not have right to access. This can be achieved by normal office restriction practices. For example, the key file in a corporate office cannot be accessed by employees working in other offices.

For consumers, if the purpose is against disclosure to a specific group of people or the rest of the world, encryption keys can be kept in a list of encryption keys at home. If the purpose is to prevent disclosure against certain family members, encryption keys are kept as private keys. They may also use combination of special terms, personal data, etc. as encryption keys. However, if the purpose is to prevent access by other family members or related members, one should avoid using critical personal data as key components.

Since for most files, the purpose is to prevent access by the public, the hackers, and rest of the world, encryption keys can be kept in an encryption key file on the table. The burden is not any bigger than how one must remember the files structure in a personal computer.

G. Problems Solved by The Invention

The patented invention solves the following problems:

1. Dramatically improving data storage security

The patented invention provides the most reliable and strongest data protection. No encryption keys are saved on the server, and no third person is involved in managing encryption keys. The file uploading method allows users to

choose a file encryption method from multiple methods, including no-encryption, encryption by account password, encryption by one key and two keys. The user can also do two layers of encryption (uploading the file with a key and getting back and uploading again with a different key). It also provides file verification method for verifying an encrypted file after file is upload. Due to the multiple forms of encryption, the system provides a method for tracking file encryption methods for each of the files. This method is the most rational method consistent with the realty that all files require different levels of data security and protection are directed against different persons.

2. Eliminating the risk of losing everything

When files in one single user account are encrypted in different encryption keys, it is impossible to hack individual files at once. Even if a hacker gets one encryption key, the hacker can only decrypt one or a few files, yet, the hacker most probably will not know which files can be decrypted. This prevents the user from losing all files under the user account. The chances are the hacker would not get any file.

When file encryption is performed on a server, encryption keys are transmitted in the network each time when a file is encrypted or decrypted. The user needs to select an encryption method, choose one or more encryption keys, with the option to use ambiguous or indirect file description. When the file storage system has millions of unidentified users (as in one use mode), a large number of unidentified files being encrypted using different encryption keys, it is impossible for hackers to target any files for attack after the files have been uploaded. It is also impossible to plan an attack to a file that is being uploaded. When a data storage system runs a large number of encryption processes with no advance information about file content, there is little incentive for a hacker to intercept all encryption keys and there is little time for a hacker to intercept one or more encryption keys. In other words, prevention of encryption keys are automatically achieved by the large entropy (too many encryption keys to be targeted in reality) and undisclosed file identities (no body knows what is in the file being presently uploaded).

Those measures are sufficiently effective to prevent server insider's attacks. Moreover, since the file-uploading process is also protected by using common transmission encryption, key-jacking in the transmission is highly impractical. It is especially so in light of short resident times. Key jacking by server employees are also more difficult: it is hard to know target keys and a successful operation would require something more than recording encryption key and file number. In uploading a file, a hacker in the network cannot know how importance a file is and must overcome the huddle of data transmission security measures.

3. Eliminating risks from losing password database

Since the files are encrypted by user-provided encryption keys that are

different from account passwords, hacking user account password database will have no use. Account passwords only allow someone to access unimportant files, which are encrypted by using a permanent account password. Thus, successful hacking of account password database or the data storage server's security method will have little use to the hacker in accessing the files protected by individual encryption keys.

4. Eliminating insider attacks and data loss by abusive legal process

Since important files are encrypted by using individual keys that are known only to the owner, the disclosure of password database or password information by file storage system insiders will have little impact on encrypted files. This method thus automatically prevents exposure which could be caused by abusive legal process. The only way to access encrypted files is that owners name files and provide encryption keys.

5. Providing new methods of sharing confidential files

The patented method allows any user to share encrypted files with other users of user accounts. The server may host a plurality of user accounts, and each user account can grant right of access to any files to the users of another user accounts. As along as the other users know encryption keys, they can decrypt the authorized files. This file sharing method is possible only for the files that are encrypted by using individualized encryption keys. In other words, the prior art methods of using one single master key for all files cannot implement this powerful file-sharing method. Not all files are equal.

6. Verifying file content in a future time

The sharing method stated above also creates a new possibility of verifying file content in a future time. This unique feature will support the formation of a new evidence-storage industry.

This patented method changes the timing of verifying file content from an upfront time to a after-event time. At the time of uploading a file, a user can verify file status for any file and record used encryption method. After certain years later, when the user has a need to prove the content of the file, the user grants access right to those users who want to verify the content of the file. Those users can use owner-provided encryption key to access the file in their own user accounts. The users can determine what was in the file and when the file was uploaded.

This method is superior to all prior art methods that conduct upfront content verification. An upfront verification poses a risk of losing the confidentiality of the file. The patented verification method gives the user a flexibility to arrange a proper time and right persons to verify file content. For example, verification persons can be designated by giving user accounts to individuals or law enforcement agencies. This method is important for storing wills, trusts, invention disclosure, and all kinds of sealed contracts. There might

be more new utilities from this verification method.

H. Patent Claim

The PTO did not find meaningful prior. Ellis (2007) was post-dated the priority date by two days. In addition, Ellis was entirely irrelevant. It discloses a file storage system. However, it did not disclose any of the following features: (1) using an individual encryption key to encrypt a file, (2) downloading and decrypting the file using the encryption key, (3) granting right of access to another user, and (4) accessing and decrypting the file by the another user, (5) using a file verification method, (6) viewing authenticity certificate of one or more files, (7) ordering hard copy authenticity certificate, (8) displaying encryption key hint on a download page, (9) creating global files for public access, (10) maintaining file histories, and (11) tracking access histories. For obvious reason, no further discussion is necessary.

The claim charts show required elements for reading on the claims.

1. Independent claim 1:

Elements	Key elements	Comment
Preamble	A file storing system, comprising a server having a network interface, and at least one client computer having a network interface, both the server and the at least one client computer being connected to the Internet, the system comprising:	A server and client computer network.
1	means for creating a user account as a safe by a first user by using safe name and password;	Read on any user account; no limit on format.
2	means for generating an uploading form with one or two input boxes, each for accepting an encryption key;	An uploading form with one or two input boxes. File uploading form is well known to get a file.
3	means for uploading a file in the safe of the first user;	Uploading the file into the safe of the first user.
4	means for encrypting the file on the server by using one or two encryption keys that the first user has provided and deleting the encryption	Encrypting the file on the server, and deleting the key.

	keys upon the finishing of the encryption on the server;	(deletion may be done by system action)
5	means for saving the uploaded and encrypted file along with tracking information on the server;	Saving the encrypted file with tracking information.
6	means for showing the file among other files in the safe of the first user;	After loading the file, the file is shown among other files in the user account.
7	means for showing any of the files and deleting any of the files in the safe of the first user;	Showing files and deleting files are essential.
8	means for generating a file-downloading page containing one or two input boxes for accepting an encryption key for a selected file, decrypting the selected file on the server by using the keys that the first user has provided, and downloading the selected file to the client computer of the first user;	Sending a download page with one or two input boxes for accepting an encryption key, decrypting the selected file using provided keys, and downloading the file to the client computer of the first user.
9	means for granting right of access to at least one file in the safe of the first user to a safe of a second user; and	Means for granting right access to other users of other accounts.
10	means for allowing the second user to access the at least one file of the first user, select a file from the at least one file of the first user, and send proper encryption keys to the server, descrypting the selected file on the server, and downloading the selected file to the client computer of the second user.	Means allowing the second user to decrypt the file and download the file to the safe of the second user.

Note: the claim 1 would read on a data storage system with the following features of (1) using an individual encryption key to encrypt a file, (2) downloading and decrypting the file using the encryption key, (3) granting right

of access to another user, and (4) accessing the file by the another user, and (5) downloading the file to the second user. Any step avoided would make a data storage system lose commercial value.

Claims 2-9 that are dependent upon claim 1

Elements	Key elements	Comment
Claim 2	The system of claim 1 wherein the uploading form contains an input box for accepting a hint for each of the one or two encryption keys and the file-downloading page displays the hint that has been entered for each of the one or two encryption keys and has been saved on the server.	The downloading page contains key hint.
Claim 3	The system of claim 1 further comprising means for allowing the first user to get an authenticity certificate for each of the files in the safe of the first user, the authenticity certificate containing file uploading time, file size, and file description.	Means for getting authenticity certificate
Claim 4	The system of claim 1 further comprising means for authorizing the safe of the second user to retrieve from the server an authenticity certificate for the at least one file or the means for sending an authenticity certificate to the second user by email.	Means for the second user to get file authenticity certificate from the first user.
Claim 5	The system of claim 1 further comprising means for making a file in the first safe to be globally accessible so that any user of the system can access it and any user having proper encryption key can decrypt and download the file.	Means for creating global file for public access (decrypting)
Claim 6	The system of claim 1 further comprising means for maintaining access histories for each of the files in each of the safes on the server.	Means for maintaining access histories.
Claim 7	The system of claim 1 further comprising means for tracking the access history of each encrypted file on the server and determining if the right of access to each of the encrypted files has expired or revoked.	Means for tracking access histories.
Claim 8	The system of claim 1 further comprising means for downloading a program for decrypting standalone files that have been encrypted using the same algorithm and the encryption keys in uploading the files to the server.	Means for downloading a program for decrypting the file off-site.

Claim 9	The system of claim 1 further comprising means for ordering a hard copy of at least one file together with an authenticity certificate certifying the file description, uploading time, and file size.	Meas for ordering a hard copy of authenticity certificate.

All of the features: displaying encryption key hint, maintaining file histories, tracking access histories, creating global files for public access, viewing authenticity certificate, and ordering hard copy authenticity certificate are all important in commercial deployment of this system. Even uploading time and file size are critical. If a server does not show a file identify, uploading time, or file size, it would create a huge confusion and invite adverse consumers reactions. A commercially viable system must be in a state of perfection.

2. Independent claim 10:

Elements	Key elements	Comments
Preamble	A method of storing confidential files on a server and client system for future proof of the substance and creation time of the files, the method comprising the steps of:	A server and client computer in a network.
1	creating a user account as a safe by a first user using a safe name and safe password;	Creating a user account
2	generating an uploading form by the server containing one or two input boxes for accepting an encryption key;	Generating an uploading form with one or two input boxes for accepting an encryption key.
3	uploading a file from the client computer of the first user;	Uploading the file.
4	encrypting the file by using the one or two encryption keys that the first user has provided and deleting the one or two encryption keys upon the finishing of encryption;	Encrypting the file and deleting the key.
5	saving the uploaded and encrypted file along with tracking information on the server;	Saving the file with tracking information.
6	sending a verification page for the encrypted file, prompting the first	Sending a verification page, and going through the

	user to enter one or two encryption keys corresponding to the one or two encryption keys used in encrypting the file in uploading, sending the encryption keys to the server and decrypting the uploaded file on the server by using the received encryption keys and deleting the encryption keys upon the finishing of the decryption, downloading the decrypted file to the client computer of the first user for inspection, and marking the uploaded file as a verified file upon successful verification;	process of verifying the file.
7	sending a file summary page to the client computer of the first user to display file information about the files in the safe of the first user, the file summary page containing file descriptions, uploading times and file sizes;	Showing the file among other files in the safe of the first user. [such summary page cannot be avoided.]
8	displaying any of the files, and deleting any of the files in the safe of the first user; and	Displaying any files in the safe and deleting any of the files in the safe.
9	generating a file-downloading page containing one or two input boxes for accepting an encryption key for a selected file, sending to the server proper encryption keys correspondent to the encryption keys used in encrypting the selected file during uploading, decrypting the selected file on the server by using the received encryption keys, deleting the encryption keys upon the finishing of decryption, and downloading the selected file to the client computer of the first user.	Generating the downloading page for downloading a file selected.

Note: the claim 10 would read on any data storage system with the

features of (1) using an individual encryption key to encrypt a file, (2) downloading the file using an encryption key, (3) a verification process for verifying an uploaded file, and (4) downloading the file to the client computer. Any step avoided would make a data storage system lose commercial value. Note there is no restriction that verification must be done at the end of uploading the file. It can be done anytime after a file is uploaded. All functions such as showing files and deleting files cannot be avoided. Such system must be perfect.

Claims 11-19 that are dependent upon claim 10

Elements	Key elements	Comment
Claim 11	The method of claim 10 further comprising the steps of granting right of access to at least one file of the safes of the first user to a safe of a second user, enabling the second user to access the file of the first user, decrypt the file on the server, and download the file to the client computer of the second user.	Granting right of access to the second safe account and downloading the file.
Claim 12	The method of claim 10 further comprising a step of allowing the first user to get an authenticity certificate for any of the encrypted files in the safe of the first user, wherein the authenticity certificate contains file uploading time, file size, and file description.	Getting authenticity certificate by the first user for his own files.
Claim 13	The method of claim 11 further comprising a step of authorizing the safe of the second user to retrieve an authenticity certificate for the files or a step of sending the authenticity to the second user by email.	Method for the second user to get file authenticity certificate from the first user.
Claim 14	The method of claim 10 further comprising a step of making a file in the safe of the first user to be globally accessible so that any user of the system can access the file and any user having proper encryption keys can decrypt and download the file.	Method for creating a global file for public access (e.g, decrypting with a key)
Claim 15	The method of claim 10 further comprising a step of maintaining access histories for each of the encrypted files for each of the safes on the server.	Maintaining file access histories.
Claim 16	The method of claim 10 further comprising a step of tracking the usage of rights of access granted to a file and determining if the right of access to the file has expired or revoked.	Tracking access-usage histories.

Claim 17	The method of claim 10 wherein the uploading form contains an input box for accepting a hint for each of the one or two encryption keys and the file-downloading page displays each hint that has been entered for each of the encryption keys and has been saved on the server.	The downloading page contains key hint.
Claim 18	The method of claim 10 further comprising a step of ordering by the second user a hard copy of files granted to the second user, together with an authenticity certificate certifying to the file descriptions, uploading times, and file sizes.	Ordering a hard copy of authenticity certificate.

All of the features: displaying encryption key hint, maintaining file histories, tracking access-usage histories, viewing authenticity certificate, and ordering hard copy authenticity certificate are all important in commercial deployment of this safe system. Even uploading time and file size are critical. If a server does not show a file identify, uploading time, or file size, it would create a huge confusion and invite adverse consumer reactions.

3. Independent claim 19:

Elements	Key elements	Comments
Preamble	A computer program product for use in operating file storage system comprising a server and at least one client computer, the computer program product comprising a computer usable medium having computer readable code embodied on the medium, the computer program code further comprising:	Read on all kinds situations involving a server and client computers.
1	program code for creating a user account as a safe by using a safe name or account number and safe password;	Generating a user account.
2	program code for generating an uploading form with one or two input boxes for accepting an encryption key;	Generate an uploading page
3	program code for uploading files to the server;	Uploading the file.
4	program code for encrypting files	Encrypting the file using the

	on the server by using one or two encryption keys that the first user has provided and deleting the encryption keys upon the finishing of encryption;	key.
5	program code for saving the uploaded file with tracking information on the server;	Saving the uploaded and encrypted file.
6	program code for sending a verification page for an encrypted file, prompting the first user to enter one or two encryption keys correspondent to the keys used in uploading the file, sending the user-entered encryption keys to the server, decrypting the uploaded file on the server by using the received encryption keys, downloading the decrypted file to the client computer of the first user for inspection, prompting the first user to indicate if the uploaded file is good, and marking the uploaded file as a verified file upon successful verification;	Sending verification page and going through all steps of file verification.
7	program code for sending a page for displaying the files, and deleting the files in any safe on the server;	Displaying files and deleting files.
8	program code for generating a file-downloading page containing one or two input boxes for accepting an encryption key for a selected file, decrypting the selected file on the server using the encryption keys the first user has provided, and downloading the selected file to the client computer of the first user;	Generating a downloading page and doing all download steps.
9	program code for granting right of access to at least one file of the first user to a safe of a second user; and	Granting right of access to a second safe/user account.

10	program code for enabling the second user to access the at least one file of the first user and select a file for downloading, sending to the server one or two encryption keys correspondent to the encryption keys used in encrypting the file in uploading, decrypting the file on the server using the received encryption keys, and downloading the uploaded file to the client computer of the second user.	Enabling the second user to access or download the file.

The claim 19 would read on a software product implementing the following features: (1) using an individual encryption key to encrypt a file, (2) downloading the file using an encryption key, (3) a verification process for verifying an uploaded file, (4) granting right of access to another user and access granted file by a second user, and (5) downloading the file to the client computer.

Claims 20 that is dependent upon claim 19

Elements	Key elements	Comment
Claim 20	A computer program product of claim 19 further comprising program code for decrypting standalone files that have been encrypted using the same algorithm and the encryption keys in uploading the files to the server.	Code for decrypting a standalone file.

I. Patent Validity

1. Patent Validity under AIA Session 33

Section 33(a) of the Leahy-Smith America Invents Act prohibits the patenting of "a claim directed to or encompassing a human organism."

Three independent claims uses the limitation on creating a user account or safe “by a user.” The question is whether the language is an issue under Session 33.

Ava Caffarini extensively examined the legislative history of the purpose of this statutory prohibition. This statute is to bar patent on various forms of human organism including a human organism, including a human embryo, fetus, infant, child, adolescent, or adult. See Ava Caffarini, Directed To or Encompassing a

Human Organism: How Section 33 of the America Invents Act May Threaten the Future of Biotechnology, 12 J. MARSHALL REV. I NTELL. PROP. L. 768 (2013). Section 33 is never intended to bar claims that merely require some actions performed by a human being. The statutory language “encompassing a human organism” is very clear.

A similar question was decided in a system claim in patent 8,692,659. On December 1, 2015, the International Trade Commission (ITC) rendered an opinion In the Matter of Certain Vision-Based Driver Assistance System Cameras, Components Thereof, and Products Containing the Same, investigation no. 337-TA-907. The claim is as follows:

> 91. The accessory mounting system of claim 90, wherein a light absorbing layer disposed at the vehicle windshield at least partially masks the presence of said attachment element from view **by a viewer who is viewing from outside the equipped vehicle** through the vehicle windshield.
>
> 92. The accessory mounting system of claim 91, wherein said light absorbing layer disposed at the vehicle windshield further at least partially masks the presence of said structure from view **by a viewer who is viewing from outside the equipped vehicle through the vehicle windshield.**

The Commission found that a person is not a limitation of the claims, and therefore, the claims are not invalid on this basis. The specification discloses "a substantially opaque black-outfrit to mask the presence of such members when viewed from outside the vehicle through the front windshield." The use of the word "when" illustrates that the patent does not require a person to actually be looking through the windshield from outside the automobile.

This result is expected considering that the claims are directed to a system, and claims 91 and 92 recite further components and structure of the system. The additional language in claims 91 and 92 of "by a viewer who is viewing from outside the equipped vehicle through the vehicle windshield" simply provide context to the claim for how the light absorbing layer functions. It is clear that "a viewer" is not being claimed as a physical component of the system.

Ex Parte Kamrava (PTAB 2012), APN 10/080,177 shows an example of a claim barred for containing a human being. The Kamrava patent is generally directed toward a uterine catheter that can be used to deposit a fertilized embryo. Some of the claims include an “embryo” as an element of the claim itself with "**the catheter ... further comprising an embryo** in the distal portion." In its November 26, 2012 decision, the Patent Trials and Appeals Board (PTAB) concluded that those claims could not be patentable.

Conclusion: “by the user” means user actions by a user. This is a common knowledge that user account is created upon user actions. The word “by” means user actions, which have been used widely.

2. Validity under Section 101

Alice challenge is unavailable to this invention. File encryption, files storage, filing opening, file sharing, etc. cannot be performed by mental steps. I have overcome Alice Rejection many times. This is an easy case. Natural law, abstract ideas are irrelevant to the claims.

3. Patent Validity under Section 103

Historically, the computer art always focuses on trusted system and trusted business relationship between the user and the server. It is very drastic concept to encrypt a file without leaving keys on the server as in 2007. While encryption is well known, the inventive concept is a working arrangement in storing files using a user-provided encryption key. Finding a combination to meet all claim limitations is unlikely, but a more extensively search needs to be done.

Defensive firms and all potential users must have studied this patent for years without filing a reexamination request. Those third party-key management methods might be developed after the publication of this patent and long after the priority date.

4. Enabling disclosure

The disclosure was based actual fully functional model. All steps can be understood by a grace at the those real screen view. There is no real defects that cannot be cured. Long claims construction has been conducted.

J. Consumers' Demand

It is obvious that cloud computing can reduce maintenance costs, increase data availability, improve data sharing efficiency, and reduce the risk of data loss. It also helps preserve environment. It is inevitable that personal computing will shift from traditional personal computers to the cloud.

1. What is required for the move to the cloud computing?

When consumers and businesses are in a position to put everything on remote servers or the public cloud, they need the highest data security. A brief review of the current security methods shows that none of the current security methods can eliminate the consumers' final reservation against moving onto the cloud. While file system encryption is used in limited cases, but such measure cannot be used to address the problems. Account password encryption method leaves a lead for hackers to solicit help from the server's insiders. File encryption measures managed by third-party vendors does not address the security concerns because business and personal secrets can be discovered by legal process such as improper subpoenas (while the user may be unable to challenge an improper subpoena due to his or her personal condition). In addition, whenever a single password or key is used, the cost of hacking all encrypted files by cracking the password or key would be considerably low.

Thus, data security is the key reservation preventing consumers from moving their personal computing to the cloud.

2. Huddles preventing the move to the cloud computing

I can easily show why consumers do not want to move their in-house computing to the cloud.

(1) Business owners cannot put confidential files and top secret documents on a third-party servers or a cloud storage system and, for that reason, they will prefer keeping in-house servers. GE for example, keeps several in-house servers for storing highly confidential files. When the massive data breaches involving 117 millions user accounts have been hacked, it is impossible to convince users of the data security. Even military would not keep their files securely.

(2) Law firms cannot put critical files on third-party servers or cloud storage system because they are concerned with at-rest data security. That is why they maintain in-house or internal servers.

(3) Organizations cannot store their files on third-party servers or a cloud storage system if they have confidential files that only their key employees may access.

(4) New immigrants will not store their personal files on a public cloud storage systems because they do not want anyone else to access their files. They rather carry their own media and personal computers with them.

(5) Inventors will not place their invention disclosure files on a third-party server or a cloud storage system because they cannot trust the current file security method.

(6) Software developers cannot place their source files on a third-party server or cloud storage system because someone might know their password.

(7) Families cannot place their confidential and secret legal documents such as wills, trusts, agreements, and family secrets on a public cloud storage system because they must keep such files away from other persons. For example, will be stored in the traditional method https://www.legalzoom.com/articles/where-to-store-a-last-will; https://www.legalzoom.com/articles/where-should-i-keep-my-last-will.

(8) Individuals always have personal secrets whether they are in files, documents, photos or other work products. They do not want anyone else to access. The best place is a Digital Safe implemented by the invention.

Each person may have specific reasons for worrying about data security. Some may concern their personal secrets, some may concern family information, some may concern their work product such as software products, and some may have personal history information. Some may want to keep secrets for everything. Therefore, it is fair to say that users-required protection scope of files may range from a small percent to all files. It would be extremely rare for a consumer to concern no privacy. If a consumer has only 1% of files that must be

fully protected, the consumer will not move his personal computing onto the cloud. It is irrelevant whether the public cloud service can secure the safety of the most of his files. In other words, if the public clouds cannot provide absolute data security for one file, several files, or a small percent files, the consumer will continue running his own computing at house.

Up to now, the industry has failed to provide measures to allow consumers to safely store critical files, it fails to attract consumers to move on to the cloud. Now, consumer's use of the public cloud is limited to subject matter that can be published as public information. The support service in most web hosting companies reveals that they provide services only in web hosting. This is a huge waste of resources and failure to use all business opportunities.

For similar reasons, if a business could not count on the data security of the public cloud, it will have to retain one or more computing servers on their own premises. Moreover, the continuous leakage of consumer data in the scale of Yahoo and Linkedln leaking types may generate a force to force the business to move back to in-house computing. The cloud vendors may need to demonstrate how they can prevent this kind of huge security breach in the future.

K. Impacts of Invention On Data Storage Industry

The patented invention may be deployed for two main models while it may be used in various other variations.

1. Pubic data storage system

It is deployed and scaled up for individual users just like a bank's safe boxes. It allows users to store their personal secret and confidential files. This can lead to huge confidential files storage and sharing system.

2. Sharing of confidential files over the internet

The patented system can be configured with a capacity of hosting a large number of safe boxes. In this system, the users can share their encrypted files by two methods: account-account sharing and owner and employee sharing. Moreover, the authorized users can access the files in different ways.

3. After-event verification services

Each encrypted file has file-tracking information and an uploading time stamp, the vendor can vouch for the content of the encrypted file and its updated time. Thus, the vendor can prove the context of any stored and encrypted file that was uploaded in the past. A file may be uploaded on January 10, 2000 without looking into the contents, but verification of the content can be performed in 2025. This is so-called future verification of the file content created in the past. The file content can also be proved by the user of other safe account by directly accessing and reading the file.

In addition to owner's control in selecting encryption method and keys, but the user can use different wording as true file identities. When the system has millions of unidentified users and a large number of the files being encrypted with different keys, such a system presents a great difficulty for hackers to pin point any file for attack. Therefore, a patented system deployed in this model is the best solution to the inherent vulnerability of public keys infrastructures.

4. Using the invention as a site tool for cloud accounts

The patented invention may be installed on dedicated servers, virtual servers, and shared servers for private use. For example, a company can use it to store and share files among its executives and employees; a person may use it to store personal confidential and secret files; and a family may use it to share files among its members. When it is so used, all features can be used except content after-event verification method. The population of potential users is very large. All individual users, small business, small law firms, and small organizations. It can easily reach the entire data storage space.

L. Impacts from Avoiding the Invention

Most companies attempt to avoid the patents by using technical equivalents, use of different arrangements of information, and use of different terms. Most designs around cannot pass challenge under the doctrine of equivalents. All claimed features are the best methods to address a serious data storage problems. Even by merely using different wording and terms could have real adverse impacts on cloud products and services. For the obvious reasons, most cloud companies must use the claimed invention to fully please their clients.

Failure to use the patented invention costs billions of dollars a year to the cloud industry and lose one or more new industries.

Most of cloud companies including all current giant companies have not figured out why the cloud space is not fully utilized. They holds the obsolete notion of meddling? the user's encryption keys and key management. Their business vision has been bound by the old concept of trusted storage system. The entire industry has sustained invisible financial loss for failing to use the patented concepts.

1. The U.S. misses a giant evidence-preservation industry

I have not seen advertisement on any confidential storage portal. This loss from failing to deploy such a portal is estimated at multiple billions.

When the cloud space can provide the best way to preserve personal confidential and secret information, the whole industry has not figured out that has prevented consumers from using it. Each time when a major data breach is reported, consumers are reminded with the reality of the industry's inability to

safe-protect consumer data. After this invention was published in 2012, most executives of the big cloud players still have not seen real problems. They continue to seek “safe way to manage one single master key”. Most companies even did not see the reality that different files require different security levels and against different disclosure targets.

Patented invention will dramatically promote the cloud utilization. By using it in the first mode, it can run the largest digital safe central portal or data warehouse. It will lead to three industries: the massive storage data warehouse with a massive confidential files sharing system, and a new industry for verification of file content (certification, and provision of court testimony in any disputes related to content of stored files).

2. A seriously limited business data service industry

While the cloud business is expanded rapidly, it has not reached a much bigger potential it should. First, the cloud use has been severely impaired by data security concerns. The fact that large companies cannot move all of their servers to the public cloud demonstrates their lack confidence in current data security models. Most of small and middle-size companies would not use the public cloud. They run only one to a few servers, as long as some of the files cannot be moved, they could not move at all. Security concern is a holdup that prevents most companies from moving onto the public cloud.

If data security is not fully addressed, the current cloud utilization may fall back. Consumers pay attention to all mega-scale data breaches. When each data breach instance harms consumer data, consumers generates force to compel the the companies to move back to in-house computing.

3. A missed consumer data backup service industry

Consumers run their computers without expert help. Therefore, they often are at very high risks to lose data. While backing up data by using media solves some of the problems of losing data, it is not completely safe. Data backup on the cloud is desirable in the following situations:

(1) backup of data against other family members and close friends

(2) backup of data against house fires and natural disasters

(3) backup of data which must be accessible anywhere

(4) backup of data that require search capability

(5) backup of data requires clear backup time order

(6) backup of data that must be rendered instantly

(7) backup of data that could not be placed in anyplace

(8) Backup of data that requires a long time storage

Backup media cannot be placed at homes or work places for various reasons. Online data backup has several advantages: it can be rendered instantly, the backup data can be accessed anywhere; the backup can be arranged for a

long duration as long as common data format is used to allow for future portability. When a search-able method is used, online data backup provides the best organization such as searching and sorting methods, which allow users to get data copies conveniently.

One main reason for online data backup on the cloud is data physical safety. USB media and other media used by consumers are not reliable for various reasons. It is well known that physical data on the cloud is much higher. One reason is that consumers are not trained in securing data safety, and are not trained to understand media durability, care about storage media, and predict the media life duration. In contrast, cloud companies have experts managing data backup to ensure that backup data are safe.

Based upon my own research, I infer that the cloud industry has gotten almost zero market size for consumer data backup. While consumers do get cloud spaces, but common use is storing public information that would be published on Facebook, social media, and web sites. Essentially, consumer data backup is still a virgin market that no vendor has been able to reach.

Since the true market size is unknown, I cannot say how much the cloud industry has lost. What I can say is that if the industry uses the patented data security models, it would easily generate a new consumer data backup market. What is the size of it? In 2016, there were about 125.82 million households in the United States. Assuming that 50% households use data backup services at annual fee of $10, the total revenue would be 125.82*0.50*10=629.1 millions per year (This does not include other value-added services).

4. A undeveloped consumer cloud computing industry

While the cloud computing is cheap and liable with a potential to make the online computing resource available anytime and anywhere, it still fails to attract consumers. Why?

The main reasons are the failure to data security models used in the current industry and the cost of deploying database applications (which I have fully addressed in other patent and pending applications).

In the past, it was successfully predicted that personal computer would be for every person and every household. Now, I predict that the cloud computing will be for everyone and every household. Some decisive advantages include fault proof-computing method, lower energy consumption, and high data availability. Those advantages dictate a move from personal computing to cloud computing. The holdups are data security and deployment costs for small business and consumers.

How much the cloud industry lose? It is in the range of tens of billions to potential one hundred billion of dollars each year. Additional loss may be in the value-added services which are common in the computing market.

5. Web hosting industry gain only one-third market

The software (“site tool”) implementing the patented concept as a cloud

site component will directly promote cloud service providers' business. The site tool will create and enlarge the demand for cloud storage space and cloud computing. Cloud service providers may gain additional market share by offering this tool by following possibilities:

1. A cloud service provider distributes this site tool to its cloud users for a monthly fee.

2. A cloud service provider sells the site tool to individual users and small businesses for fixed fees.

3. A cloud service provider distributes the site tool to its customers as a bundled tool so that it increases demand for the cloud.

4. A cloud service provider sells the site tool as independent product to its users so it will promote the general demand for the cloud. Cloud service providers will benefit from the enlarged demand for their cloud.

5. A cloud service provider creates a cloud provisional setup page (just like a controlling panel for signing up a cloud user account) which allows a user to deploy Digital Safe by making a single click.

M. Conclusion

The acceptability of the cloud computing and cloud storage is limited by the public concern with at-rest data security. None of the methods such as many methods such a file system encryption, file encryption by account password, and third-party administered encryption methods can address the problems.

Patented invention is intended to boost consumer confidence in using third-party cloud space. It allows users to encrypt files on a file-by-file basis and use multiple layers of encryption. Those methods, in conjunction with the lack of user identities and the presence of a large number of encrypted files, result in highest security entropy. The invention will promote the cloud computing and cloud storage by removing consumer's final reservation against the cloud.

The patented invention can lead to a new industry of preserving evidence and confidential and secret files, a new consumer-data back industry, and a true consumer cloud computing industry. It can easily result in billions dollars revenue each year.

The patented invention will help cloud companies dramatically expand web hosting industry. It will dramatically promote the demand for the cloud. The patented concept is useful for most companies in data storage management.

Its potential market scope is extremely large due to the expanded coverage of the internet access, availability of mobile devices, and increased need for maintaining personal confidential and secret files. The wide availability of access methods including public hot-spots, WIFI, wireless internet, TV based internet

access, and free public sites will further promote the consumers to use the cloud.

N. Contact Information

To contact patent owner, please contact Jianqing Wu at 202-560-3000 and tempaddr2@atozpatent.com.