



- (51) **International Patent Classification:**
G06F 21/62 (2013.01) *G06F 21/60* (2013.01)
- (21) **International Application Number:**
PCT/US2015/067941
- (22) **International Filing Date:**
29 December 2015 (29.12.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/097,426 29 December 2014 (29.12.2014) US
- (71) **Applicant:** F16APPS, INC. [US/US]; 3960 Howard Hughes Pkwy., Ste. 500, Las Vegas, NV 89169 (US).
- (72) **Inventor:** NAIEM, Ahmed Essam; #1 Dr Mohamed Sobhy St. Flat 6, Giza (EG).
- (74) **Agents:** LORD, Robert, P. et al.; Osha · Liang LLP, 909 Fannin Street, Suite 3500, Houston, TX 77010 (US).

- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title:** TIERED ACCESS CONTROL

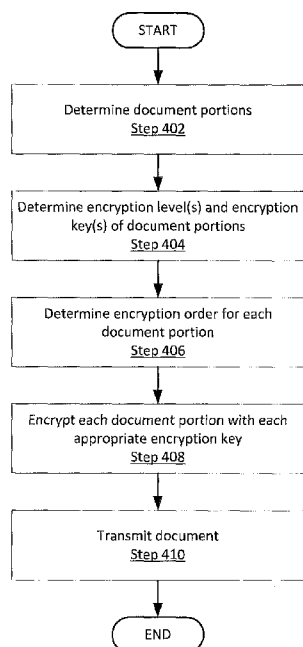


FIG. 4

(57) **Abstract:** A method involves providing tiered access control to a document. The method may include determining document portions of the document, determining encryption levels and encryption keys for each of the document portions, determining an encryption order for each of the document portions, the encryption levels, and the encryption keys, encrypting each of the document portions using the encryption levels, encryption keys, and encryption orders for each of the document portions, and transmitting the document to client interfaces. The method may further include receiving the document at a client device, determining the document portions of the document, decrypting one or more of the document portions using client encryption keys present at the client device into decrypted sections, and displaying the decrypted sections on a client interface of the client device.



Published:

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

TIERED ACCESS CONTROL

BACKGROUND

[0001] In general, encryption of files and folders protect sensitive documents from unwanted access. An encrypted document may be decrypted only by authorized recipients possessing a decryption key. In such a scenario, authorized recipients may be granted access to the entirety of the document. Further, all authorized recipients may be granted identical access to the same document.

SUMMARY

[0002] In general, in one aspect, embodiments relate to a method for providing tiered access control to a document. The method includes determining a plurality of document portions of the document. The method further includes determining a plurality of encryption levels and a plurality of encryption keys for each of the plurality of document portions. The method further includes determining an encryption order for each of the plurality of document portions, the plurality of encryption levels, and the plurality of encryption keys. The method further includes encrypting each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions. The method further includes transmitting the document to a plurality of client interfaces.

[0003] In general, in one aspect, embodiments relate to a system for providing tiered access control to a document. The system includes a processor, a memory executable by the processor, and an encryption server sharing platform stored in the memory and executing on the computer processor. The encryption server sharing platform further comprises a document parser and an encryption engine. The memory includes functionality for determining a plurality of document portions of the document. The memory further includes

functionality for determining a plurality of encryption levels and a plurality of encryption keys for each of the plurality of document portions. The memory further includes functionality for determining an encryption order for each of the plurality of document portions, the plurality of encryption levels, and the plurality of encryption keys. The memory further includes functionality for encrypting each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions. The memory further includes functionality for transmitting the document to a plurality of client interfaces.

[0004] In general, in one aspect, embodiments relate to a non-transitory computer readable medium (CRM) storing various instructions for providing tiered access control to a document. The instructions include functionality for determining a plurality of document portions of the document. The instructions further include functionality for determining a plurality of encryption levels and a plurality of encryption keys for each of the plurality of document portions. The instructions further include functionality for determining an encryption order for each of the plurality of document portions, the plurality of encryption levels, and the plurality of encryption keys. The instructions further include functionality for encrypting each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions. The instructions further include functionality for transmitting the document to a plurality of client interfaces.

[0005] Other aspects of the invention will be apparent from the following description and the appended claims.

BRIEF DESCRIPTION OF DRAWINGS

[0006] FIGs. 1-3 show schematic diagrams in accordance with one or more embodiments of the invention.

[0007] FIGs. 4-5 show flowcharts in accordance with one or more embodiments of the invention.

[0008] FIG. 6 shows a computing system in accordance with one or more embodiments of the invention.

DETAILED DESCRIPTION

[0009] Specific embodiments of the invention will now be described in detail with reference to the accompanying figures. Like elements in the various figures are denoted by like reference numerals for consistency.

[0010] In the following detailed description of embodiments of the invention, numerous specific details are set forth in order to provide a more thorough understanding of the invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid unnecessarily complicating the description.

[0011] Throughout the application, ordinal numbers (*e.g.*, first, second, third, etc.) may be used as an adjective for an element (*i.e.*, any noun in the application). The use of ordinal numbers is not to imply or create any particular ordering of the elements nor to limit any element to being only a single element unless expressly disclosed, such as by the use of the terms "before", "after", "single", and other such terminology. Rather, the use of ordinal numbers is to distinguish between the elements. By way of an example, a first element is distinct from a second element, and the first element may encompass more than one element and succeed (or precede) the second element in an ordering of elements.

[0012] In general, embodiments of the invention relate to a method, system, and computer readable medium (CRM) for providing tiered access control to a document, including determining a plurality of document portions of the document, determining a plurality of encryption levels and a plurality of

encryption keys for each of the plurality of document portions, determining an encryption order for each of the plurality of document portions, the plurality of encryption levels, and the plurality of encryption keys, encrypting each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions, and transmitting the document to a plurality of client interfaces. Embodiments of the invention also relate to a method, system, and CRM for receiving the document at a client device, determining the plurality of document portions of the document, decrypting one or more of the document portions using a plurality of client encryption keys present at the client device into a plurality of decrypted sections, and displaying the plurality of decrypted sections on a client interface of the client device.

[0013] FIG. 1 shows client devices (*e.g.*, client device A (100), client device B (104), and client device C (108)), client interfaces (*e.g.*, client interface A (102), client interface B (106), and client interface C (110)), an encryption server (112), and an encryption network (114) in accordance with one or more embodiments of the invention. In one or more embodiments, the client devices (*e.g.*, client device A (100), client device B (104), and client device C (108)) and the encryption server (112) may be connected via an encryption network (114) (*e.g.*, a local area network (LAN), or wide area network (WAN) such as the Internet, mobile network, or any other type of network). The client devices (*e.g.*, client device A (100), client device B (104), and client device C (108)) and encryption server (112) may take the form of a specialized computer system of the type found and described in relation to FIG. 6, for use in the operations described below in connection with FIGs. 4-5.

[0014] In one or more embodiments, a client device (*e.g.*, client device A (100), client device B (104), and client device C (108)) may be operatively connected to a public or private encryption network (114) and/or a local or remote server via a wired and/or wireless connection. In one or more embodiments, a client

includes functionality to communicate directly with the encryption server (112). In one or more embodiments, a client includes functionality to communicate indirectly with the encryption server (112) via a public or private encryption network (114). In this embodiment, the functionality to communicate indirectly with the encryption server (112) via a public or private encryption network (114) includes the functionality to transmit and receive via HTTPS (hypertext transfer protocol secure).

[0015] In one or more embodiments, a client device (*e.g.*, client device A (100), client device B (104), and client device C (108)) includes functionality to receive and store one or more client encryption keys received from the encryption server (112). In one or more embodiments, a client device (*e.g.*, client device A (100), client device B (104), and client device C (108)) includes functionality to decrypt a plurality of the document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300) using one or more client encryption keys received from the encryption server (112) into a plurality of decrypted sections.

[0016] In one or more embodiments, a client interface (*e.g.*, client interface A (102), client interface B (106), and client interface C (110)) is a software application written in any programming language and designed to be used to manage the encryption and decryption of a plurality of the document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300). A client interface (*e.g.*, client interface A (102), client interface B (106), and client interface C (110)) may include instructions that, when executed by a processor, enable a client device (*e.g.*, client device A (100), client device B (104), and client device C (108)) to perform one or more of the functions described below.

[0017] In one or more embodiments, a client interface (*e.g.*, client interface A (102), client interface B (106), and client interface C (110)) is a software application written in any programming language and designed to be used to display a plurality of decrypted sections that have been decrypted from the document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300) using a client encryption key present on the client device (*e.g.*, client device A (100), client device B (104), and client device C (108)).

[0018] In one or more embodiments, an encryption server (112) is a computer system or group of computer systems configured to service encryption related requests. For example, the encryption server may be configured to determine a plurality of encryption levels and a plurality of encryption keys for each of the plurality of encryption sections, determine an encryption order for each of the plurality of encryption sections, and encrypt each of the plurality of encryption sections using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of encryption sections. In one embodiment, the encryption server (112) interacts with users via a user interface (202). In another embodiment, the encryption server (112) interacts with users via a network interface (204). In one embodiment, the encryption server (112) and one or more of the client devices (*e.g.*, client device A (100), client device B (104), and client device C (108)) are implemented on the same server. In another embodiment of the invention, the encryption server (112) and one or more of the client devices (*e.g.*, client device A (100), client device B (104), and client device C (108)) are connected via an encryption network (114).

[0019] FIG. 2 shows an encryption server (112) in accordance with one or more embodiments of the invention. The encryption server (112) includes a user interface (202), a network interface (204), an encryption engine (206), a

document parser (208), and a data repository (210) comprising storage for encryption keys (212) and a document store (214). In one or more embodiments, the components of the encryption server (212) (*e.g.*, a user interface (202), a network interface (204), an encryption engine (206), a document parser (208), and a data repository (210)) are interconnected such that each component of the encryption server (212) may communicate with each other component of the encryption server (212). Further, in one or more embodiments, the components of the encryption server (212) (*e.g.*, a user interface (202), a network interface (204), an encryption engine (206), a document parser (208), and a data repository (210)) may be implemented in software, hardware, or some combination of hardware and software. Further, in one or more embodiments, two or more of the components of the encryption server (212) (*e.g.*, a user interface (202), a network interface (204), an encryption engine (206), a document parser (208), and a data repository (210)) may be combined into the same hardware and/or software within the encryption server (212).

[0020] In one or more embodiments, the user interface (202) is a software application written in any programming language and designed to be used to manage the encryption and decryption of a plurality of the document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300). In one or more embodiments, a user interface (202) is a software application written in any programming language and designed to be used to display a plurality of the document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300). The user interface (202) is also configured to associate one or more encryption levels with a document portion (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300).

[0021] In one or more embodiments, the network interface (204) is a process or group of processes configured to interact with the client devices (*e.g.*, client device A (100), client device B (104), and client device C (108)) via a public or private encryption network (114) and/or a server via a wired and/or wireless connection. Specifically, the network interface (204) may be configured to send and receive documents (300) for storage and retrieval in the document store (214) of the data repository (210). Further, the network interface (204) may be configured to receive requests related to the encryption of one or more documents (300) as described below. The network interface (204) may also be configured to receive requests for the documents (300) in the document store (214) of the data repository (210) and to transmit a document (300) to a plurality of client interfaces.

[0022] In one or more embodiments, the encryption engine (206) is a process or group of processes configured to encrypt and decrypt one or more document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300), as further described below in connection with FIG. 4. In one or more embodiments, the encryption engine (206) generates one or more encryption keys (212) for storage in the data repository (210) and/or transmission to a client device (*e.g.*, client device A (100), client device B (104), and client device C (108)) via a public or private encryption network (114). In one or more embodiments, the encryption engine (206) is configured to determine a plurality of encryption levels and a plurality of encryption keys for the document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300), as described below in connection with FIG. 4. In one or more embodiments, the encryption engine (206) is configured to determine an encryption order for a plurality of document portions (*e.g.*, document portion A (302), document portion B (304), document

portion C (306), document portion D (308), and document portion E (310)) of a document (300), as described below in connection with FIG. 4.

[0023] In one or more embodiments, the document parser (208) is a process or group of processes configured to determine a plurality of document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300). In one or more embodiments, the document parser is configured to determine the plurality of document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300) using input from a user via a user interface (202) or a network interface (204). In another embodiment, the document parser is configured to determine the plurality of document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) of a document (300) without using input from a user.

[0024] In one or more embodiments of the invention, the data repository (210) is any type of storage unit and/or device (*e.g.*, a file system, database, collection of tables, or any other storage mechanism) for storing data, including the encryption keys (212) and the document store (214). Further, the data repository (210) may include multiple different storage units and/or devices. The multiple different storage units and/or devices may or may not be of the same type or located at the same physical site. In one or more embodiments of the invention, the encryption keys (212) are generated, stored, and used by the encryption engine (206).

[0025] In one or more embodiments of the invention, the document store (214) is for storage and retrieval of a document (300) received via the network interface (204) and/or the user interface (202), which then may be stored in the data repository (210).

[0026] FIG. 3 shows a document (300) in accordance with one or more embodiments of the invention. A document (300) may be any of a variety of content, such as web pages, word processor documents, social media posts, pictures, videos, text, presentations, spreadsheets, source code, applications, etc. In one or more embodiments, a document (300) comprises one or more document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)). A document portion (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) is any subset of the content contained in a document (300). In one or more embodiments, document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) may be distinct portions within the document (300) (*e.g.*, document portion A (302), document portion B (304), and document portion C (306)). In another embodiment, document portions (*e.g.*, document portion A (302), document portion B (304), document portion C (306), document portion D (308), and document portion E (310)) may overlap partially or wholly within a document (*e.g.*, document portion D (308) and document portion E (310)).

[0027] While FIGs. 1-3 show a configuration of components, other configurations may be used without departing from the scope of the invention. For example, various components may be combined to create a single component. As another example, the functionality performed by a single component may be performed by two or more components.

[0028] FIG. 4 shows a flowchart in accordance with one or more embodiments for providing tiered access control to a document. In one or more embodiments, in STEP 402, the document parser of the encryption server determines a plurality of document portions of the document. The document portions may be distinct from each other within the document or may overlap

wholly or partially. In one or more embodiments, the document parser determines the plurality of document portions based on input from the user received via the user interface of the encryption server. For example, a user may view a document via an output device connected to the user interface and select one or more areas delineating a plurality of document portions via an input device connected to the user interface. In one or more embodiments, the document parser determines the plurality of document portions based on input from the user received via the network interface of the encryption server. For example, a user may select one or more areas delineating a plurality of document portions via an input device connected to the client interface of a client device, which is then transmitted to the document parser via the encryption network. In another embodiment, the document parser of determines a plurality of document portions without input from the user.

[0029] In STEP 404, in one or more embodiments of the invention, the encryption engine of the encryption server determines a plurality of encryption levels and a plurality of encryption keys for each of the plurality of document portions. In one embodiment, the encryption keys are stored in the data repository of the encryption server. In one or more embodiments, the encryption keys correspond to different encryption levels. For example, a first encryption key may correspond to an encryption level of “high trust” or “family,” while a second encryption key may correspond to an encryption level of “low trust” or “acquaintance.” In one or more embodiments, the encryption levels are distinct from each other. In one or more embodiments, the encryption levels are tiered. For example, the encryption level of “high trust” may encompass the encryption level of “low trust,” such that users associated with a “high trust” encryption level can also view content associated with a “low trust” encryption level, however users of a “low trust” encryption level can only view content associated with a “low trust” encryption level. In this example, the encryption engine may determine that the encryption levels of both “low trust” and “high trust” apply to one or more document portions.

[0030] The encryption engine of the encryption server may determine the plurality of encryption levels and the plurality of encryption keys for each of the plurality of document portions based on input from the user received via the user interface of the encryption server. Further, the encryption engine of the encryption server may determine the encryption level and encryption key for each of the plurality of document portions based on input from the user received via an input device connected to the client interface of a client device, which is then transmitted to the document parser via the encryption network. For example, a user may select a first document portion to be for “high trust” or “family” level. In another example, a user may select a second document portion to be for “low trust” or “acquaintance” level. In one or more embodiments of the invention, the encryption engine may determine that a document portion may receive one or more encryption levels and encryption keys (*e.g.*, document portion A having both a “high trust” and a “low trust” encryption level). In one or more embodiments, each encryption level (*e.g.*, “high trust” and “low trust”) has an associated encryption key.

[0031] In STEP 406, in one or more embodiments of the invention, the encryption engine of the encryption server determines an encryption order for each of the plurality of document portions. The encryption order is the order in which the encryption engine applies the encryption keys to encrypt the plurality of document portions, and may include applying more than one encryption key to a document portion. In one or more embodiments, the encryption engine determines an encryption order using the order of appearance of a document portion within a document. In another embodiment, the encryption engine determines an encryption order based on any overlap among the document portions. For example, if document portion D is encompassed by document portion E, the encryption engine determines that document portion D should have an encryption order before document portion E.

[0032] In another embodiment, the encryption engine determines an encryption order for tiered encryption levels using the relative relationship of the tiered encryption levels. For example, an encryption level of “high trust” may encompass an encryption level of “low trust” such that users associated with the encryption level “high trust” can view content associated with both encryption level “high trust” and encryption level “low trust.” In this example, the encryption engine may determine that the encryption order for a document portion with multiple encryption levels may be encrypted multiple times using the multiple encryption keys associated with the multiple encryption levels. In this example, the document portion intended to be seen by users of both a “high trust” and a “low trust” encryption level may receive a first encryption order for encryption using the encryption key associated with “high trust” and a second encryption order for encryption using the encryption key associated with “low trust.”

[0033] In STEP 408, in one or more embodiments of the invention, the encryption engine of the encryption server encrypts each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions. In one or more embodiments, for partially or wholly overlapping document portions, one or more document portions may be encrypted using a first encryption key and then the output of the first encryption encrypted again using a second encryption key. In one or more embodiments, for tiered encryption levels, one or more document portions may be encrypted using a first encryption key followed by the unencrypted document portion being encrypted again using a second encryption key, resulting in two encrypted document portions corresponding to the same document portion but encrypted using different encryption keys.

[0034] In STEP 410, in one or more embodiments of the invention, the network interface of the encryption server transmits the document to a plurality of client

interfaces. In one or more embodiments, the document contains one or more encrypted document portions.

[0035] FIG. 5 shows a flowchart in accordance with one or more embodiments for providing tiered access control to a document. In STEP 502, in one or more embodiments of the invention, a client device receives the document. In one or more embodiments of the invention, the document contains one or more document portions that have been encrypted with one or more encryption keys. The client device may receive the document from the encryption server via the encryption network.

[0036] In STEP 504, in one or more embodiments of the invention, the client device determines the plurality of document portions of the document. In one or more embodiments, the document portions may be partially or wholly overlapping.

[0037] In STEP 506, in one or more embodiments of the invention, the client device decrypts one or more of the document portions within the document using a plurality of client encryption keys present at the client device. In this embodiment, the result of the decryption is a plurality of decrypted sections. In one embodiment, the plurality of client encryption keys may have been received from the encryption server via the encryption network via HTTPS (hypertext transfer protocol secure). In another embodiment, the plurality of client encryption keys may have been stored locally on the client device. In one or more embodiments, decryption of each document portion is attempted with each client encryption key. In one or more embodiments, in the event of partially or wholly overlapping document portions, the client may use one or more client encryption keys following the decryption of a first document portion to decrypt a second document portion contained within the first document portion. In one or more embodiments, if a client device lacks the client encryption key to decrypt a document portion, the client device does not decrypt the document portion.

[0038] In STEP 508, in one or more embodiments of the invention, the client device displays the decrypted sections to the user. In one or more embodiments, the decrypted sections are displayed using a client interface of the client device. In one or more embodiments, the decrypted sections are fewer than the total set of document portions contained in the document.

[0039] In one or more embodiments, a first client device may contain different client encryption keys than a second client device. For example, a first client device may correspond to a “high trust” user while a second client device may correspond to a “low trust” user. In this example, the first client device contains client encryption keys for decrypting document portions associated with the “high trust” encryption level, while the second client device contains client encryption keys for decrypting document portions associated with the “low trust” encryption level. In this example, the first client device may display different document portions than the second client device, even with the same document if the document portions are encrypted using different encryption levels. In another example, the first client device and second client device may display the same document portions based on an overlap of the encryption levels associated with the first client device and the second client device and their associated client encryption keys.

[0040] While the various steps in the flowcharts in FIGs. 4-5 are presented and described sequentially, one of ordinary skill will appreciate that some or all of the steps may be executed in different orders, may be combined or omitted, and some or all of the steps may be executed in parallel. Furthermore, the steps may be performed actively or passively. For example, some steps may be performed using polling or be interrupt driven in accordance with one or more embodiments of the invention. By way of an example, determination steps may not require a processor to process an instruction unless an interrupt is received to signify that condition exists in accordance with one or more embodiments of the invention. As another example, determination steps may

be performed by performing a test, such as checking a data value to test whether the value is consistent with the tested condition in accordance with one or more embodiments of the invention.

[0041] Embodiments of the invention may be implemented on a computing system. Any combination of mobile, desktop, server, embedded, or other types of hardware may be used. For example, as shown in FIG. 6, the computing system (600) may include one or more computer processor(s) (602), associated memory (604) (*e.g.*, random access memory (RAM), cache memory, flash memory, *etc.*), one or more storage device(s) (606) (*e.g.*, a hard disk, an optical drive such as a compact disk (CD) drive or digital versatile disk (DVD) drive, a flash memory stick, *etc.*), and numerous other elements and functionalities. The computer processor(s) (602) may be an integrated circuit for processing instructions. For example, the computer processor(s) may be one or more cores, or micro-cores of a processor. The computing system (600) may also include one or more input device(s) (610), such as a touchscreen, keyboard, mouse, microphone, touchpad, electronic pen, or any other type of input device. Further, the computing system (600) may include one or more output device(s) (608), such as a screen (*e.g.*, a liquid crystal display (LCD), a plasma display, touchscreen, cathode ray tube (CRT) monitor, projector, or other display device), a printer, external storage, or any other output device. One or more of the output device(s) may be the same or different from the input device(s). The computing system (600) may be connected to a network (612) (*e.g.*, a local area network (LAN), a wide area network (WAN) such as the Internet, mobile network, or any other type of network) via a network interface connection (not shown). The input and output device(s) may be locally or remotely (*e.g.*, via the network (612)) connected to the computer processor(s) (602), memory (604), and storage device(s) (606). Many different types of computing systems exist, and the aforementioned input and output device(s) may take other forms.

[0042] Software instructions in the form of computer readable program code to perform embodiments of the invention may be stored, in whole or in part, temporarily or permanently, on a non-transitory computer readable medium such as a CD, DVD, storage device, a diskette, a tape, flash memory, physical memory, or any other computer readable storage medium. Specifically, the software instructions may correspond to computer readable program code that when executed by a processor(s), is configured to perform embodiments of the invention.

[0043] Further, one or more elements of the aforementioned computing system (600) may be located at a remote location and connected to the other elements over a network (612). Further, embodiments of the invention may be implemented on a distributed system having a plurality of nodes, where each portion of the invention may be located on a different node within the distributed system. In one embodiment of the invention, the node corresponds to a distinct computing device. Alternatively, the node may correspond to a computer processor with associated physical memory. The node may alternatively correspond to a computer processor or micro-core of a computer processor with shared memory and/or resources.

[0044] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

CLAIMS

What is claimed is:

1. A method for providing tiered access control to a document, comprising:
 - determining a plurality of document portions of the document;
 - determining a plurality of encryption levels and a plurality of encryption keys for each of the plurality of document portions;
 - determining an encryption order for each of the plurality of document portions, the plurality of encryption levels, and the plurality of encryption keys;
 - encrypting each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions; and
 - transmitting the document to a plurality of client interfaces.
2. The method of claim 1 further comprising:
 - receiving the document at a first client device;
 - determining by the first client device the plurality of document portions of the document;
 - decrypting one or more of the document portions using a plurality of client encryption keys present at the first client device into a first plurality of decrypted sections; and
 - displaying the first plurality of decrypted sections on a first client interface of the first client device.
3. The method of claim 2 further comprising:
 - receiving the document at a second client device;
 - determining by the second client device the plurality of document portions of the document;
 - decrypting one or more of the document portions using a plurality of client encryption keys present at the second client device into a second plurality of decrypted sections wherein the plurality of client encryption

- keys present at the first client device is different than the plurality of client encryption keys present at the second client device; and displaying the second plurality of decrypted sections on a second client interface of the second client device wherein first plurality of decrypted sections is different than the second plurality of decrypted sections.
4. The method of claim 2, further comprising transmitting the plurality of client encryption keys to the first client device.
 5. The method of claim 4, wherein the transmitting is performed via hypertext transfer protocol secure (HTTPS).
 6. A system for providing tiered access control to a document, comprising:
 - a processor;
 - memory; and
 - an encryption server sharing platform stored in the memory and executing on the processor, comprising:
 - a document parser configured to determine a plurality of document portions of the document;
 - an encryption engine configured to:
 - determine a plurality of encryption levels and a plurality of encryption keys for each of the plurality of document portions,
 - determine an encryption order for each of the plurality of document portions, and
 - encrypt each of the plurality of document portions using the plurality of encryption levels, plurality of encryption keys, and encryption orders for each of the plurality of document portions; and
 - a network interface configured to transmit the document to a plurality of client interfaces.

7. The system of claim 6 further comprising:
 - a first client device configured to:
 - receive the document,
 - determine the plurality of document portions of the document,
 - decrypt one or more of the document portions using a plurality of client encryption keys present at the first client device into a first plurality of decrypted sections, and
 - display the first plurality of decrypted sections on a first client interface of the first client device.
8. The system of claim 7 further comprising:
 - a second client device configured to:
 - receive the document,
 - determine the plurality of document portions of the document,
 - decrypt one or more of the document portions using a plurality of client encryption keys present at the second client device into a second plurality of decrypted sections wherein the plurality of client encryption keys present at the first client device is different than the plurality of client encryption keys present at the second client device; and
 - display the second plurality of decrypted sections on a second client interface of the second client device wherein first plurality of decrypted sections is different than the second plurality of decrypted sections.
9. The system of claim 7, wherein the network interface is further configured to transmit the plurality of client encryption keys to the first client device.
10. The system of claim 9, wherein the network interface is further configured to transmit the plurality of client encryption keys to the first client device via hypertext transfer protocol secure (HTTPS).
11. A computer readable medium for providing tiered access control to a document, comprising instructions that, when executed by a processor, perform the steps of:

determining a plurality of document portions of the document;
determining a plurality of encryption levels and a plurality of encryption keys
for each of the plurality of document portions;
determining an encryption order for each of the plurality of document portions;
encrypting each of the plurality of document portions using the plurality of
encryption levels, plurality of encryption keys, and encryption orders for
each of the plurality of document portions; and
transmitting the document to a plurality of client interfaces.

12. The computer readable medium of claim 11, further comprising instructions that, when executed by a processor, perform the steps of:

receiving the document at a first client device;
determining by the first client device the plurality of document portions of the
document;
decrypting one or more of the document portions using a plurality of client
encryption keys present at the first client device into a first plurality of
decrypted sections; and
displaying the first plurality of decrypted sections on a first client interface of
the first client device.

13. The computer readable medium of claim 12, further comprising instructions that, when executed by a processor, perform the steps of:

receiving the document at a second client device;
determining by the second client device the plurality of document portions of
the document;
decrypting one or more of the document portions using a plurality of client
encryption keys present at the second client device into a second
plurality of decrypted sections wherein the plurality of client encryption
keys present at the first client device is different than the plurality of
client encryption keys present at the second client device; and

displaying the second plurality of decrypted sections on a second client interface of the second client device wherein first plurality of decrypted sections is different than the second plurality of decrypted sections.

14. The computer readable medium of claim 12, further comprising instructions that, when executed by a processor, perform the steps of transmitting the plurality of client encryption keys to the first client device.
15. The computer readable medium of claim 14, further comprising instructions that, when executed by a processor, perform the steps of transmitting the plurality of client encryption keys to the first client device via hypertext transfer protocol secure (HTTPS).

1/6

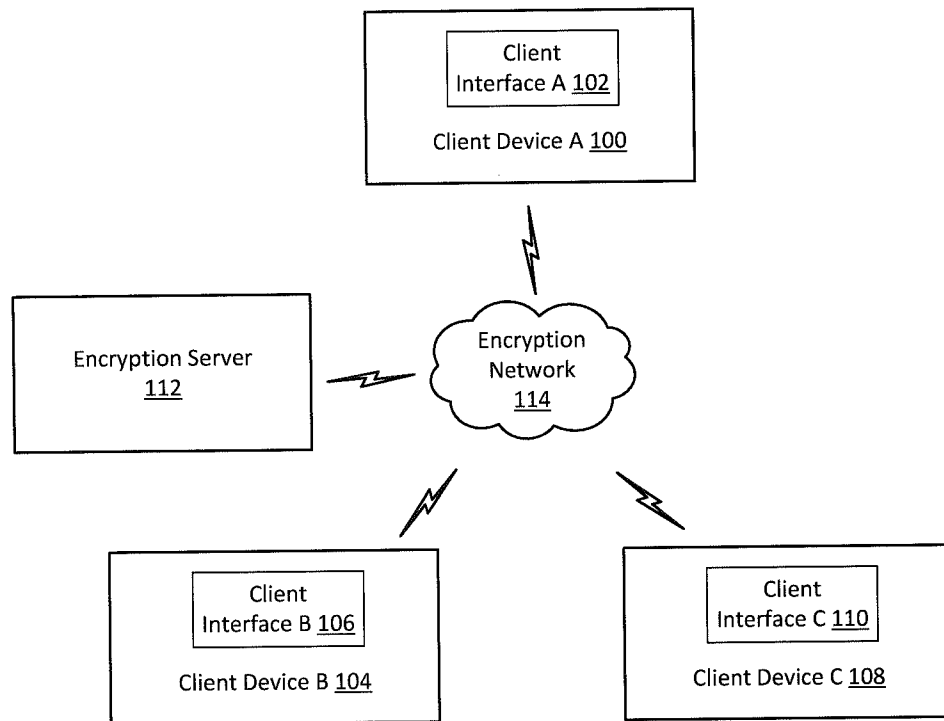


FIG. 1

2/6

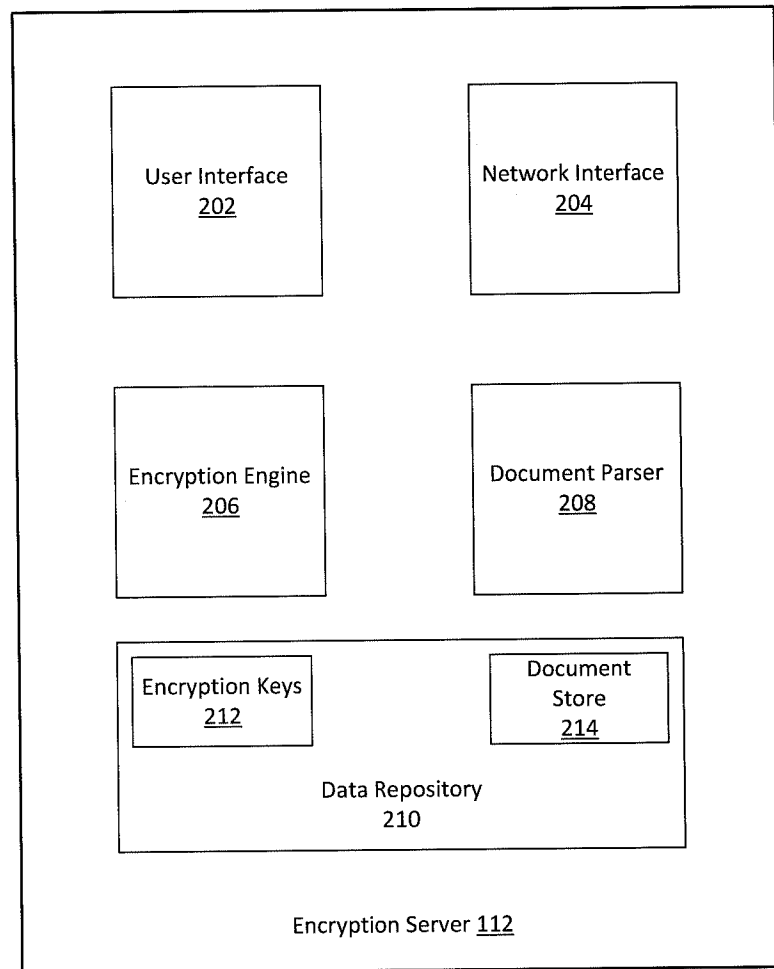


FIG. 2

3/6

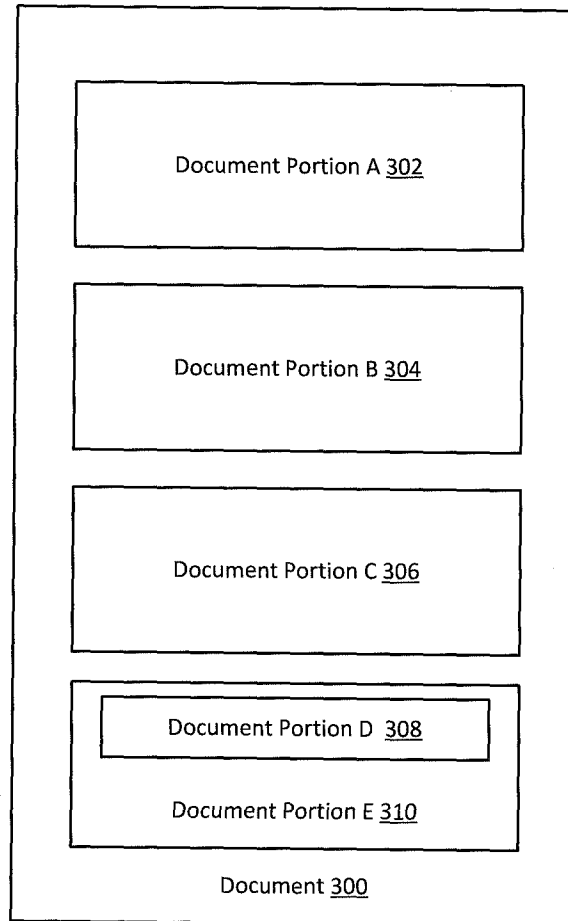
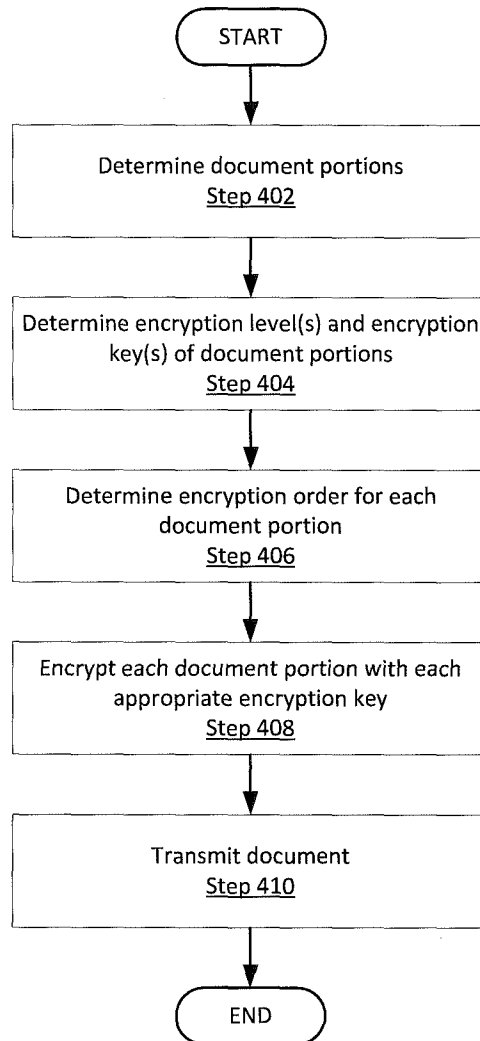
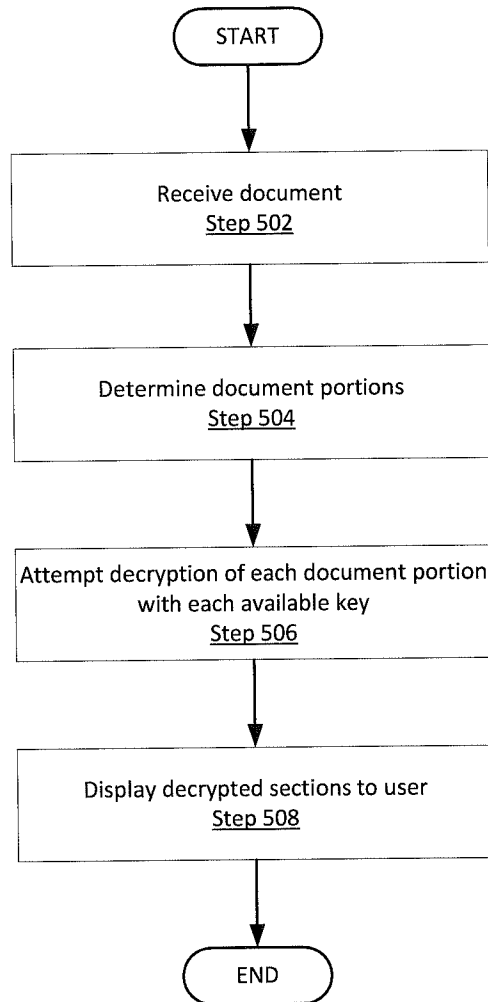


FIG. 3

4/6

FIG. 4

5/6

FIG. 5

6/6

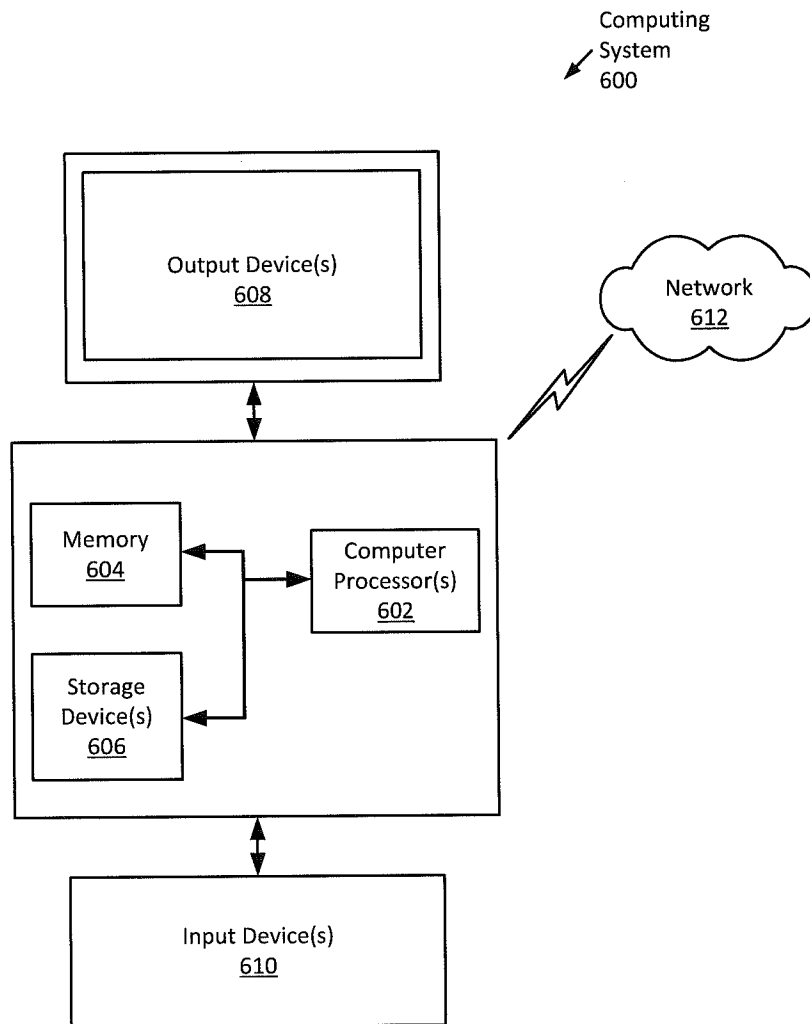


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/067941**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/62(2013.01)i, G06F 21/60(2013.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/62; G02B 21/00; G06F 11/30; H04N 1/44; H04L 9/32; H04L 9/00; G06F 1/24; G02B 21/16; G06F 21/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & keywords: document portions, encryption levels, encryption keys, decrypt, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6598161 B1 (KAREN RUTH KLUTTZ et al.) 22 July 2003 See column 6, line 55 - column 8, line 58; claims 1-11; and figures 3-6.	1-15
A	WO 02-01271 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 03 January 2002 See page 2, line 31 - page 6, line 9; claims 1, 12; and figures 1-6.	1-15
A	US 2008-0270807 A1 (RANDOLPH MICHAEL FORLENZA et al.) 30 October 2008 See paragraphs [0006], [0030]-[0031], [0036]-[0038]; claims 28-36; and figures 2, 7.	1-15
A	US 2006-0107044 A1 (GIRISH R. KRISHNA et al.) 18 May 2006 See paragraphs [0025]-[0035]; claims 1-2; and figures 3-4.	1-15
A	US 2007-0076874 A1 (MOHAMMAD A. SULEIMAN et al.) 05 April 2007 See paragraphs [0023]-[0026]; claim 1; and figure 2.	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

04 May 2016 (04.05.2016)

Date of mailing of the international search report

04 May 2016 (04.05.2016)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

CHIN, Sang Bum

Telephone No. +82-42-481-8398



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/067941

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6598161 B1	22/07/2003	None	
WO 02-01271 A1	03/01/2002	CN 1471661 A EP 1374009 A2 JP 2004-502379 A KR 10-2002-0041809 A WO 02-001271 A3 WO 02-01271 A2	28/01/2004 02/01/2004 22/01/2004 03/06/2002 02/10/2003 03/01/2002
US 2008-0270807 A1	30/10/2008	US 2005-0152531 A1 US 2005-0235163 A1 US 2007-0258577 A1 US 2009-0249083 A1 US 7092510 B2 US 7484107 B2 US 7889858 B2 US 7917771 B2 US 7986776 B2	14/07/2005 20/10/2005 08/11/2007 01/10/2009 15/08/2006 27/01/2009 15/02/2011 29/03/2011 26/07/2011
US 2006-0107044 A1	18/05/2006	JP 2006-139784 A US 7506160 B2	01/06/2006 17/03/2009
US 2007-0076874 A1	05/04/2007	JP 2007-104665 A US 8467530 B2	19/04/2007 18/06/2013