



(51) International Patent Classification:  
*G06F 21/10* (2013.01) *G06F 9/44* (2006.01)

(21) International Application Number:  
PCT/US2015/036901

(22) International Filing Date:  
22 June 2015 (22.06.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **KALIBJIAN, Jeff**; Hewlett Packard, 1140 Enterprise Way, Sunnyvale, California 94089 (US). **LOPEZ, Scott**; Hewlett Packard, 5400 Legacy, Plano, Texas 75024 (US).

(74) Agents: **FEBBO, Michael A.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (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,

[Continued on next page]

(54) Title: CONTROL OF APPLICATION LOG CONTENT

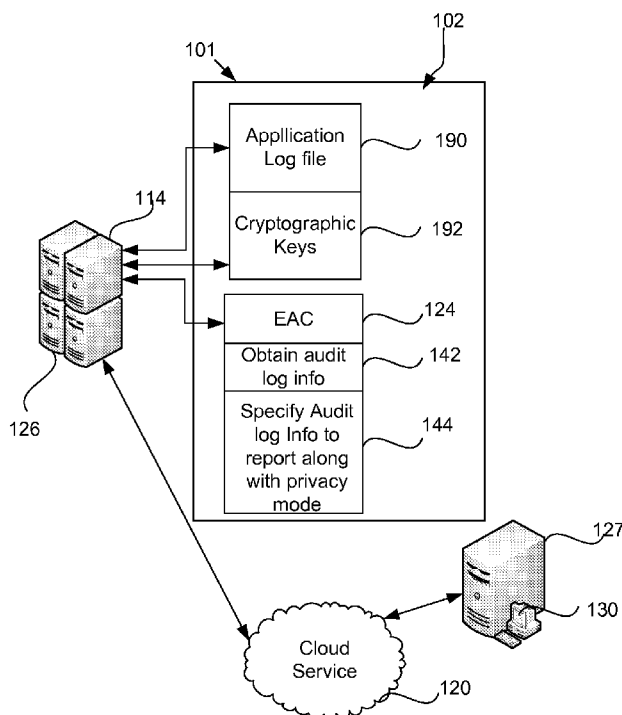


Fig. 2

(57) Abstract: A cloud-based application allows a client to obtain audit log information from an application. The application also allows the client to specify which audit log information from the application is reported and secured to a log file of the application.



DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, **Published:**

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).

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

**Declarations under Rule 4.17:**

- *as to applicant's entitlement to apply for and be granted  
a patent (Rule 4.17(ii))*

## CONTROL OF APPLICATION LOG CONTENT

### BACKGROUND

**[0001]** It is common for computer applications to write important information about its activities and events to a discrete output log file. Originally this information was used to debug applications or better monitor the application performance. In the meantime, another use of the data within the discrete output log file has been found. Specifically, an application's log data may be used, along with other event log data from other applications and network devices to detect threats in an information technology (IT) environment. This use of the log data has led to the development of an IT application known as a Security Information Event Management (SIEM) tool. SIEM applications enable event log data to be collected from many different classes of applications that write their event data to event log files. Generally, a SIEM application aggregates, normalizes, filters, and correlates event data enabling it to identify potential threats in an IT environment. Accordingly, a SIEM application can also report, analyze, and audit which may facilitate its use as a compliance and governance tool.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0002]** The disclosure is better understood with reference to the following drawings. The elements of the drawings are not necessarily to scale relative to each other. Rather, emphasis has instead been placed upon clearly illustrating the claimed subject matter. Furthermore, like reference numerals designate corresponding similar parts through the several views.

Fig. 1 is an example cloud system incorporating a SIEM Manager for multiple applications having an extended application command set;

Fig. 2 is another example cloud system incorporating a SIEM Manager with at least one application modified with an extended application command set;

Fig. 3 is a table of an example extended application command set;

Fig. 4 is a table with an example format of event log elements, descriptions and units returned by an application as a set of three indexed arrays;

Fig. 5 is a table of an example format of event log elements and their respective privacy and key rotation options to be sent to an application as a set of four indexed arrays;

Fig. 6 is a table of various example privacy options;

Fig. 7 is a table of various example key usage or key rotation options;

Fig. 8 is an example operational methodology for configuring an application's event log options and interacting with a SIEM manager;

Fig. 9 is an example flowchart of implementing an extended application command set;

Fig. 10 is an example computer system with computer readable memory executable by a processor to implement an application having an extended application command set; and

Fig. 11 is an example non-transitory computer readable medium to allow for client control of application log data.

## DETAILED DESCRIPTION

**[0003]** Today, both government and commercial organizations make use of internal and third party SIEM tools to monitor both their internal IT environments and application services for security and compliance with internal, industry, and government governance mandates (e.g. PCI DSS, HIPAA, etc.). There is a growing trend to migrate applications used by these organizations to cloud computing or to integrate with cloud computing services. Due to the use of these cloud computing and cloud services provided by third party vendors, the information collected by SIEM tools, particularly by the third parties, maybe out of the control of an organization, an application, or the application's user, herein collectively referred to herein in this description as a client.

**[0004]** These clients typically have no control over what a particular application logs or which client initiated events are collected and recorded regarding use of any particular application service. In fact, most applications are normally designed to log and record all details of a client's use in a monolithic fashion, no matter the identity of the client or what the client's desire may be regarding the retention of their application-use details.

**[0005]** This lack of control over the content of application logs and audit information may be less problematic in an IT setting in which the client and the applications are both owned by the same organization as access to the application logs can be restricted by the organization. However, this lack of control may become a significant issue in cloud environments where the owner/provider of the cloud environment controls the SIEM tools and thusly any collected application audit log information may be assembled, aggregated, and moved into other network domains not under the control of the client organization. This lack of client control may actually become a business-related issue for the cloud provider as not allowing client control over the disclosure of its use details in the application event log files may become a factor for a particular client in deciding whether or not to use

particular cloud applications or services of the cloud provider.

**[0006]** Fig. 1 is an example cloud-based environment 100 with a SIEM manager 130. A client may connect one or more computing devices to a cloud service 120. Such computing devices include handheld devices 110, such as cellphones, PDA, tablets and the like, portable computers 112, such as laptops, notebooks, convertibles, hybrids, portable workstations, etc., personal computers 116, such as desktops PCs, all-in-ones, workstations, personal servers, etc., and tablet-like devices 118, such as iPads™, tablet entry devices, etc. While these computing devices may run applications directly on their host machines, it is increasingly becoming common practice among organizations to use web-based or cloud-based applications that are accessed by the client devices. For instance, the cloud service 120 may host one or more multi-user applications 114 in a set of one or more real or virtual servers 126, or multiple single-user applications 114' running on separate real or virtual servers 126, which may be connected to common databases, file storage, or other data management systems. Each of the multi-user applications 114 and multiple single user applications 114' create log event data based on the use of the application by the client computing device. Also, each of the multi-user applications 114 or single user applications 114' may include an extended application command set 124 as will be explained in more detail below.

**[0007]** SIEM systems typically rely on an object known as a collector 128 (or alternatively connector) to both interpret and collect specific data from an application log file. A common example for creating application log file data is "Syslog" which is widely used in computing as a standard for message logging. Syslog permits separation of the software that generates messages, the system that stores them, and the software, such as SIEM tools, that reports and analyzes them. It is the connector 128 that determines what is collected out of the application log file. A client interacting with an application, whose actions are generating detailed information that is placed in the event log file, typically has no control over this unilateral action by the connector (or

the application that deposits the information regarding client activity in the application event log file) 128. Connectors 128 are generally available for many classes of computer software that can generate event log files including operating systems and databases, web servers, and web-based applications along with client identity management solutions. There are also connectors 128 for network devices, such as routers and switches, as well as network analyzers including net flow data and traffic analyzers. For security solutions, connectors 128 are available for intrusion prevention/detection systems (IPS/IDS), firewalls, virtual private networks (VPNs), and vulnerability scanners as well. While in the abstract connectors from each SIEM product (e.g. HP ArcSight™, RSA envision™, etc.) work similarly; their actual implementation architecture may vary.

**[0008]** Once event log data is obtained by the SIEM manager 130, the SIEM manager 130 may forward the event log data to other applications, or merge it with other event log data from other applications. Typically, the SIEM manager 130 will have a management console graphical user interface (GUI) 132 to help view and inspect the log event data collected. The client entity has no guarantees that any log information revealing details regarding what it did with the application will be kept private in the environment of cloud service 120. This lack of control may be an issue given various new governance regulations relating to privacy, healthcare, or financial services. Because of the legal need to meet these regulations, a client's inability to control what event log data is collected and recorded when it interacts with an application may be a large impediment to having the client choose to make use of an application or services of the cloud organization.

**[0009]** For instance, there are various Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPPA), and Payment Card Industry Data Security Standard (PCI DSS) requirements for monitoring and reporting data movement under the control of the client organization. Accordingly, a client organization may desire to keep such or other information of how it uses an application (and the data it provides the

application) private. A client organization may only choose to utilize applications of a cloud provider that give the client absolute control over what is written to the application event log file regarding its activities. At the same time, clients are under pressure to reduce costs by outsourcing much of their IT infrastructure and applications to cloud service providers in order to enhance revenue and also to increase productivity and uptime by having 24 hour support and IT redundancy in case of failures. Further, the cloud service providers need access to the event log data to meet their own regulatory and security requirements and are thus typically unwilling not to be allowed or permitted to collect event log data the client creates. Accordingly, there is a tension and conflict between clients and cloud service providers regarding the logging of application event log data that may be impeding the growth and expansion of cloud services.

**[0010]** To help solve this dilemma, a new paradigm has been created to facilitate awareness of a client to understand the totality of what an application 114, 114' can log regarding its activities and then allow the client to specify to the application 114, 114' both a) what it will allow the application 114, 114' to record regarding its activities and b) the privacy preferences for those pieces of recorded information it allows the application to collect.

**[0011]** Applications 114, 114' generally support a communication protocol and command set for interacting with client applications. The command set is transported via the communication protocol and any data exchanged may be encoded in eXtensible Markup Language (XML), Hyper-text Mark-up Language (HTML), JavaScript Object Notation (JSON), or other such data-exchange formats. Common communication protocols and command sets include Simple Object Access Protocol (SOAP), REpresentational State Transfer (REST), Web Services Description Language (WSDL), Highway Addressable Remote Transducer (HART), and Universal Description, Discovery and Integration (UDDI), just to name a few. Depending on the communication protocol used, the command set is expanded with a set of extended application commands (EAC) 124 to support a new command that

will allow a client to request the types of information being collected and recorded to the application event log file.

**[0012]** Also, an additional new command is available that allows a client to inform the application which of the application event log file elements it will allow the application 114, 114' to record regarding its activities. In addition, for each of application event log file content items that are permitted to be collected and recorded, the client is able to specify the privacy requirements of collected elements. Specifically, the client can specify whether the collected item should be not encrypted, encrypted by the application only, or encrypted by both the client and the application. This last encryption option creates a dual control paradigm for the application event log content item allowing both the client and cloud service provider to restrict access to the viewing of the client's recorded event log data. For ease of understanding, application 114 used henceforth will include both multiuser applications 114 and single user applications 114'.

**[0013]** Fig. 2 is an example cloud-based system 102 that includes a first set of processors 126 configured to execute an application 114 from computer readable memory 101 coupled to the first set of processors 126 wherein the application 114 includes a set of extended application commands (EAC) 124 to:

- a. inform a client of the types of event data the application 114 records to its application log file 190 (Obtain audit log info 142), and
- b. allow the client to inform the application 114 which of the available event log elements are permitted to be recorded to the application log file 190 of the application 114, wherein the set of EAC 124 is further to c) allow the client to obtain at least partial control of cryptographic keys 192 utilized to secure the elements of the application log file 190 that are related to the client activity with the application 114 (Specify audit log to report along with privacy mode 144).

**[0014]** A second set of processors 127, coupled to cloud service 120 and first set of processors 126, is configured to execute a security and information event management application 130 to incrementally receive the contents of the application log file 190 of the application 114.

**[0015]** The table 140 in Fig. 3 is one example of a set of expanded commands 124 that could be used over a protocol by the application 114. Other names and formats for the commands are possible, as well as the addition of additional extended commands. Further the two example commands listed may be combined into a single command structure. There are several ways of implementing an extended command set as known by those of skill in the art. The following description of expanded application commands (EAC) 124 is for illustration purposes and not meant to be limiting.

**[0016]** The GET\_LOG\_CONTENT command provides the application event log content definition which may be an array or stream of content item names, item descriptions, and item units. Each of these three item elements, name, description, and unit may be returned in a format that is readily parsable, typically an array, for every item that can be recorded in the application's event log file. Accordingly, the GET\_LOG\_CONTENT command may return the event log content in a manner that may be easily parsed for review by the client.

**[0017]** One example format for the GET\_LOG\_CONTENT command is illustrated in the table 150 of Fig. 4. In this example, the application returns the event log content in three arrays, where an index I may be used to access array content for the first event log content item (index 0) to the last (index N). For instance, the first element in the array indexed by I may contain the element name, the second array first element, the description corresponding to the first element name, and the third array first element, the element unit corresponding to the first element name, and continuing on for each successive I index. Because interpretation of particular application event log data elements can be quite difficult to decipher and understand, it is likely that

knowledgeable client users will need to review the returned event log content. However, this review of the returned event log content can be hastened by having an application log graphical user interface (GUI) displaying the responses of the application to the expanded commands to help the knowledgeable application user understand and determine which particular log event item information relating to the client's activity will be allowed or permitted to be recorded in the application's event log file. In some examples, the inclusion of natural language processing can be done to assist in cataloging or prioritizing the various event log items.

**[0018]** The SET\_LOG\_CONTENT command from the table 140 in Fig. 3 allows the client to return two additional pieces of information back to the application in addition to the event element name. The first additional item is the privacy control desired and the second additional item is the associated cryptographic key management details, such as key rotation modes, that may be specified.

**[0019]** An example format for the SET\_LOG\_CONTENT command is illustrated in table 160 of Fig. 5 and depicts how the client specifies back to the application event log elements it desires to be written to the application log file and their privacy and key rotation modes. In this example, four arrays are returned to the application, each indexed respectively by index I. The first array references the event log element name such as any of the event log element names of Fig. 4. The second array references whether the particular log element named in the first array is to be output, such as by a 'y/n' indication. If the second array has a 'y', the third and fourth arrays are completed, otherwise if 'n' they can be left to default values or nulled as they have no application when event data elements are not to be output. Alternatively, the application may decide not to examine and process the third and fourth array entries for an index I when the second array has a value of 'n'. The third array specifies the respective privacy option for the named element in the first array, which is described for one example in Fig. 6. The fourth array specifies the respective key rotation option for the named element

in the first array, which is described for one example in Fig. 7.

**[0020]** Fig. 6 is a table 170 that summarizes the four example privacy options available to the client for event log data it selects to have output to the application event log file. These options include:

- a. no preference
- b. do not encrypt
- c. encrypt using a cryptographic key in sole control of the application
- d. encrypt using dual control cryptographic keys.

The no preference option implies that the default application security policy will be utilized. The dual control cryptographic encryption option may use a symmetric key that is first encrypted with a public key of the client and then the public key of the application 114 to create a double encrypted symmetric key. In order for the log element to be revealed, the application 114 first decrypts the double encrypted symmetric key with its private key, then passes the once decrypted symmetric key to the client, which will then decrypt the already once decrypted symmetric key entity with its private key; thereby, revealing an unencrypted symmetric key that can decrypt the event log element of interest. The SIEM Manager 130 may be given custody of the key by the application using the application's private key to decrypt the twice encrypted key and then communicating the once decrypted symmetric key to the SIEM manager over a secure channel. Once in the SIEM manager custody, the SIEM manager could encrypt the key with its public key. When the SIEM manager needs to access data protected with the doubly encrypted symmetric key, the SIEM manager must decrypt the key with its private key, then provide the once decrypted symmetric key to the client over a secure channel, where the client may decrypt it using the client's private key. It could then send the doubly decrypted symmetric key back to the SIEM manager over a secure channel. After the SIEM manager utilized the key it may keep it cached for a limited amount of time for further use. Once the time limit

expires the decrypted key should be destroyed.

**[0021]** Fig. 7 is a table 180 reflecting various example options for symmetric key rotation for each element name specified. Although asymmetric key cryptography may be used, symmetric key cryptography is computationally more efficient than dual asymmetric key cryptography. Accordingly, in some examples a symmetric key may be utilized to encrypt a log file element. In addition, the application may be directed on how often to use a symmetric key. The key rotation options shown in the table of Fig. 7 include generating:

- a. a new symmetric key for every log file element output (use per element);
- b. a same symmetric key for all elements output that have the same time stamp (use per set); and
- c. a symmetric key based on application defaults. This third option is 'no preference', which allows the application to use its default setting.

**[0022]** Fig. 8 is an example operational setting 104 with an application 114 communicating event log data 152 to a SIEM manager 130 via a connector 128. Log content management of the SIEM manager 130 is controlled by a client with a management console GUI interface 132. Before a client can utilize the application 114, it requests the GET\_LOG\_CONTENT information using EAC extensions 124 from the application 114 and may assist client users to interpret the application response leveraging an application log GUI interface 148. In other examples, the interaction with the application 114 may take place in a command line session, a custom program, or other programmable interface in place or in addition to the application log GUI interface 148.

**[0023]** The event log content items (see Fig. 4) are loaded into the application log GUI interface 148 to allow a client user to examine and specify which log content items it will allow the application 114 to record with the application logger 115 regarding the client's activity with the application 114.

Further, for each item that will be permitted to be written to the application log file, the respective privacy mode and respective symmetric cryptographic key rotation schedule is specified. This selected information is submitted back to the application 114 using the SET\_LOG\_CONTENT command.

**[0024]** The communication interactions between the client and the application 114 may leverage Transport Layer Security (TLS) session security 146 or other web security protocol with both the application log GUI 148 and the application 114 authentication enabled. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. While use of TLS 146 protects the content of the communications between the application log GUI 148 and the application 114, it also enables the application 114 to definitively know who is making the GET/SET log content requests. The application 114 can build a database of each client's event log file content preferences and tie that information to a client's X.509 certificate that is exchanged in the TLS146 transaction. When communicating a dual controlled key to the SIEM manager 130, the application 114 would use its private key to first decrypt the twice encrypted symmetric key. At this point the symmetric key would still be encrypted with the client's public key. This still once encrypted symmetric key would be securely transported to the SIEM manager 130, where it would use its public key to re-encrypt the once doubly encrypted key. When the SIEM manager needs to access data under dual control it must send a request to the client that has part of the control. The request would accompany the symmetric key, now once decrypted with the private key of the SIEM manager and awaiting decryption by the client private key. Once received, the client would need to decrypt the key, then send it back to the SIEM manager using a secure protocol.

**[0025]** Once the application log GUI 148 receives an acknowledgement that the SET\_LOG\_CONTENT command has been properly processed by the application 114, the client may begin to use the application 114 as normally done, now being confident that the client's event log element preferences will

be properly carried out. As the application 114 continues to function and log events as event log data 152, they are captured by the connector 128, which may be a custom connector for the application 114 or a connector device, which receives application log data 154 from several applications. The connector 128 helps to capture, sort and preprocess log data 156 before sending to the SIEM Manager 130.

**[0026]** Fig. 9 is an example flowchart 200 of a process to implement a set of extended application commands to support client control of application log content. For instance, in block 202, a first command is received by the application to provide event log content definition from the application to the client. In block 204, a set of content item names, content item descriptions, and content item units are returned to the client from the application. In block 206, the application receives a second command that informs the application which event log content items are to be collected and recorded along with a respective privacy setting for each event log content item to be collected. Block 208 enables the event log content items to be recorded in the application log file 190 along with its respective privacy mode setting.

**[0027]** Other possible steps of the process 200 include receiving a respective key rotation schedule for each of the event log content items that are to be collected and recorded along with the second command. The key rotation schedule may include a request to use a same symmetric key for every event log item with the same time stamp or a request to use a different symmetric key for each of the event log content items. Another option for the key rotation schedule would be to let the application use its default key rotation setting. A further step of process 200 may encompass wherein after enabling the event log content items, an acknowledgement is returned signifying the application 114 can be used with the requested event logging enabled.

**[0028]** Fig. 10 is an example computer system 300 that includes a processor 302 coupled to non-transitory computer readable memory 308. The processor 302 can execute computer readable instructions and read/write

data stored on the non-transitory computer readable memory 308. The non-transitory computer readable memory also includes non-transitory storage 304 which is accessible by the processor 302 via memory controller 306 and network interface 316 in some examples. In other examples, the processor 302 may access storage 304 using memory controller 306 and input/output (I/O) controller 312 and either Universal Serial Bus (USB) ports 322 or Advanced Technology Attachment (ATA) ports 324 or both. Of course, other disc or storage interfaces such as SATA (Serial ATA), SCSI (Small Computer System Interface), and SAS (Serial Attached SCSI) can be used as well. Memory controller 306 is attached to a graphics system 318 to allow for viewing output from the computer system 300. The non-transitory computer readable memory 308 may include the application software code 310, the extended application command code (EAC) 320 to implement EAC 124. The EAC 320 code can include commands to extend the application command set such as a first command to obtain audit log info 330, and a second command to specify what audit log info to report 340. The extended application commands can also be expanded to accommodate dual key management 342, such as for encryption of selected event log contents with an application generated symmetric key. To protect the application's 114 symmetric key and facilitate dual control, the application would receive the client's public key (for instance in the client's X.509 certificate) and use it to encrypt the symmetric key; then use its own public key to encrypt the once encrypted symmetric key. The storage 304 can be used to store the encrypted symmetric cryptographic keys 192 and any application log files 190.

**[0029]** Fig. 11 is an example non-transitory computer readable medium 106 to allow for client control of application log data. The non-transitory computer readable medium 106 includes instructions 122 which when executed by a processor 126 from computer readable memory 308 cause the processor 126 to obtain audit log information 143 from an application 114. The instructions also allow the processor 126 to control 145 which audit log information from the application 114 is reported to a log file 190 of the application 114. Further instructions allow the processor 126 to obtain partial cryptographic key control

147 of a set of cryptographic keys 192 utilized to secure at least a part of an audit log record in the log file 190 of the application 114.

**[0030]** Fig 11 may be implemented in a cloud-based system 120 to allow for client control of application 114 log content. The processor 126 may include one or more of a first set of physical or virtual processors coupled to the computer readable memory 308. The processor 126 may be configured to execute the application 114 from the computer readable memory 308 wherein the application 114 includes a protocol and command set with a set of extended application commands 124. The protocol and command set may allow the application 114 to inform a client using the application 114 which available event contents of the application are recordable to an application log file 190. By this command, the client may obtain audit log information 143. The protocol and command set may also allow the client to inform the application 114 which of the available event contents are allowed or permitted to be recorded to the application log file 190 of the application. This command enables the processor 126 to control audit log information to be reported to the log file 145. To help secure the available event contents of the application log file 190, the protocol and command set may allow the client to obtain partial control of cryptographic keys 192 to secure at least part of the application log file 190 of the application 114. By this command, the client is thus able to obtain partial cryptographic control 147 to secure part of audit log record in the log file 190

**[0031]** While the claimed subject matter has been particularly shown and described with reference to the foregoing examples, those skilled in the art will understand that many variations may be made therein without departing from the intended scope of subject matter in the following claims. This description should be understood to include all novel and non-obvious combinations of elements described herein, and claims may be presented in this or a later application to any novel and non-obvious combination of these elements. The foregoing examples are illustrative, and no single feature or element is essential to all possible combinations that may be claimed in this or a later

application. Where the claims recite “a” or “a first” element of the equivalent thereof, such claims should be understood to include incorporation of one or more such elements, neither requiring nor excluding two or more such elements.

What is claimed is:

## CLAIMS

1. A method to support client control of application log content, comprising:
  - receiving a first command to provide event log content definition for an application;
  - returning a set of event log content items including content item names, content item descriptions, and content item units for the application for the event log content definition;
  - receiving a second command to inform the application which event log content items are to be recorded, and to specify a respective privacy mode for each of the event log content items that are to be recorded; and
  - enabling the event log content items that are to be recorded in the application log file along with their respective privacy mode.
2. The method of claim 1 wherein the second command includes specifying a respective key rotation schedule for each of the event log content items that are to be recorded.
3. The method of claim 1 wherein the second command includes specifying a same symmetric key for every event log content with the same time stamp.

.
4. The method of claim 1 wherein the second command includes specifying a different symmetric key for each of the event log content items.
5. The method of claim 1 wherein after enabling the event log content items, an acknowledgement is returned signifying the application can be used.

6. A non-transitory computer readable medium comprising instructions which when executed by a processor from computer readable memory cause the processor to:

obtain audit log information from an application;

control which audit log information from the application is reported to a log file of the application; and

obtain partial cryptographic key control of a set of cryptographic keys utilized to secure at least a part of an audit log record in the log file of the application.

7. The non-transitory computer readable medium of claim 6 further comprising instructions to establish a dual control paradigm for the application and a client using the application.

8. The non-transitory computer readable medium of claim 7 wherein the dual control paradigm includes dual control of the symmetric cryptographic key used to protect selected application log content, first using a dual asymmetric public key of the client to create a once encrypted symmetric key, then using a dual asymmetric public key of the application to further encrypt the once encrypted symmetric key.

9. The non-transitory computer readable medium of claim 6 further comprising instructions to transmit the log file of the application to a security information event management tool.

10. The non-transitory computer readable medium of claim 6 further comprising instructions to support a protocol and command set for allowing interaction with the application to obtain the audit log information and to control which audit log information from the application is to be reported to the log file of the application.

11. A cloud-based system to allow for control of log content of an application, comprising:

computer readable memory; and

a first set of processors coupled to the computer readable memory, the first set of processors configured to execute the application from the computer readable memory wherein the application comprises an extended application command set to:

a) inform a client which available event contents of the application are recordable to an application log file, and

b) allow the client to inform the application which of the available event contents are permitted to be recorded to the application log file of the application, and

c) allow the client to obtain at least partial cryptographic key control to secure at least part of the application log file of the application when collected by a security and information event (SIEM) tool.

12. The cloud based system of claim 11, wherein the cryptographic keys are a symmetric key used to encrypt selected event log data and a set of dual asymmetric public keys to protect the symmetric key, one in control of the application and the other in control of the client.

13. The cloud based system of claim 11, wherein the first set of processors includes a graphical user interface to assist client users in understanding information responses from the extended application command set.

14. The cloud based system of claim 11, wherein interaction between the client and the application uses Transport Layer Security with a X.509 certificate of the client, and wherein the application log file of the application ties the X.509 certificate of the client to the available event contents of the application to be recorded by the SIEM tool.

15. The cloud based system of claim 11, further comprising:
- a second computer readable memory; and
  - a second set of processors coupled to the second computer readable memory and configured to execute the SIEM tool from the second computer readable memory to receive and record the application log file of the application.

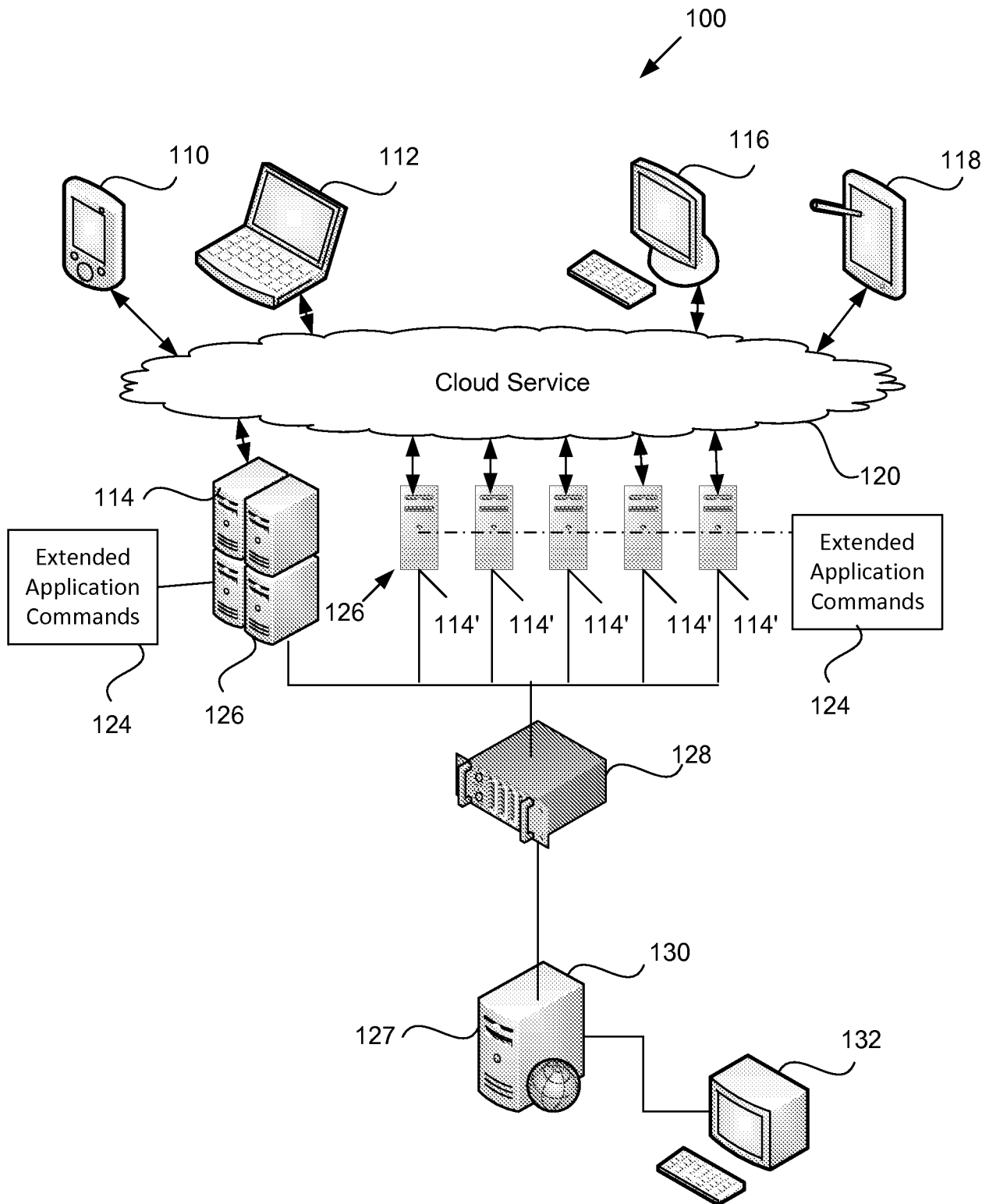


Fig. 1

2/7

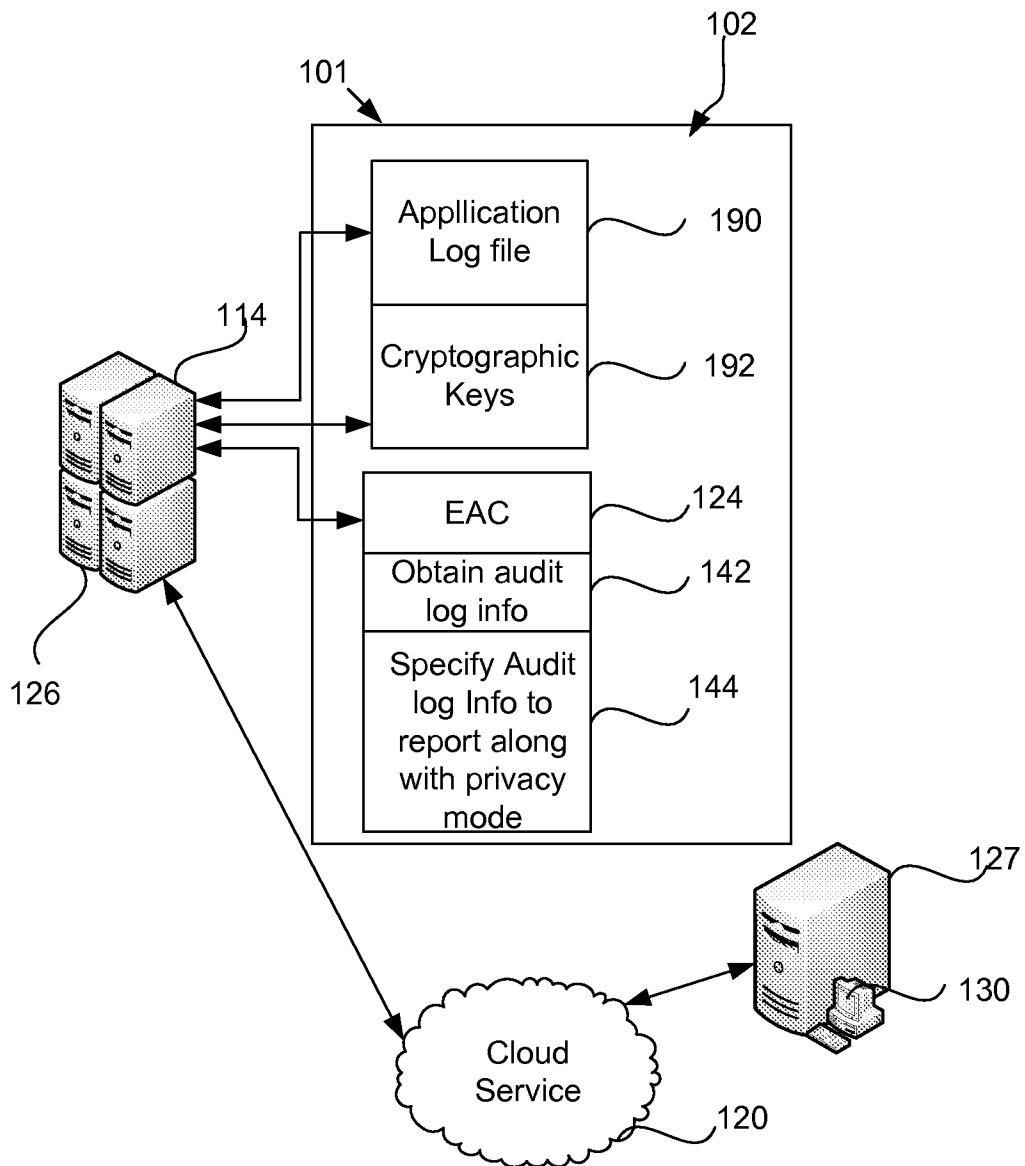


Fig. 2

140

| Command ID of Extended Application Commands (EAC) | Command Name    | Description                                                                                                                                                                                        | Result                                                                                                                                                                      | Format                                                                                                                                                             | Notes                                        |
|---------------------------------------------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| EAC_001                                           | GET_LOG_CONTENT | Provide Application event log content definition                                                                                                                                                   | Return arrays with content item name, item description, and item units                                                                                                      | Item name, Item description, Item Units returned for every Item that can be recorded in log file                                                                   | Client sends this request to the Application |
| EAC_002                                           | SET_LOG_CONTENT | Inform the Application which Application event log content items may be recorded regarding the client's activity with the Application, also specify their privacy modes, and key rotation schedule | Application disables recording client specified event log items in its event log file, sets privacy modes, and key rotation schedule for elements to be written to log file | For each event element that can be recorded in the log file - an indication of which elements are to be written out, their privacy mode, and key rotation schedule | Client sends this request to the Application |

Fig. 3

150

| Array of Event Log Element Names | Array of Event Log Element Descriptions | Array of Event Log Units |
|----------------------------------|-----------------------------------------|--------------------------|
| [0] <1st element name>           | [0] <text description of 1st element>   | [0]<first element units> |
| [1]<2nd element name>            | [1] <text description of 2nd element>   | [1] <2nd element units>  |
| ...                              | ...                                     | ...                      |
| [N]<last element name>           | [N]<text description of last element>   | [N]<lasat element units> |

Fig. 4

4/7

160

| Array: Event Log Element Name       | Array: Is Log Element to be written? [y/n] | Array: Privacy Constraints | Array: Key Rotation Schedule |
|-------------------------------------|--------------------------------------------|----------------------------|------------------------------|
| [0] <name_1st_element_in- log_file> | [0] <y/n>                                  | [0] <privacy-option>       | [0] <rotation option>        |
| [1] <name_2nd_element in log_file>  | [1] <y/n>                                  | [1] <privacy_option>       | [1] <rotation option>        |
| ...                                 | ...                                        | ...                        | ...                          |

Fig. 5

170

| Privacy Option      | Description                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------|
| Do not encrypt      | Do not encrypt the log element                                                               |
| No preference       | Application uses its default setting                                                         |
| Application Control | Uses a cryptographic key in control of the application only                                  |
| Dual Control        | Uses two cryptographic keys, one in control of the Application, one in control of the Client |

Fig. 6

180

| Key Usage Options | Description                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------|
| No preference     | Use the Application default setting for symmetric key rotation on log file element          |
| Use per set       | Use the same symmetric key for every log field element with the same time stamp             |
| Use per element   | Use a new symmetric key on each element written to log file (even with the same time stamp) |

Fig. 7

5/7

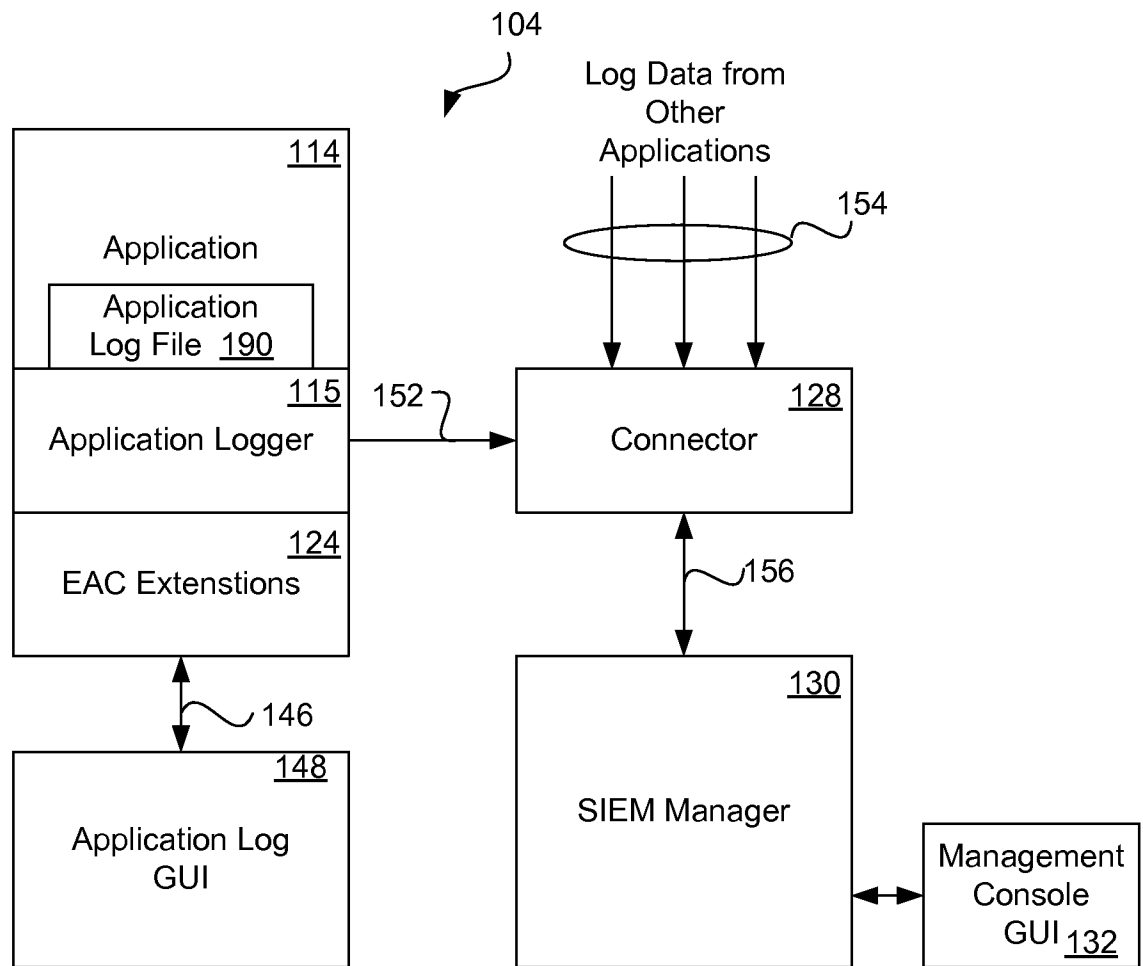


Fig. 8

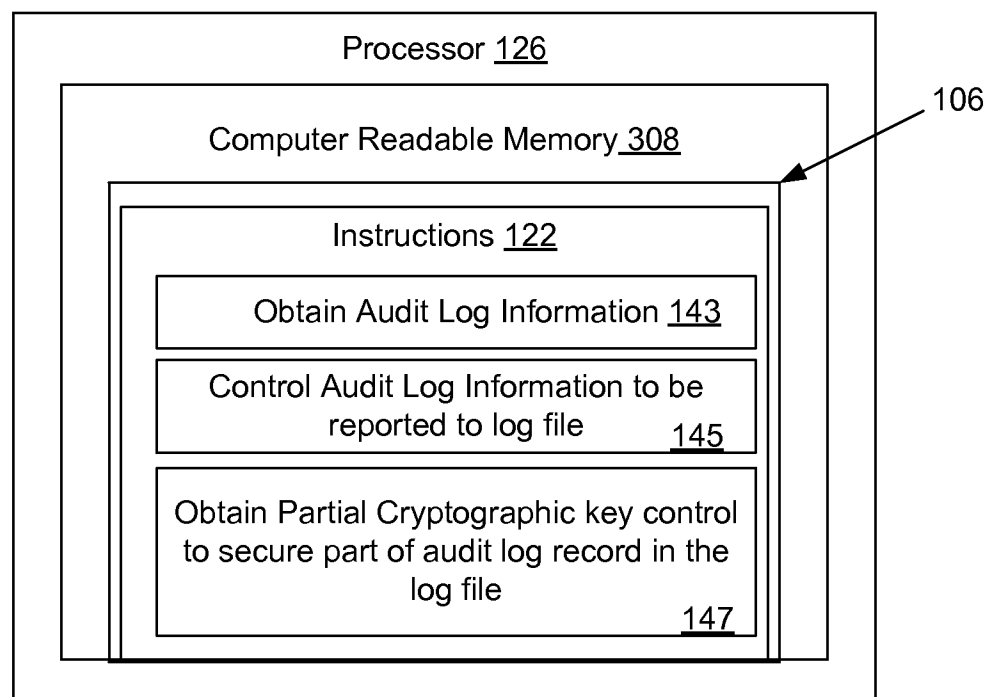


Fig. 11

6/7

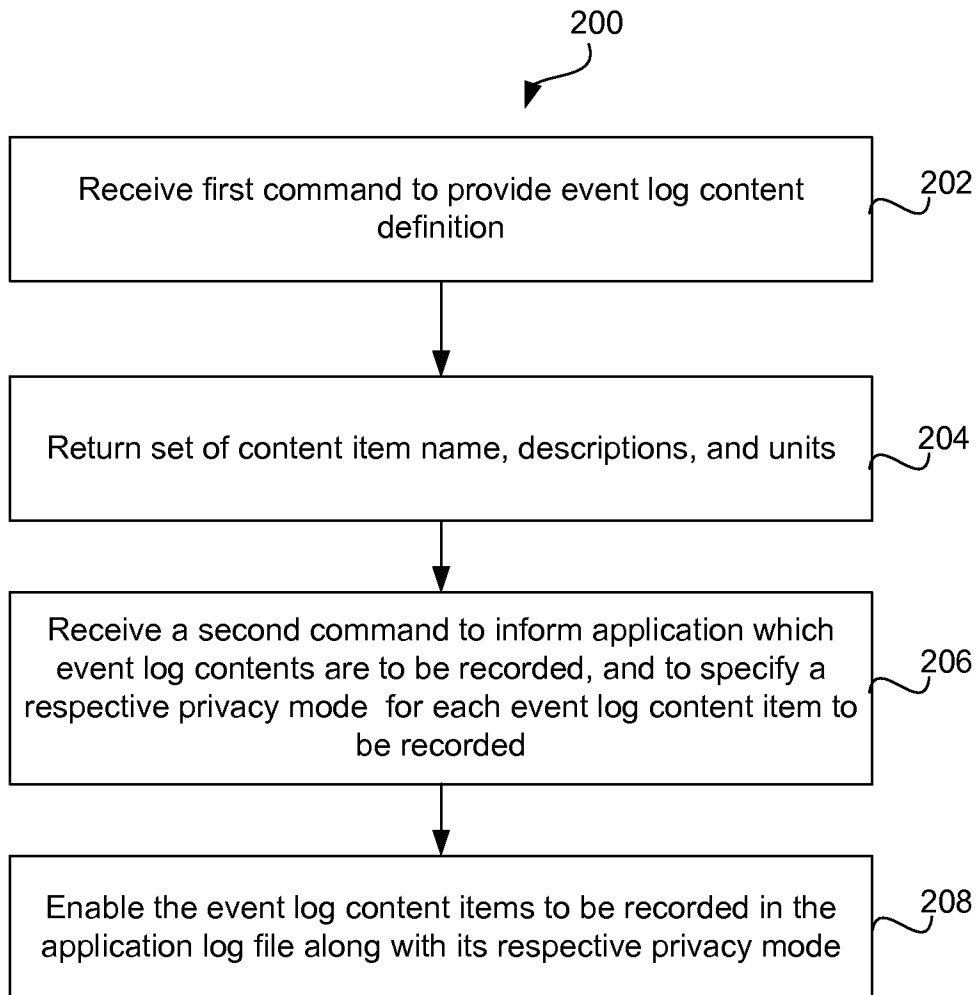


Fig. 9

7/7

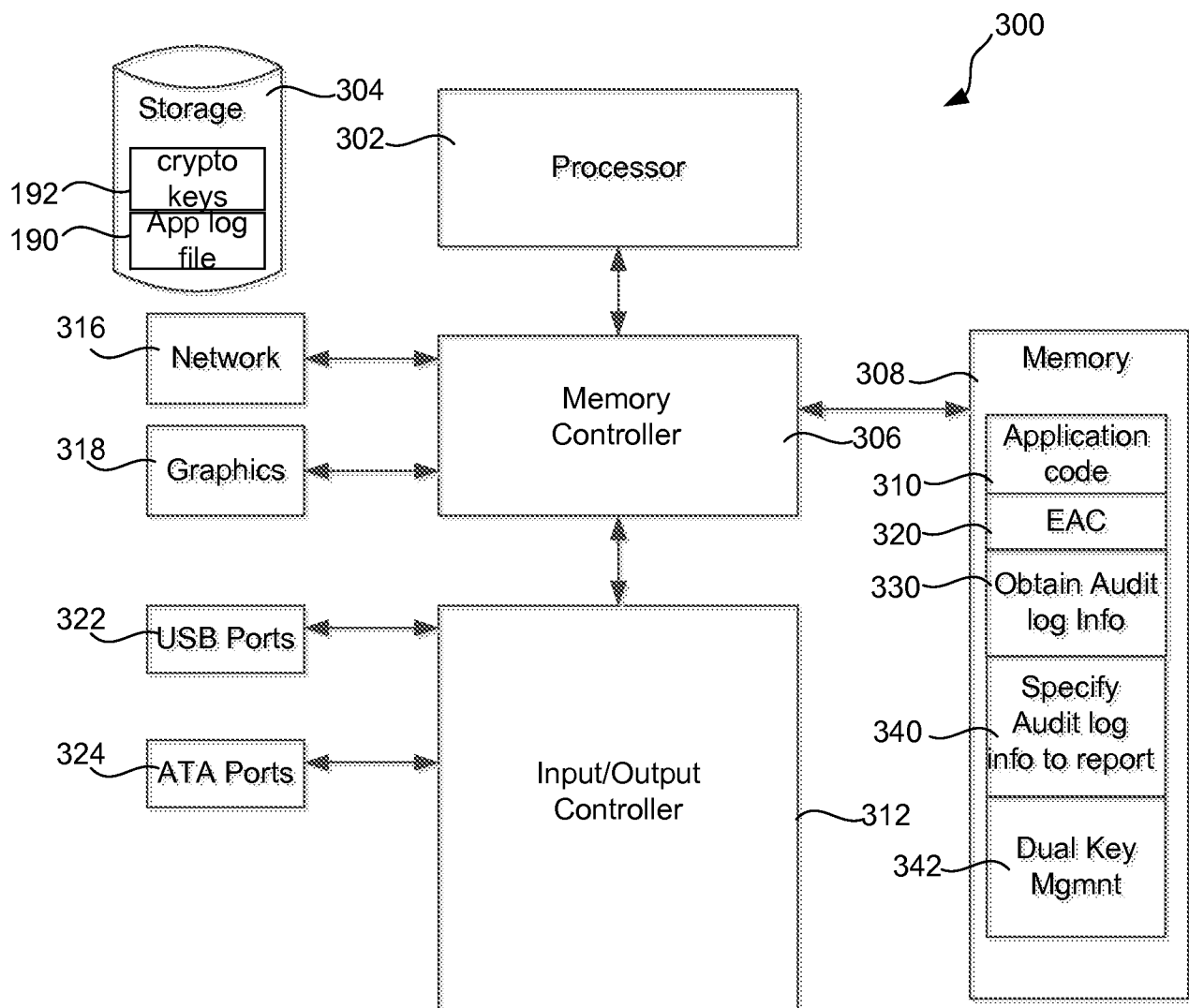


Fig. 10

## INTERNATIONAL SEARCH REPORT

International application No.  
**PCT/US2015/036901****A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/10(2013.01)i, G06F 9/44(2006.01)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 21/10; G06F 9/54; G06F 15/16; H04L 9/08; G06F 11/30; G06F 17/30; G06F 21/00; G06F 11/00; G06F 9/44

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) &amp; keywords: client control, cloud, application log content, record, privacy mode

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                              | Relevant to claim No. |
|-----------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | US 2013-0125143 A1 (KATSURO KIKUCHI et al.) 16 May 2013<br>See paragraphs [0044]-[0054], [0103]; claim 1; and figures 1A-1D.    | 11-15                 |
| Y         |                                                                                                                                 | 1-10                  |
| Y         | US 2014-0109188 A1 (VLADIMIR PAVLOV et al.) 17 April 2014<br>See paragraphs [0019]-[0025]; claim 1; and figure 2.               | 1-10                  |
| A         | US 2007-0271273 A1 (RYAN K. CRADICK et al.) 22 November 2007<br>See paragraphs [0018]-[0026]; claim 1; and figure 1.            | 1-15                  |
| A         | US 2014-0019753 A1 (JOHN HOUSTON LOWRY et al.) 16 January 2014<br>See paragraphs [0062]-[0071]; claims 1-12; and figures 2A-2D. | 1-15                  |
| A         | US 7502972 B1 (SAMPATH KUMAR CHILUKURI et al.) 10 March 2009<br>See column 4, lines 1-19; and figure 1.                         | 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

16 March 2016 (16.03.2016)

Date of mailing of the international search report

**17 March 2016 (17.03.2016)**

Name and mailing address of the ISA/KR

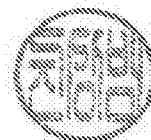
International Application Division  
Korean Intellectual Property Office  
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 35208,  
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

CHIN, Sang Bum

Telephone No. +82-42-481-8398



**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2015/036901**

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s)                                               | Publication<br>date                                  |
|-------------------------------------------|---------------------|--------------------------------------------------------------------------|------------------------------------------------------|
| US 2013-0125143 A1                        | 16/05/2013          | JP 05325177 B2<br>JP 2012-038142 A<br>US 8966502 B2<br>WO 2012-020512 A1 | 23/10/2013<br>23/02/2012<br>24/02/2015<br>16/02/2012 |
| US 2014-0109188 A1                        | 17/04/2014          | None                                                                     |                                                      |
| US 2007-0271273 A1                        | 22/11/2007          | US 7805675 B2                                                            | 28/09/2010                                           |
| US 2014-0019753 A1                        | 16/01/2014          | EP 2873189 A1<br>WO 2014-011313 A1                                       | 20/05/2015<br>16/01/2014                             |
| US 7502972 B1                             | 10/03/2009          | None                                                                     |                                                      |