



- (51) **International Patent Classification:**
H04L 29/06 (2006.01)
- (21) **International Application Number:**
PCT/US2014/030958
- (22) **International Filing Date:**
18 March 2014 (18.03.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/846,974 19 March 2013 (19.03.2013) US
- (63) **Related by continuation (CON) or continuation-in-part (CIP) to earlier application:**
US 13/846,974 (CON)
Filed on 19 March 2013 (19.03.2013)
- (71) **Applicant:** RAYTHEON COMPANY [US/US]; 870 Winter Street, Waltham, Massachusetts 02451-1449 (US).
- (72) **Inventors:** NEUMANN, Matthew D.; 5555 E Mockingbird Lane, Apt# 3807, Dallas, Texas 75206 (US). SMITH, Michael W.; 300 Huntington Drive, Murphy, Texas 75094-4451 (US).
- (74) **Agents:** MADDEN, Robert B. et al.; P.O. Box 2938, Minneapolis, Minnesota 55402 (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, LT, 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, 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).

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))

(54) **Title:** METHODS AND APPARATUSES FOR SECURING TETHERED DATA

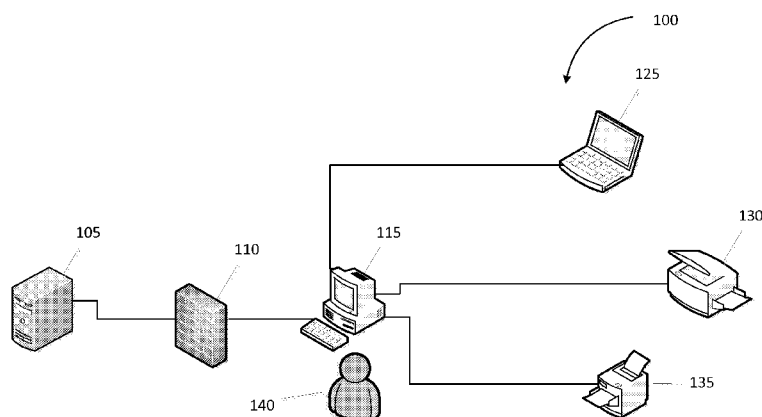


FIG. 1

(57) **Abstract:** Embodiments of a method and apparatus for securing and accessing files are generally described herein. In some embodiments, the method includes adding a communication portion to the file. The communication portion may communicate with an authentication agent on the first computing device. The method may include encrypting data of the file using a first key received through the communication portion from the authentication agent. The first key may be generated based on identification information of a second computing device in a trusted network of computing devices with the first computing device. The method may include saving the file to a remote file storage location.

METHODS AND APPARATUSES FOR SECURING TETHERED DATA

5 CLAIM OF PRIORITY

This application claims the benefit of priority to United States Application Serial Number 13/846,974, filed March 19, 2013, which is incorporated herein by reference in its entirety.

10

TECHNICAL FIELD

Some embodiments relate to file security. Some embodiments relate to creating environment-specific encryption keys for file security.

15

BACKGROUND

Corporations and government entities may seek to reduce or eliminate instances of unauthorized access to various types of sensitive information. Some systems may reduce or prevent unauthorized access by requiring users to log on to file storage systems with credentials such as user names and passwords. These systems, however, may not prevent authorized users from copying sensitive information and thereby removing sensitive information to unauthorized locations or computers. Other systems may bind sensitive information to one computer or computing system. However, these systems may be overly restrictive in limiting movement of data.

Thus, there are general needs for systems and methods for flexibly securing sensitive files such that the sensitive files cannot be used outside a secure environment, while still allowing a creator of a file to permit the file to be tethered to one machine regardless of that machine's physical location.

30

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a system in accordance with some embodiments.

FIG. 2 is a procedure for securing a file in accordance with some
5 embodiments.

FIG. 3 is a block diagram of a secured file in accordance with some
embodiments.

FIG. 4 is a procedure for opening a secured file in accordance with some
embodiments.

10 FIG. 5 is a block diagram of a system for implementing procedures in
accordance with some embodiments.

FIG. 6 is a block diagram of a processor for implementing procedures in
accordance with some embodiments.

15 DETAILED DESCRIPTION

The following description and the drawings sufficiently illustrate specific
embodiments to enable those skilled in the art to practice them. Other
embodiments may incorporate structural, logical, electrical, process, and other
20 changes. Portions and features of some embodiments may be included in, or
substituted for, those of other embodiments. Embodiments set forth in the claims
encompass all available equivalents of those claims.

Current corporate and governmental file security systems may seek to
ensure the confidentiality of data by reducing or preventing access by
25 unauthorized users. Some systems may attempt to reduce or prevent instances of
unauthorized access by requiring that a user enter credentials such as a user
name or password. Nevertheless, an adversary who has authorized access to the
sensitive data may copy the data to an external drive, such as a USB drive, and
remove the sensitive data from authorized premises. Other persons or entities
30 that do not have authorized access may thereafter access the sensitive data.

Some systems may provide an area of device memory, such as an area of
a hard disk, which is encrypted upon access to sensitive information. This area
may be decrypted upon termination of the access. However, these systems may

still allow the data to be left on the hard disk, and the data may therefore still be subjected to brute force attack.

These or other systems may bind the sensitive data to a computing device or a virtual machine, and decrypt the data at the time of access of the data. This approach may aggressively restrict the access of sensitive data by hindering movement of the computing device or virtual machine to another server or data center in the event of network or server failure. Further, these systems do not prevent copying of sensitive data once the data is accessed and decrypted.

Example embodiments may tether sensitive data to a machine or to a virtual machine executing in a trusted network by authenticating the environment in which the data is being saved or accessed. Example embodiments may further provide user authentication mechanisms before the data may be accessed. Example embodiments may provide the option for a creator of a file to enable secured local saving of the file to a machine.

FIG. 1 is a system 100 in which example embodiments may be implemented. The system 100 includes a server 105 for storage of data files, including sensitive data files. A firewall 110 may be present between the server 105 and at least one user computer or device 115. Other devices 125, 130, and 135 may be in a network, for example a trusted network, with the device 115. A user 140 may wish to create a secured file on the device 115. The device 115 may implement a procedure 200 as discussed below with respect to FIG. 2, to create a secured file.

FIG. 2 is a procedure 200 for securing a file created on a computing device, for example the device 115 (FIG. 1).

In operation 210, the device 115 may add a communication portion to the file. The communication portion may communicate with an authentication agent executing on the device 115.

In operation 220, the device 115 may encrypt data of the file using a first key received through the communication portion from the authentication agent. The first key may be generated based on identification information of a second computing device in a trusted network of computing devices. The second device may be, for example, one or more of devices 125, 130, or 135 (FIG. 1). The trusted network may include the device 115 and the second computing device.

The identification information of the second computing device 125, 130, or 135 may include a media access control (MAC) address of the second computing device 125, 130, or 135.

In operation 230, the device 115 may save the file to a remote file storage location. For example, the device 115 may save the file to the server 105 (FIG. 1).

The procedure 200 may further include setting a metadata indicator within the file to a value. The value may indicate whether permissions exist to save the file locally to the device 115. If the value indicates that permissions exist to save the file to the device 115, the procedure 200 may further include encrypting data of a second version of the file using a second key received through the communication portion from the authentication agent. The second key may be generated based on identification information of the device 115. The procedure 200 may further include saving the second version of the file to a local storage of the device 115. The procedure 200 may further include setting a second metadata indicator within the file to a value. The value may indicate whether the file has been saved locally on the device 115 so that a user 105 opening the file at a later time can open the file using the second key.

The procedure 200 may further include deleting the file from the device 115 upon closing the file in an editor executing on the device 115 if the indicator has been set to indicate that permissions do not exist for saving the file locally to the device 115. Deleting the file may include removing a pointer to the file. The procedure 200 includes destroying or deleting the unencrypted local file upon closing the file in the editor if the indicator has been set to indicate that permissions do not exist for saving the file locally to the device 115. If the file is to remain locally, the file will be encrypted with the local system key. The procedure 200 may further include destroying the file upon a failure of the communication portion to communicate with the authentication agent. The destroying may include encrypting the file a plurality of times using a random key.

FIG. 3 is an illustrative example of a file 300, secured according example embodiments of the procedure 200. The example file 300 may include executable code 310, for example binary code, etc., for communicating with an

authentication agent. The example file 300 may further include metadata 320. The metadata 320 may have an indicator 325, for example a local save enable flag, for indicating whether the file may be saved locally on the device 115. The metadata 320 may have another indicator 335, for example a locally-saved flag, for indicating whether the file was encrypted with a key created based on data of the local machine, such that the file may be opened on the device 115 without being connected to the trusted network. The example file may further include encrypted file data 330 encrypted with, for example, one or more keys received from the authentication agent. The encrypted file data 330 may include data created with various editors, for example text editors, video editors, and graphics editors.

FIG. 4 is a procedure 400 for opening a secured file on a computing device, for example the device 115 (FIG. 1). The secured file may be similar to the file discussed above with respect to FIG. 3.

In operation 410, the device 115 may retrieve the secured file from a file storage. The secured file, as discussed above with respect to FIG. 3, may include a communication portion for communicating with an authentication agent on the device 115 and an encrypted data portion. The communication portion may be similar to the executable code 310 (FIG. 3). The encrypted data portion may be similar to the encrypted file data 330 (FIG. 3).

The file storage may be a remote file storage. The key may be based on identification information of at least one other device, such as for example a computer, router, switch, or other network element in the network. For example, the key may be based on identification information of the device 125, 130 or 135 (FIG. 1). The identification information may be, for example, a MAC address of the device 125, 130 or 135, a secured shell (SSH) key of the device 125, 130 or 135, service names and port numbers on which services are communicating on the device 125, 130, or 135, etc.

In operation 420, the device 115 may decrypt the data portion using a key received through the communication portion from the authentication agent.

In operation 430, the device 115 may open the decrypted data portion for viewing or editing in an editing application or a viewing application.

The procedure 400 may further include authenticating access permissions of the device 115 to the remote file storage. The authenticating may be performed through, for example, a lightweight directory access protocol (LDAP) mechanism, through an Active Directory mechanism, etc.

5 The procedure 400 may further include determining that permissions for local file storage are enabled based on an inspection of a value of a metadata indicator within the secured file. The metadata indicator may be similar to the local save enable flag 325 (FIG. 3). The procedure 400 may further include
10 retrieving the secured file from a local memory, wherein the key for the decrypting is based on identification information of the device 115, based on the value of the metadata indicator. The procedure 400 may further include examining the metadata to determine whether a second indicator was set, indicating that the file was saved locally, and opening the file using on a local key or a remote key based on the value of the second indicator. The second
15 indicator may be similar to the locally-saved indicator 335 (FIG. 3).

The procedure 400 may further include destroying the file upon a failure of the communication portion to communicate with the authentication agent. Destroying the file may include encrypting the file a plurality of times using a random key, for example.

20 FIG. 5 is a block diagram of a computer 500 for implementing methods according to example embodiments. The computer 500 may be appropriate for performing the functionalities of the device 115 (FIG. 1). The computer 500 may be appropriate for viewing and editing files of various types.

The computer 500 may include a communication interface 510. The
25 computer 500 may include a processor 515. The processor 515 may include components as shown in FIG. 6. Referring to FIG. 6, the processor 615 may include an authentication agent 620 and one or more file editors 630. The authentication agent 610 may communicate with a remote file storage, for example the server 105 (FIG. 1) over the communication interface 625.

30 The one or more file editors 630 may be used to create a secured file as described above with respect to FIG. 2-3. The secured file may include a communication portion for requesting the encryption key from the authentication agent and a data portion including data encrypted with the encryption key. The

communication portion may be similar to the executable code 310 (FIG. 3). The data portion may be similar to the encrypted file data 330 (FIG. 3).

The authentication agent 630 may generate the encryption key based on identification information of the computer 500 or upon a second computing
5 device in a trusted network with the computer 500, for example the devices 125, 130 or 135 (FIG. 1). For example, the authentication agent may retrieve data specific to different machines in the networked environment, such as router names, computer medium access control (MAC) addresses, etc. The data
10 obtained may be unique for each sensitive data file, and the identity of the components of data used for creation of the key may be stored in metadata inside the sensitive data file. The metadata may be stored such that the actual key locations are not visible to the end user. For example, the actual key locations may be hashed, and the communication interface 510 may use the hash to look up the actual key location.

15 The authentication agent 630 may further be arranged to save the secured file to the remote file storage, for example the server 105 (FIG. 1). The authentication agent 630 may be arranged to save the secured file to local file storage, for example to memory 520 (FIG. 5). The authentication agent 630 may be arranged to save the secured file to both remote file storage and local file
20 storage, based on an indicator in the metadata of the secured file.

Referring again to FIG. 5, the computer 500 may store the secured file locally in a memory 520. In one embodiment, the memory 520 includes, but is not limited to, random access memory (RAM), dynamic RAM (DRAM), static RAM (SRAM), synchronous DRAM (SDRAM), double data rate (DDR)
25 SDRAM (DDR-SDRAM), or any device capable of supporting high-speed buffering of data. The computer 500 may include computer instructions 540 that, when implemented on the computer 500, cause the computer 500 to implement functionality in accordance with example embodiments.

For example, the computer instructions 540 may, when executed on the
30 computer 500, cause the computer 500 to receive a request for a first encryption key for encrypting a file. The computer instructions 540 may, when executed on the computer 500, cause the computer 500 to query a first network device for data of the first network device. The first network device may be a member of a

trusted network including at least the first network device and the computer 500. For example, the first network device may be the device 125, 130, or 135 (FIG. 1). The computer instructions, when executed on the computer 500, may cause the computer 500 to create the first encryption key using the data of the first
5 network device and write a secured file to a file storage. The secured file may include an encrypted data portion encrypted with the first encryption key. The encrypted data portion may be similar to the encrypted file data 330 (FIG. 3).

The instructions 540 may be stored on a computer-readable storage device, which may be read and executed by at least one processor 515 to
10 perform the operations described herein. In some embodiments, the instructions 540 are stored on the processor 515 or the memory 520 such that the processor 515 or the memory 520 act as computer-readable media. A computer-readable storage device may include any non-transitory mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a
15 computer-readable storage device may include ROM, RAM, magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media.

The Abstract is provided to comply with 37 C.F.R. Section 1.72(b) requiring an abstract that will allow the reader to ascertain the nature and
20 gist of the technical disclosure. It is submitted with the understanding that it will not be used to limit or interpret the scope or meaning of the claims. The following claims are hereby incorporated into the detailed description, with each claim standing on its own as a separate embodiment.

CLAIMS

What is claimed is:

1. A method for securing a file created, the method comprising:
 - 5 adding a communication portion to the file, the communication portion communicating with an authentication agent on a first computing device; encrypting data of the file using a first key received through the communication portion from the authentication agent, the first key being generated based on identification information of a second computing device in a
 - 10 trusted network of computing devices, the trusted network including the first computing device and the second computing device; and saving the file to a remote file storage location.
2. The method of claim 1, wherein the identification information of the second
- 15 computing device includes a media access control (MAC) address of the second computing device.
3. The method of claim 1, further comprising:
 - 20 setting a metadata indicator within the file to a value, the value indicating whether permissions exist to save the file locally to the first computing device; and
 - if the value indicates that permissions exist to save the file to the first computing device, encrypting data of a second version of the file using a second key
 - 25 received through the communication portion from the authentication agent, the second key being generated based on identification information of the first computing device, and
 - saving the second version of the file to a local memory of the first computing device.

30

4. The method of claim 3, further comprising:
deleting the file from the first computing device upon closing the file in an editor if the indicator has been set to indicate that permissions do not exist for saving the file locally to the first computing device.
- 5
5. The method of claim 1, further comprising:
destroying the file upon a failure of the communication portion to communicate with the authentication agent.
- 10 6. The method of claim 5, wherein the destroying comprises:
encrypting the file a plurality of times using a random key.
7. A method for opening a secured file on a first computing device, the method comprising:
- 15 retrieving the secured file from a file storage, the secured file including
a communication portion for communicating with an
authentication agent on the first computing device, and
an encrypted data portion;
decrypting the data portion using a key received through the
- 20 communication portion from the authentication agent; and
opening the decrypted data portion for viewing or editing in an editing
application or a viewing application.
8. The method of claim 7, wherein:
- 25 the file storage is a remote file storage, and
the key is based on identification information of at least one other computing
device in the network.
9. The method of claim 8, further comprising:
- 30 authenticating access permissions of the computing device to the remote
file storage.

10. The method of claim 9, wherein the authenticating is performed through a lightweight directory access protocol (LDAP) mechanism or through an Active Directory mechanism.

5 11. The method of claim 7, further comprising:

determining that permissions for local file storage are enabled based on an inspection of a value of a metadata indicator within the secured file; and

retrieving the secured file from a local memory, wherein
the key for the decrypting is based on identification information of the first
10 computing device.

12. The method of claim 7, further comprising:

destroying the file upon a failure of the communication portion to communicate with the authentication agent.

15

13. A non-transitory computer-readable medium comprising instructions that, when executed on a machine, cause the machine to:

receive a request for a first encryption key for encrypting a file;

query a first network device for data of the first network device, the first
20 network device being a member of a trusted network including at least the first network device and the machine;

create the first encryption key using the data of at least first network device, the data being collected by an aggregation server; and

write a secured file to a file storage, the secured file including an encrypted data
25 portion encrypted with the first encryption key.

14. The computer-readable medium of claim 13, wherein the data of the first network device includes a medium access control (MAC) address of the first network device.

30

15. The computer-readable medium of claim 13, further comprising instructions that, when executed on the machine, cause the machine to:
- determine whether to write the secured file to a local file storage of the machine, to a remote file storage, or to both the local file storage and the remote
- 5 file storage based on a value of an indicator in metadata of the secured file, the value indicating whether permissions are enabled for local file storage of the secured file.
16. The computer-readable medium of claim 15, further comprising instructions
- 10 that, when executed on the machine, cause the machine to:
- if a value of the indicator indicates that permissions exist for enabling local file storage of the secured file, create a second encryption key using at least one piece of identification data of the machine.
17. The computer-readable medium of claim 16, further comprising instructions
- 15 that, when executed on the machine, cause the machine to:
- receive a request for a decryption key for decrypting the file; and provide the first encryption key or the second encryption key in response to the request based on the value of the indicator.
- 20
18. The computer-readable medium of claim 17, wherein the request is received over a connection to a communication portion of the file, the communication portion comprising computer-executable code.
19. An apparatus comprising:
- 25 a communication interface;
- an authentication agent to
- communicate with a remote file storage over the communication interface, and
- 30 generate an encryption key based on identification information of the apparatus or on identification information of at least a second apparatus in a trusted network with the apparatus, the identification information being collected by an aggregation server; and

one or more file editors to create a secured file, the secured file including a communication portion for requesting the encryption key from the authentication agent and a data portion including data encrypted with the encryption key.

5

20. The apparatus of claim 19, further comprising a memory for local file storage of the secured file.

21. The apparatus of claim 20, wherein the authentication agent is further
10 arranged to:

save the secured file to the remote file storage, to the local file storage, or to both the remote file storage and the local file storage based on an indicator in the metadata of the secured file.

15 22. The apparatus of claim 19, further comprising:

a credentials agent to authenticate the apparatus to the remote file storage.

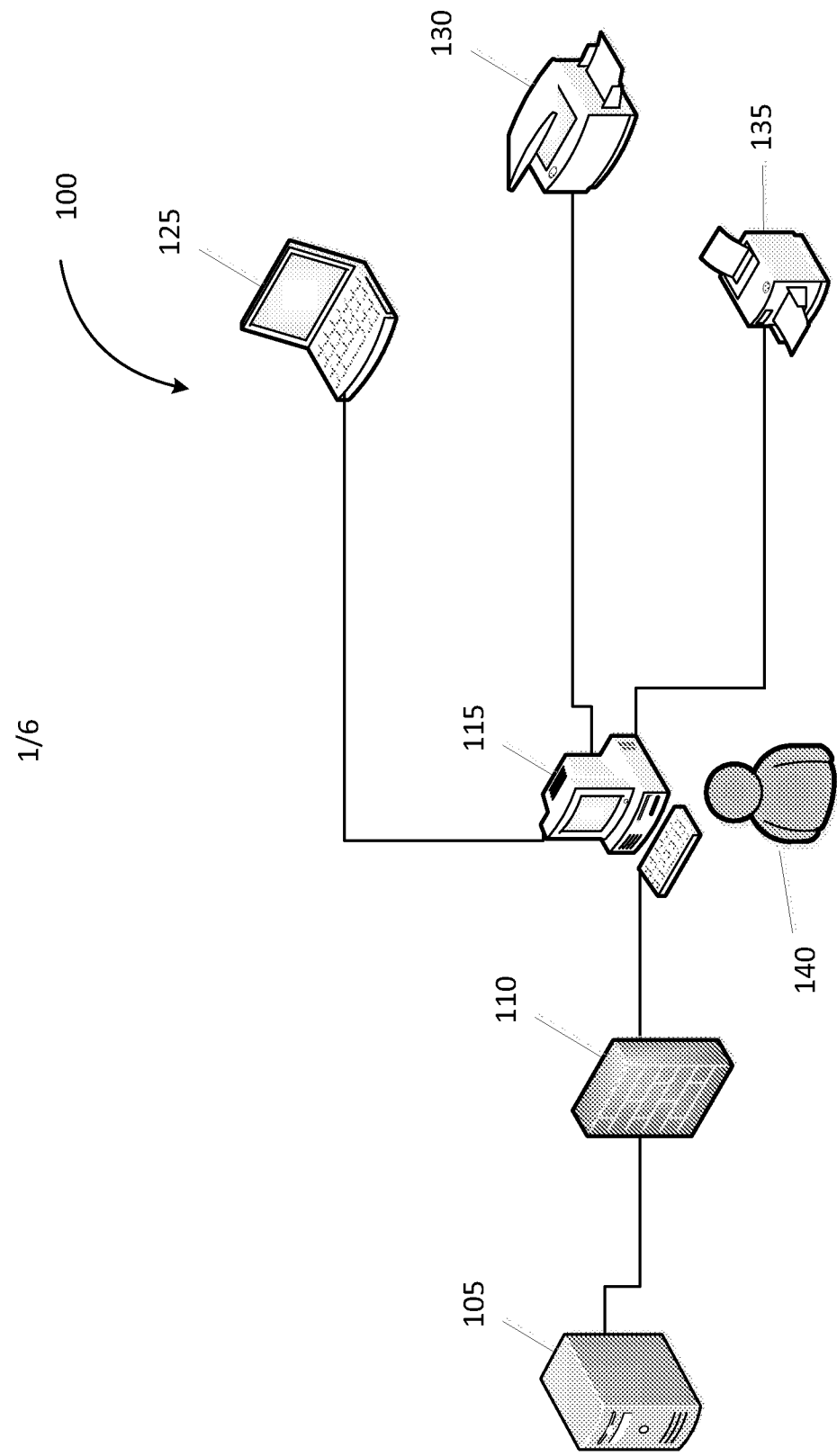


FIG. 1

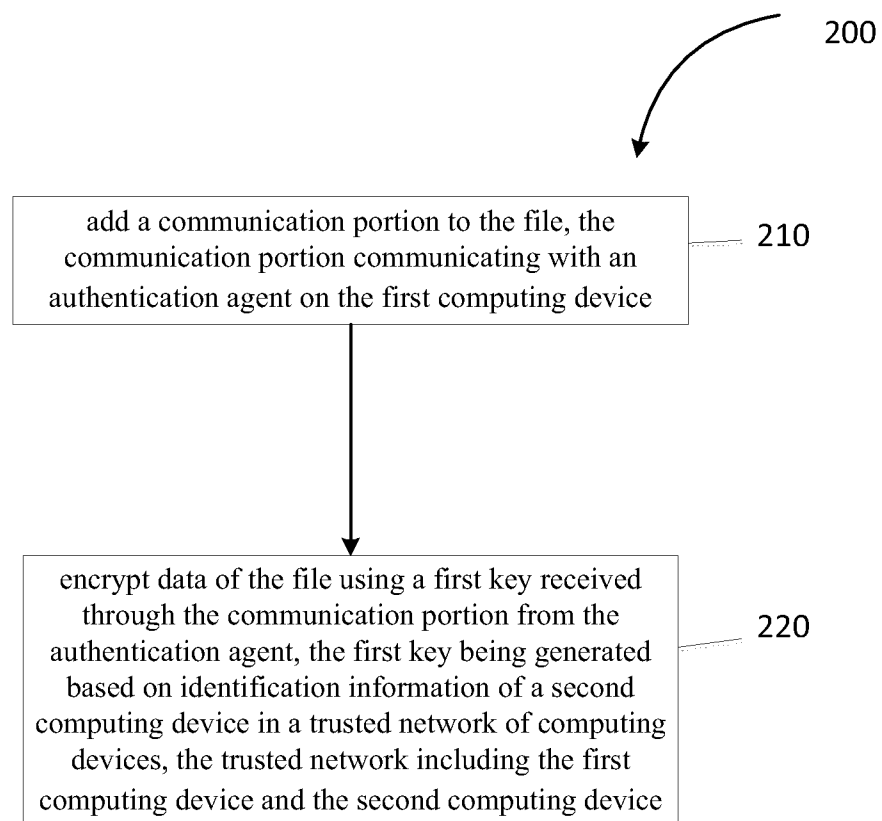


FIG. 2



FIG. 3

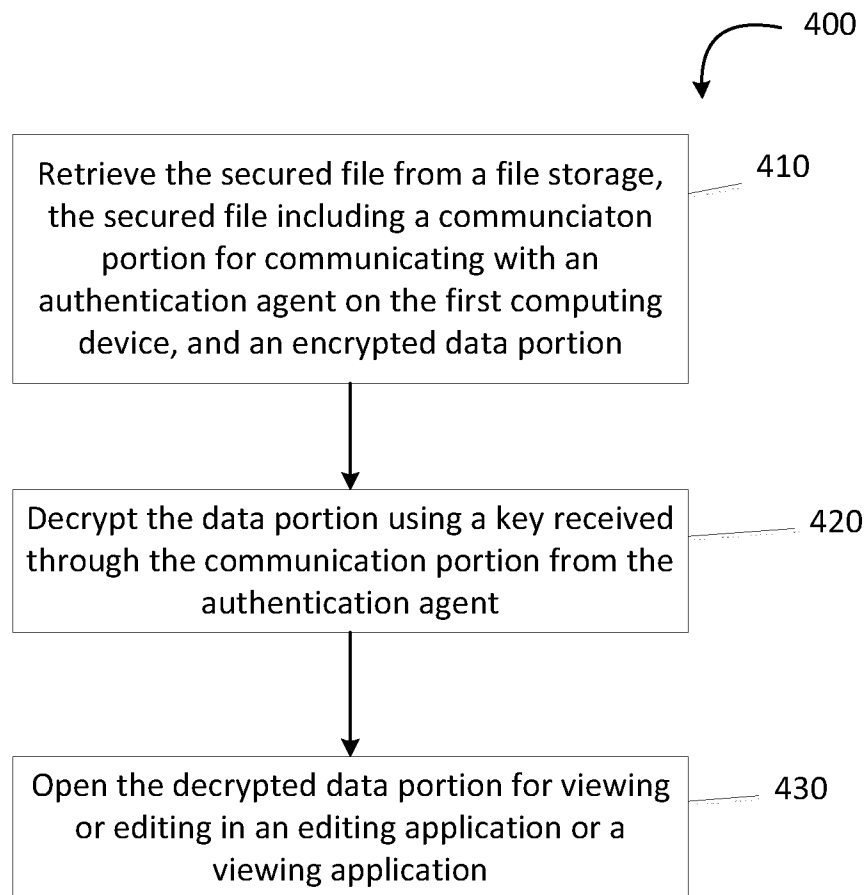


FIG. 4

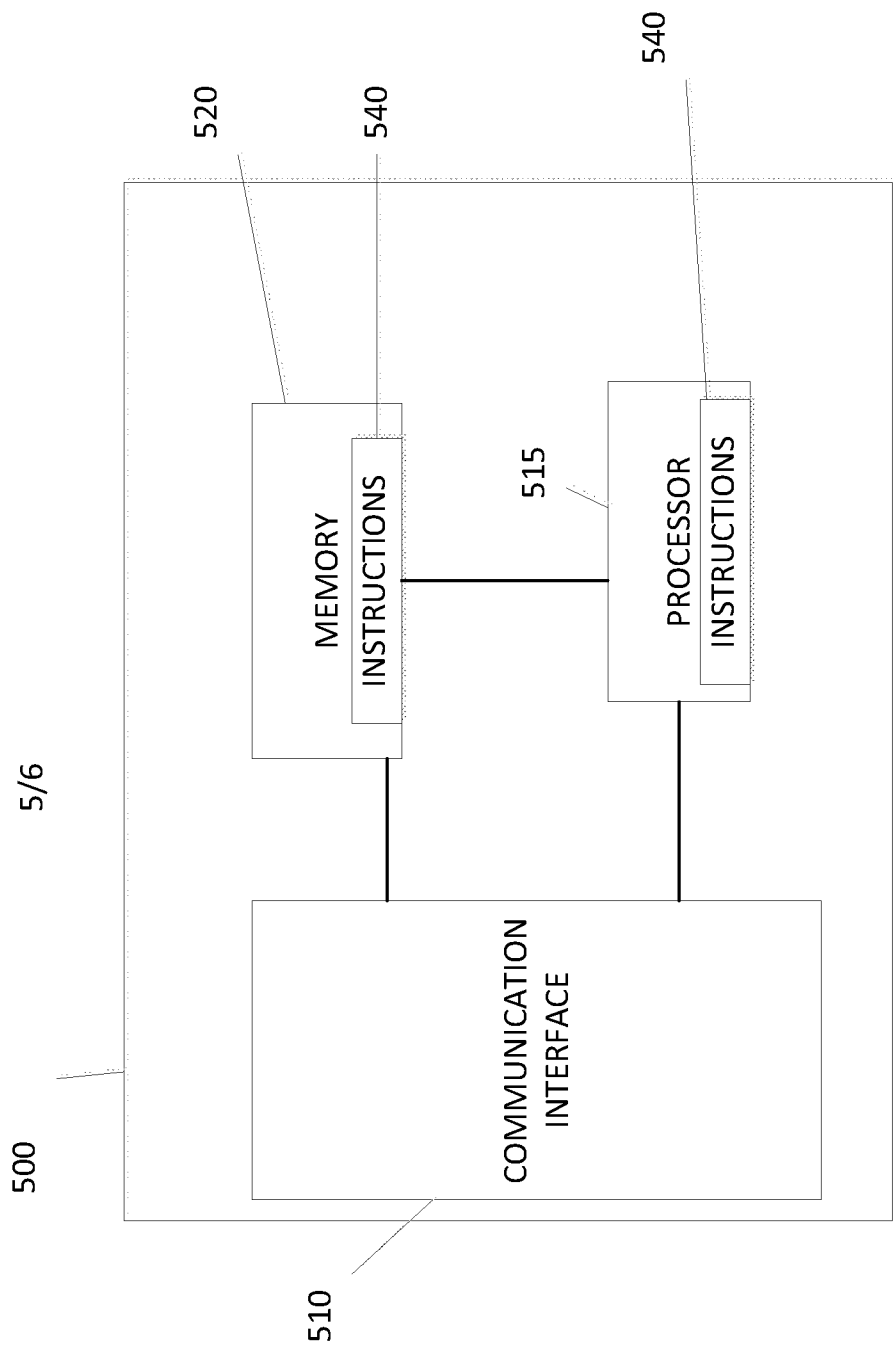


FIG. 5

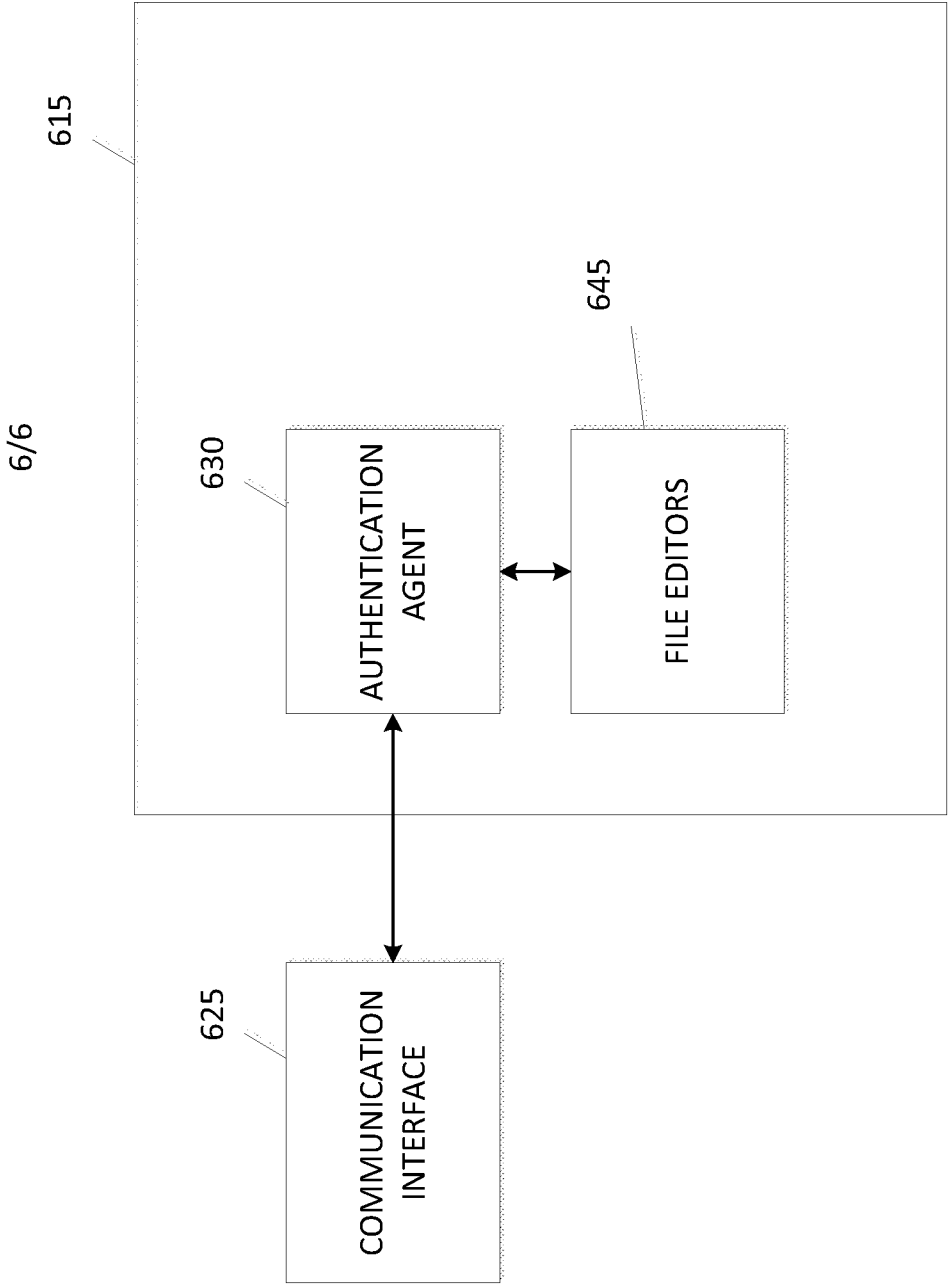


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/030958

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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)
H04L G06F

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

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

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Menezes, Vanstone, Oorschot: "HANDBOOK OF APPLIED CRYPTOGRAPHY; Chapter 13: Key Management Techniques", CRC PRESS, BOCA RATON, FL, US, PAGE(S) 543 - 590	1,2, 7-10,13, 14,19, 20,22
A	1 October 1996 (1996-10-01), XP001525013, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL: http://www.cacr.math.uwaterloo.ca/hac/ [retrieved on 2014-08-20] page 546 - page 550 page 561 - page 562 ----- -/-	3-6,11, 12, 16-18,21



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

20 August 2014

Date of mailing of the international search report

27/08/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

San Millán Maeso, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/030958

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012/084544 A1 (FARINA RALPH ROBERT [US] ET AL) 5 April 2012 (2012-04-05) abstract; figure 10 paragraph [0014] - paragraph [0019] paragraph [0119] - paragraph [0123] -----	1-22
A	US 2011/235799 A1 (SOVIO SAMPO JUHANI [FI] ET AL) 29 September 2011 (2011-09-29) abstract -----	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2014/030958

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012084544	A1	05-04-2012	AU 2011313985 A1 09-05-2013 AU 2011329455 A1 23-05-2013 EP 2625643 A1 14-08-2013 EP 2625839 A1 14-08-2013 US 2012084544 A1 05-04-2012 US 2012084545 A1 05-04-2012 US 2012084562 A1 05-04-2012 US 2012084566 A1 05-04-2012 US 2012084838 A1 05-04-2012 WO 2012051006 A1 19-04-2012 WO 2012067726 A1 24-05-2012
US 2011235799	A1	29-09-2011	NONE