



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/US2016/015834
- (22) **International Filing Date:**
29 January 2016 (29.01.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** ENTIT SOFTWARE LLC [US/US]; 1140 Enterprise Way, Building G, Sunnyvale, CA 94089 (US).
- (72) **Inventors:** SPIES, Terence; 20400 Stevens Creek Blvd., Suite 500, Cupertino, California 95014 (US). SANDER, Tomas; 5 Vaughn Drive, Suite 301, Princeton, New Jersey 08540 (US). LANGFORD, Susan K; 1160 Enterprise Way, Sunnyvale, California 94089 (US).
- (74) **Agents:** LEE, Rachel Jeong-Eun et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, Colorado 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, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LI, 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:** ENCRYPTION OF COMMUNITY-BASED SECURITY INFORMATION

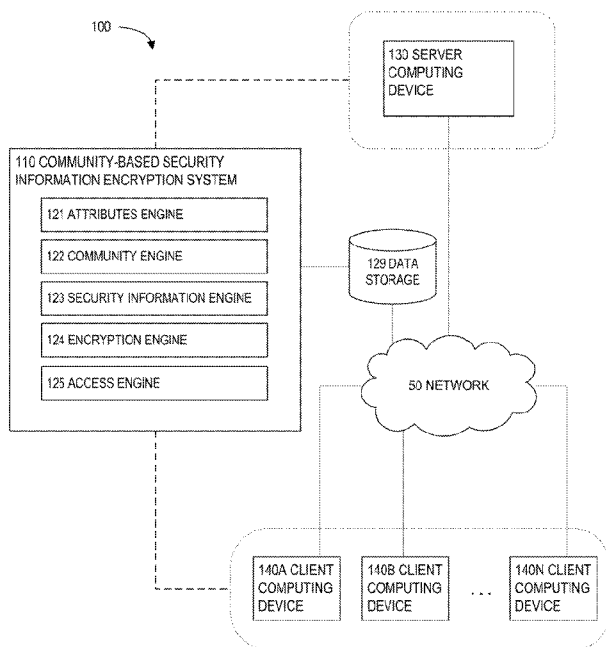


FIG. 1

- (57) **Abstract:** Examples disclosed herein relate to encryption of community-based security information. Some examples may enable authorizing a user of a community to access an encrypted data item (e.g., at least an encrypted portion of community-based security information of that community) using a decryption key. The community may be generated on a security information sharing platform based on a set of community attributes. The decryption key may comprise a private key corresponding to each user attribute of a set of user attributes that are associated with the authorized user where the set of user attributes satisfy the set of community attributes.

**Declarations under Rule 4.17:**

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

Published:

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

ENCRYPTION OF COMMUNITY-BASED SECURITY INFORMATION

BACKGROUND

[0001] Users of a security information sharing platform share security indicators, security alerts, and/or other security-related information (e.g., mitigations strategies, attackers, attack campaigns and trends, threat intelligence information, etc.) with other users in an effort to advise the other users of any security threats, or to gain information related to security threats from other users.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram depicting an example environment in which various examples may be implemented as a community-based security information encryption system.

[0004] FIG. 2 is a block diagram depicting an example community-based security information encryption system.

[0005] FIG. 3 is a block diagram depicting an example machine-readable storage medium comprising instructions executable by a processor for encrypting community-based security information.

[0006] FIG. 4 is a block diagram depicting an example machine-readable storage medium comprising instructions executable by a processor for encrypting community-based security information.

[0007] FIG. 5 is a flow diagram depicting an example method for encrypting community-based security information.

[0008] FIG. 6 is a flow diagram depicting an example method for encrypting community-based security information.

DETAILED DESCRIPTION

[0009] The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar parts. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only. While several examples are described in this document, modifications, adaptations, and other implementations are possible. Accordingly, the following detailed description does not limit the disclosed examples. Instead, the proper scope of the disclosed examples may be defined by the appended claims.

[0010] Users of a security information sharing platform share security indicators, security alerts, and/or other information (e.g., mitigations strategies, attackers, attack campaigns and trends, threat intelligence information, etc.) with other users in an effort to advise the other users of any security threats, or to gain information related to security threats from other users. The other users with whom the security information is shared typically belong to a community that is selected by the user for sharing, or to the same community as the user. The other users of such communities may further share the security information with further users and/or communities. A "security indicator," as used herein, may refer to a detection guidance for a security threat and/or vulnerability. In other words, the security indicator may specify what to detect or look for (e.g., an observable) and/or what it means if detected. For example, the security indicator may specify a certain Internet Protocol (IP) address to look for in the network traffic. The security indicator may include the information that the detection of that IP address in the network traffic can indicate a certain malicious security threat such as a Trojan virus.

[0011] A "user," as used herein, may include an individual, organization, or any entity that may send, receive, and/or share the security information. A community may include a plurality of users. For example, a community may include a plurality of individuals in a particular area of interest. A community may include a global community where any user may join, for example, via subscription. A community

may also be a vertical-based community. For example, a vertical-based community may be a healthcare or a financial community.

[0012] A community may also be a private community with a limited number of selected users. A private community may be defined by explicitly enumerating its members by, for example, selecting a particular set of users of the security information sharing platform. However, it is not an easy task to identify and/or add each individual user to be included if a large number of users were to be added to the community. Further, a community built based on enumerating individual community members usually comprises a close net of users who already know each other, which decreases a likelihood of receiving information that is not readily available to the users otherwise (e.g., information from other users outside of their existing network).

[0013] In some instances, community-based security information of the community may be encrypted to protect the community-based security information from compromise. The "community-based security information," as used herein, may refer to any security indicators, information related to those security indicators, information related to the community, or any other information originated from (and/or submitted to the community) by a user of that community. In this case, it may be technically challenging to enforce a security policy in such a way that the members of the community that are authorized to access the encrypted community-based security information are provided with a proper decryption key.

[0014] Examples disclosed herein provide technical solutions to these technical challenges by generating a community based on a particular set of community attributes that describe users to be included in the community, and authorizing a user of the community to access an encrypted portion of the community-based security information of that community using a decryption key. The decryption key may be generated using a private key corresponding to each user attribute of a set of user attributes associated with the authorized user, where the set of user attributes satisfy the set of community attributes. In this way, a community may be generated based on attributes characterizing its members rather than explicitly enumerating each

individual member. Further, the members of the community may be provided with a proper decryption key to be able to access the encrypted portion of the community-based security information of that community.

[0015] Some examples may enable authorizing a user of a community to access an encrypted data item (e.g., at least an encrypted portion of community-based security information of that community) using a decryption key. The community may be generated on a security information sharing platform based on a set of community attributes. The decryption key may comprise a private key corresponding to each user attribute of a set of user attributes that are associated with the authorized user where the set of user attributes satisfy the set of community attributes.

[0016] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting. As used herein, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. The term "plurality," as used herein, is defined as two or more than two. The term "another," as used herein, is defined as at least a second or more. The term "coupled," as used herein, is defined as connected, whether directly without any intervening elements or indirectly with at least one intervening elements, unless otherwise indicated. Two elements can be coupled mechanically, electrically, or communicatively linked through a communication channel, pathway, network, or system. The term "and/or" as used herein refers to and encompasses any and all possible combinations of one or more of the associated listed items. It will also be understood that, although the terms first, second, third, etc. may be used herein to describe various elements, these elements should not be limited by these terms, as these terms are only used to distinguish one element from another unless stated otherwise or the context indicates otherwise. As used herein, the term "includes" means includes but not limited to, the term "including" means including but not limited to. The term "based on" means based at least in part on.

[0017] FIG. 1 is an example environment 100 in which various examples may be implemented as a community-based security information encryption system 110. Environment 100 may include various components including server computing device 130 and client computing devices 140 (illustrated as 140A, 140B, ..., 140N). Each client computing device 140A, 140B, ..., 140N may communicate requests to and/or receive responses from server computing device 130. Server computing device 130 may receive and/or respond to requests from client computing devices 140. Client computing devices 140 may be any type of computing device providing a user interface through which a user can interact with a software application. For example, client computing devices 140 may include a laptop computing device, a desktop computing device, an all-in-one computing device, a tablet computing device, a mobile phone, an electronic book reader, a network-enabled appliance such as a "Smart" television, and/or other electronic device suitable for displaying a user interface and processing user interactions with the displayed interface. While server computing device 130 is depicted as a single computing device, server computing device 130 may include any number of integrated or distributed computing devices serving at least one software application for consumption by client computing devices 140.

[0018] The various components (e.g., components 129, 130, and/or 140) depicted in FIG. 1 may be coupled to at least one other component via a network 50. Network 50 may comprise any infrastructure or combination of infrastructures that enable electronic communication between the components. For example, network 50 may include at least one of the Internet, an intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a SAN (Storage Area Network), a MAN (Metropolitan Area Network), a wireless network, a cellular communications network, a Public Switched Telephone Network, and/or other network. According to various implementations, community-based security information encryption system 110 and the various components described herein may be implemented in hardware and/or a combination of hardware and programming that

configures hardware. Furthermore, in FIG. 1 and other Figures described herein, different numbers of components or entities than depicted may be used.

[0019] Community-based security information encryption system 110 may comprise an attributes engine 121, a community engine 122, a security information engine 123, an encryption engine 124, an access engine 125, and/or other engines. The term “engine”, as used herein, refers to a combination of hardware and programming that performs a designated function. As is illustrated respect to FIGS. 3-4, the hardware of each engine, for example, may include one or both of a processor and a machine-readable storage medium, while the programming is instructions or code stored on the machine-readable storage medium and executable by the processor to perform the designated function.

[0020] Attributes engine 121 may manage and/or store, in a database (e.g., data storage 129), various user attributes associated with a user of the security information sharing platform. As used herein, a “user attribute” may refer to a characteristic and/or property of the user with which the user attribute is associated.

[0021] Various user attributes associated with a user may comprise an attribute related: an industry sector of the user (e.g., a financial industry, healthcare industry, etc.), a geographical region of the user (e.g., a geographical region where the user is located in), an organization that the user belong to (e.g., a name, size, threat profile and/or any other information about the organization such as an employer, a standards organization, etc.), user reputations of the user (e.g., a user level or badge status of the user such as “Trusted User,” “Malware Expert Level V,” “Forensics Expert,” “High Performer,” etc.), a citizenship status of the user, an environmental condition (e.g., terrorist threat level of the geographical region of the user, etc.), an indication of whether the user represents a threat intelligence feed vendor, a security clearance level of the user, user status of the user in the security information sharing platform (e.g., paid subscription level to the security information sharing platform such as Silver status, Platinum status, Gold status, etc.), etc.

[0022] User attributes may be assigned to, therefore be associated with, a user in various ways. In one example, the user may specify a user attribute that describes that user by providing information to the security information sharing platform regarding the user's organization, geographical region, expertise, etc. In another example, a user attribute may be automatically extracted from a user profile of the user. A user profile may be created within the security information sharing platform for internal use. In some instances, a user profile that has been externally created may be imported into the security information sharing platform. User attributes included in the user profile may be extracted, parsed, and/or stored in a database (e.g., data storage 129). In yet another example, another user may be allowed to assign a user attribute to the user. In this example, a third-party user may be delegated an authority to assign a user attribute to the user (e.g., a reseller of a product may designate user attributes to its customers).

[0023] In some implementations, user attributes that are associated with a user may be hidden from the user. The security information sharing platform may store (e.g., in a data storage 129) a set of user attributes, a user identification of the user, and/or associations thereof, but it may be configured not to reveal the associations to the user.

[0024] In some implementations, a certain collection of user attributes may form a set of community attributes to be used to generate a particular community. "A set of community attributes," as used herein, may refer to a particular collection and/or assembly of user attributes that describe users to be included in a particular community. For example, a set of community attributes may be in form of monotonic expression. It may be expressed as: "Top 10 US Bank" AND "Security Clearance." Any users associated with a first user attribute (e.g., "TOP 10 US Bank") and a second user attribute (e.g., "Security Clearance") would satisfy this set of community attributes. Another example set of community attributes may comprise: ("Top 10 US Bank" AND "Security Clearance") OR "China". Note that a user that is not associated with the user attribute "China" may still satisfy this set of community attributes as long as the user is associated with "Top 10 US Bank" and

"Security Clearance." In some situations, a set of community attributes may be expressed in such a way that it includes a negation such as: ("Top 10 US Bank" AND "Security Clearance") NOT "Russia". In this case, a user that is associated with "Russia" may not satisfy the set of community attributes as defined.

[0025] In some implementations, the set of community attributes may be used as a name and/or label for the community being generated based on that set of community attributes. In this way, by simply looking at the name and/or label, the type of the community can be easily identified.

[0026] Community engine 122 may generate a community on the security information sharing platform. The generation of the community may be user-initiated or system-initiated. In some implementations, a user (e.g., a case initiator) may create the community by providing a list of users to be included in the community (e.g., explicitly enumerating a particular set of users). A user (e.g. a case initiator) may create a community in an implicit way by defining a set of community attributes characterizing its members/users rather than explicitly enumerating each individual member/user to be included. In this way, if a large number of users with a common set of characteristics were to be added to the community, it may be more effective to create a community based on a set of community attributes.

[0027] In some implementations, the security information sharing platform may automatically identify and/or invite users who might be interested in joining the community based on information that have been collected about users of the platform (e.g., the platform may automatically identify and/or invite users who have been under similar security threats in the past). In some instances, a set of community attributes (e.g., "Banks" AND "US") may be automatically determined based on a certain triggering event (e.g., a serious threat noticed in banks in US). In this case, users associated with a set of user attributes that would satisfy the set of community attributes may join the community (e.g., the community generated based on "Banks" AND "US").

[0028] In some implementations, once the set of community attributes are defined (e.g., whether user-initiated or system-initiated), community engine 122 may notify users associated with user attributes that would satisfy the set of community attributes. Users may be asked to confirm (e.g., accept or reject) the invitation to join the community.

[0029] In some implementations, an identification of one user of the community may be kept hidden from another user of the same community. The user may choose to voluntarily reveal the user's identity (e.g., add it to the community member list) or keep it anonymous.

[0030] Security information engine 123 may obtain a security indicator for the community (e.g., generated by community engine 122 as discussed herein). The security indicator may comprise at least one observable. A "security indicator," as used herein, may refer to a detection guidance for a security threat and/or vulnerability. In other words, the security indicator may specify what to detect or look for (e.g., an observable) and/or what it means if detected. For example, the security indicator may specify a certain Internet Protocol (IP) address to look for in the network traffic. The security indicator may include the information that the detection of that IP address in the network traffic can indicate a certain malicious security threat such as a Trojan virus. An "observable," as used herein, may refer to an event pertinent to the operation of computers and networks (e.g., an event occurring in network, servers, applications, databases, and/or various components of any computer system). Examples of an observable may include but are not limited to: an IP address, a domain name, an e-mail address, Uniform Resource Locator (URL), and a software file hash. A security indicator may comprise a single observable (e.g., "a new file is created by an executable") or a plurality of observables (e.g., "a new file is created by an executable and "the executable connects to domain X").

[0031] A security indicator may be created by and/or originated from at least one of a plurality of source entities. For example, the plurality of source entities may include a user. A security indicator may be manually created and/or added to the security information sharing platform (e.g., and/or to a particular community in the

platform) by the user. In another example, the plurality of source entities may include a threat intelligence provider that provides threat intelligence feeds. A security indicator that is found in the intelligence feeds, for example, may be created and/or added to the security information sharing platform (e.g., and/or to a particular community in the platform). There exist a number of providers of threat intelligence feeds. The threat intelligence feeds may be provided by independent third parties such as security service providers. These providers and/or sources may supply the threat intelligence feeds that provide information about threats the providers have identified. Most threat intelligence feeds, for example, include lists of domain names, IP addresses, and URLs that various providers have classified as malicious or at least suspicious according to different methods and criteria.

[0032] "Information" related to a security indicator, as used herein, may comprise information about: an investigation result that is provided by a user of the community, an indicator score for the security indicator, a source entity for the security indicator, a threat actor (e.g., attacker) for the security indicator, a level of confidence (e.g., the level of confidence that the indicator is actually malicious), a level of severity (e.g., the level of severity or likely impact that the indicator may pose), a sighting of an observable of the security indicator, and/or other information related to the security indicator.

[0033] In some implementations, security information engine 123 may obtain a security indicator for the community and/or include the security indicator (and/or information related to the security indicator) in community-based security information of that community. The "community-based security information," as used herein, may refer to any security indicators, information related to those security indicators, information related to the community, or any other information originated from (and/or submitted to the community) by a user of that community. For example, a user of the community may create and/or submit the security indicator to the community using the security information sharing platform. The user when creating the security indicator may specify some information related to the security indicator such as a level of confidence associated with the security indicator (e.g., the level of

confidence that the indicator is actually malicious) and/or a level of severity (e.g., likely impact) associated with the security indicator (e.g., the level of severity or likely impact that the indicator may pose), and/or other information the user is aware of about the security indicator.

[0034] In some implementations, security information engine 123 may provide the security indicator to the community to obtain additional information about the security indicator from the users of the community. For example, a user of the community may create a new security indicator using the security information sharing platform and/or submit it to the community so that other users of the community may collaboratively investigate the security indicator and provide their input. In doing so, security information engine 123 may present, via a user interface (e.g., of the security information sharing platform), the security indicator to the users of the community. A user of the community may investigate the security indicator being presented, assess the reliability of the source entity of the indicator, the level of confidence, and/or the level of severity, report a sighting of an observable (e.g., a sighting indicating that the user observed the observable), provide information about a potential threat actor (e.g., attacker) behind the security indicator, etc. The security indicator along with any associated information may be included and/or stored as part of the community-based security information of that community.

[0035] In some implementations, the community may choose to keep the security indicator (and/or associated information) private within the community or selectively share the security indicator (and/or associated information) with the security sharing platform, another community, and/or another user. The community-based security information that is kept private within the community may be accessed by the users who belong to that community but may not be accessible by or visible to the security information sharing platform, another community, and/or another user. In some situations, a case initiator who defined a set of community attributes to create a community may not be associated with user attributes that satisfy the set of community attributes. In other words, although the community is created by the case initiator, the case initiator is not part of the

community and therefore is not given access to the community-based security information of that community. To authorize the case initiator (and/or any other users outside of the community) to access at least a portion of the community-based security information of that community, the community members (or at least some portion of the community members) may decide on whether to grant access to the case initiator (and/or any other users outside of the community). For example, it may be determined based on a result of voting by the members of the community (or at least some portion of the community members).

[0036] Encryption engine 124 may encrypt at least a portion of the community-based security information of the community with an encryption key. In some implementations, encryption engine 124 may obtain a data item that is originated from a source entity. A "data item," as used herein, may be a security indicator, any information related to the security indicator, and/or other information that, if submitted to a community of the security information sharing platform, may be part of the community-based security information of that community. Since different data items and/or source entities may have different requirements for security, a particular security key management capability (e.g., a particular encryption mechanism) may be selected or otherwise determined from a set of available security key management capabilities (e.g., Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), masking keys, etc.) based on the security requirement.

[0037] In some implementations, encryption engine 124 may identify a security requirement by, for example, extracting the security requirement from at least one of: the data item and a user profile of the source entity (e.g., from which the data item is originated). "Security requirement," as used herein, may define and/or specify at least one user that is authorized to access the data item. For example, a security requirement may comprise, but is not limited to: (i) a set of user attributes that describe users to be authorized to access the data item, (ii) an identification of a user to be authorized to access the data item, and (iii) an identification of a pre-defined group of users to be authorized to access the data item.

[0038] In one example, a source entity may produce regular reports (e.g., data item) that are to be encrypted and distributed to a small group or community where the identifications of its members are known. In this case, the encryption mechanism "IBE" may be selected to encrypt those reports. IBE is a type of public-key encryption (also called asymmetric encryption) where a public key is used to encrypt the reports. A user (e.g., the recipient of the reports) may decrypt the encrypted reports using a decryption key (e.g., a private key corresponding to the public key) obtained from a trusted key management authority wherein the decryption key is generated based on some unique information about the identity of the user (e.g., the user's email address).

[0039] In another example, the source entity may produce reports (e.g., data item) that has a wider readership list, where the readers are described by their attributes (e.g., and therefore generating a community that comprises those readers associated with user attributes that satisfy a set of community attributes, as discussed herein with respect to community engine 122). In this example, encryption engine 124 may encrypt the reports using the encryption mechanism "ABE." ABE is a type of public-key encryption where a public key may be used to encrypt the reports. A user (e.g., the recipient of the reports) may be provided with a decryption key that matches with a pre-defined set of attributes. As such, any users having the set of attributes may be given the decryption key to access the encrypted reports.

[0040] If the encryption mechanism "ABE" is used to encrypt the data item (e.g., the data item that represents at least a portion of the community-based security information of a particular community), the decryption key that is able to decrypt the encrypted data item may comprise a private key corresponding to each user attribute of the set of user attributes. Referring back to community engine 122 as discussed herein, a community may be defined by a set of community attributes, where users that are associated with user attributes that satisfy the set of community attributes may access community-based security information of that community on the security information sharing platform. Assuming that the set of

community attributes is expressed as: ("Top 10 US Bank" AND "Security Clearance") OR "China." A first set of user attributes including "Top 10 US Bank" and "Security Clearance" would satisfy this set of community attributes. A first user associated with the first set of user attributes may be provided with a first decryption key that comprises a first private key corresponding to "Top 10 US Bank" and a second private key corresponding to "Security Clearance." Any users associated with the first set of user attributes may be provided with the first decryption key that can be used to decrypt the encrypted data item. Similarly, a second set of user attribute including "China" would also satisfy the set of community attributes. A second user associated with the second set of user attributes may be provided with a second decryption key that comprises a third private key corresponding to "China." Any users associated with the second set of user attributes may be provided with the second decryption key that can be used to decrypt the encrypted data item. However, a user that is associated with neither of the two sets of user attributes would be prevented from accessing and/or decrypting the encrypted data item.

[0041] Access engine 125 may receive, from a user, a request to access the community-based security information of the community. "Access," as used herein, may refer to an ability to view/read, add, modify, delete, or a combination thereof. Upon receiving the request, access engine 125 may determine whether the community-based security information of the community should be accessible by that user. In the case that the community is generated based on a set of community attributes (e.g., as discussed herein with respect to community engine 122), this may depend on the determination of whether the user is associated with a set of user attributes that would satisfy the set of community attributes. In some situations, the user credentials (e.g., login and/or password) of the user may already be associated with the set of user attributes of that user. Thus, when the user is logged into the security information sharing platform, the user may automatically gain access to the community-based security information of the community.

[0042] In response to determining that the community-based security information of the community is accessible by the user (e.g., from which the request to access was received), access engine 125 may authorize the user to access the community-based security information of the community. If authorized to access the community-based security information of the community, the user may view/read, add modify, and/or delete information from the community-based security information (e.g., submit a security indicator, submit information related to the security indicator, or otherwise collaborate with other users in the community, as discussed herein with respect to community engine 122). On the other hand, in response to determining that the community-based security information of the community is not accessible by the user, access engine 125 may prevent that user from accessing the community-based security information of the community.

[0043] In performing their respective functions, engines 121-124 may access data storage 129 and/or other suitable database(s). Data storage 129 may represent any memory accessible to community-based security information encryption system 110 that can be used to store and retrieve data. Data storage 129 and/or other database may comprise random access memory (RAM), read-only memory (ROM), electrically-erasable programmable read-only memory (EEPROM), cache memory, floppy disks, hard disks, optical disks, tapes, solid state drives, flash drives, portable compact disks, and/or other storage media for storing computer-executable instructions and/or data. Community-based security information encryption system 110 may access data storage 129 locally or remotely via network 50 or other networks.

[0044] Data storage 129 may include a database to organize and store data. The database may reside in a single or multiple physical device(s) and in a single or multiple physical location(s). The database may store a plurality of types of data and/or files and associated data or file description, administrative information, or any other data.

[0045] FIG. 2 is a block diagram depicting an example community-based security information encryption system 210. Community-based security information encryption system 210 may comprise an attributes engine 221, a security information

engine 223, an encryption engine 224, an access engine 225, and/or other engines. Engines 221 and 223-225 represent engines 121 and 123-125, respectively.

[0046] FIG. 3 is a block diagram depicting an example machine-readable storage medium 310 comprising instructions executable by a processor for encrypting community-based security information.

[0047] In the foregoing discussion, engines 121-125 were described as combinations of hardware and programming. Engines 121-125 may be implemented in a number of fashions. Referring to FIG. 3, the programming may be processor executable instructions 321-325 stored on a machine-readable storage medium 310 and the hardware may include a processor 311 for executing those instructions. Thus, machine-readable storage medium 310 can be said to store program instructions or code that when executed by processor 311 implements community-based security information encryption system 110 of FIG. 1.

[0048] In FIG. 3, the executable program instructions in machine-readable storage medium 310 are depicted as attributes instructions 321, community instructions 322, security information instructions 323, encryption instructions 324, and access instructions 325. Instructions 321-325 represent program instructions that, when executed, cause processor 311 to implement engines 121-125, respectively.

[0049] FIG. 4 is a block diagram depicting an example machine-readable storage medium 410 comprising instructions executable by a processor for encrypting community-based security information.

[0050] Referring to FIG. 4, the programming may be processor executable instructions 422, 424, and 425 stored on a machine-readable storage medium 410 and the hardware may include a processor 411 for executing those instructions. Thus, machine-readable storage medium 410 can be said to store program instructions or code that when executed by processor 411 implements community-based security information encryption system 110 of FIG. 1.

[0051] In FIG. 4, the executable program instructions in machine-readable storage medium 410 are depicted as community instructions 422, encryption instructions 424, and access instructions 425. Instructions 422, 424, and 425 represent program

instructions that, when executed, cause processor 411 to implement engines 122, 124, and 125, respectively.

[0052] Machine-readable storage medium 310 (or machine-readable storage medium 410) may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. In some implementations, machine-readable storage medium 310 (or machine-readable storage medium 410) may be a non-transitory storage medium, where the term "non-transitory" does not encompass transitory propagating signals. Machine-readable storage medium 310 (or machine-readable storage medium 410) may be implemented in a single device or distributed across devices. Likewise, processor 311 (or processor 411) may represent any number of processors capable of executing instructions stored by machine-readable storage medium 310 (or machine-readable storage medium 410). Processor 311 (or processor 411) may be integrated in a single device or distributed across devices. Further, machine-readable storage medium 310 (or machine-readable storage medium 410) may be fully or partially integrated in the same device as processor 311 (or processor 411), or it may be separate but accessible to that device and processor 311 (or processor 411).

[0053] In one example, the program instructions may be part of an installation package that when installed can be executed by processor 311 (or processor 411) to implement community-based security information encryption system 110. In this case, machine-readable storage medium 310 (or machine-readable storage medium 410) may be a portable medium such as a floppy disk, CD, DVD, or flash drive or a memory maintained by a server from which the installation package can be downloaded and installed. In another example, the program instructions may be part of an application or applications already installed. Here, machine-readable storage medium 310 (or machine-readable storage medium 410) may include a hard disk, optical disk, tapes, solid state drives, RAM, ROM, EEPROM, or the like.

[0054] Processor 311 may be at least one central processing unit (CPU), microprocessor, and/or other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 310. Processor 311 may

fetch, decode, and execute program instructions 321-325, and/or other instructions. As an alternative or in addition to retrieving and executing instructions, processor 311 may include at least one electronic circuit comprising a number of electronic components for performing the functionality of at least one of instructions 321-325, and/or other instructions.

[0055] Processor 411 may be at least one central processing unit (CPU), microprocessor, and/or other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 410. Processor 411 may fetch, decode, and execute program instructions 422, 424, 425, and/or other instructions. As an alternative or in addition to retrieving and executing instructions, processor 411 may include at least one electronic circuit comprising a number of electronic components for performing the functionality of at least one of instructions 422, 424, 425, and/or other instructions.

[0056] FIG. 5 is a flow diagram depicting an example method 500 for encrypting community-based security information. The various processing blocks and/or data flows depicted in FIG. 5 (and in the other drawing figures such as FIG. 6) are described in greater detail herein. The described processing blocks may be accomplished using some or all of the system components described in detail above and, in some implementations, various processing blocks may be performed in different sequences and various processing blocks may be omitted. Additional processing blocks may be performed along with some or all of the processing blocks shown in the depicted flow diagrams. Some processing blocks may be performed simultaneously. Accordingly, method 500 as illustrated (and described in greater detail below) is meant to be an example and, as such, should not be viewed as limiting. Method 500 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as storage medium 310, and/or in the form of electronic circuitry.

[0057] In block 521, method 500 may include identifying a set of community attributes to be used to generate a community on a security information sharing platform that enables sharing of security information among a plurality of

communities. Referring back to FIG. 1, attributes engine 121 may be responsible for implementing block 521.

[0058] In block 522, method 500 may include obtaining a security indicator from a first user of the community. The first user may be associated with a set of user attributes that satisfy the set of community attributes, wherein each user attribute in the set of user attributes corresponds to a private key. Referring back to FIG. 1, security information engine 123 may be responsible for implementing block 522.

[0059] In block 523, method 500 may include obtaining information related to the security indicator from a second user of the community. Referring back to FIG. 1, security information engine 123 may be responsible for implementing block 523.

[0060] In block 524, method 500 may include including the security indicator and the information related to the security indicator in community-based security information of the community. Referring back to FIG. 1, security information engine 123 may be responsible for implementing block 524.

[0061] In block 525, method 500 may include encrypting at least a portion of the community-based security information of the community with an encryption key. Referring back to FIG. 1, encryption engine 124 may be responsible for implementing block 525.

[0062] In block 526, method 500 may include generating a decryption key using the private key corresponding to the each user attribute in the set of user attributes. Referring back to FIG. 1, encryption engine 124 may be responsible for implementing block 526.

[0063] In block 527, method 500 may include authorizing a third user to access the encrypted portion of the community-based security information of the community using the decryption key. The third user may be associated with the set of user attributes. Referring back to FIG. 1, access engine 125 may be responsible for implementing block 527.

[0064] FIG. 6 is a flow diagram depicting an example method 600 for encrypting community-based security information. Method 600 as illustrated (and described in greater detail below) is meant to be an example and, as such, should not be viewed

as limiting. Method 600 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as storage medium 210, and/or in the form of electronic circuitry.

[0065] In block 621, method 600 may include identifying a set of community attributes to be used to generate a community on a security information sharing platform that enables sharing of security information among a plurality of communities. Referring back to FIG. 1, attributes engine 121 may be responsible for implementing block 621.

[0066] In block 622, method 600 may include obtaining a security indicator from a first user of the community. The first user may be associated with a first set of user attributes that satisfy the set of community attributes, wherein each user attribute in the first set of user attributes corresponds to a private key. Referring back to FIG. 1, security information engine 123 may be responsible for implementing block 622.

[0067] In block 623, method 600 may include obtaining information related to the security indicator from a second user of the community. Referring back to FIG. 1, security information engine 123 may be responsible for implementing block 623.

[0068] In block 624, method 600 may include including the security indicator and the information related to the security indicator in community-based security information of the community. Referring back to FIG. 1, security information engine 123 may be responsible for implementing block 624.

[0069] In block 625, method 600 may include encrypting at least a portion of the community-based security information of the community with an encryption key. Referring back to FIG. 1, encryption engine 124 may be responsible for implementing block 625.

[0070] In block 626, method 600 may include generating a decryption key using the private key corresponding to the each user attribute in the first set of user attributes. Referring back to FIG. 1, encryption engine 124 may be responsible for implementing block 626.

[0071] In block 627, method 600 may include authorizing a third user to access the encrypted portion of the community-based security information of the community using the decryption key. The third user may be associated with the first set of user attributes. Referring back to FIG. 1, access engine 125 may be responsible for implementing block 627.

[0072] In block 628, method 600 may include preventing a fourth user from accessing the encryption portion of the community-based security information of the community. The fourth user is associated with a second set of user attributes that do not satisfy the set of community attributes. Referring back to FIG. 1, access engine 125 may be responsible for implementing block 628.

[0073] The foregoing disclosure describes a number of example implementations for encrypting community-based security information. The disclosed examples may include systems, devices, computer-readable storage media, and methods for encrypting community-based security information. For purposes of explanation, certain examples are described with reference to the components illustrated in FIGS. 1-4. The functionality of the illustrated components may overlap, however, and may be present in a fewer or greater number of elements and components.

[0074] Further, all or part of the functionality of illustrated elements may co-exist or be distributed among several geographically dispersed locations. Moreover, the disclosed examples may be implemented in various environments and are not limited to the illustrated examples. Further, the sequence of operations described in connection with FIGS. 5-6 are examples and are not intended to be limiting. Additional or fewer operations or combinations of operations may be used or may vary without departing from the scope of the disclosed examples. Furthermore, implementations consistent with the disclosed examples need not perform the sequence of operations in any particular order. Thus, the present disclosure merely sets forth possible examples of implementations, and many variations and modifications may be made to the described examples. All such modifications and variations are intended to be included within the scope of this disclosure and protected by the following claims.

CLAIMS

1. A method for encryption of community-based security information on a security information sharing platform, the method comprising:

identifying a first set of community attributes to be used to generate a first community on the security information sharing platform that enables sharing of security information among a plurality of communities;

obtaining a first security indicator from a first user of the first community, the first user associated with a first set of user attributes that satisfy the first set of community attributes, wherein each user attribute in the first set of user attributes corresponds to a private key;

obtaining information related to the first security indicator from a second user of the first community;

including the first security indicator and the information related to the first security indicator in community-based security information of the first community;

encrypting at least a portion of the community-based security information of the first community with a first encryption key;

generating a first decryption key using the private key corresponding to the each user attribute in the first set of user attributes; and

authorizing a third user to access the encrypted portion of the community-based security information of the first community using the first decryption key, the third user associated with the first set of user attributes.

2. The method of claim 1, wherein the first set of user attributes comprises a first user attribute and a second user attribute, the first attribute corresponding to a first private key and the second attribute corresponding to a second private key.

3. The method of claim 2, comprising:

generating the first decryption key using the first private key and second private key.

4. The method of claim 1, wherein the first security indicator comprises at least one of: observable including an Internet Protocol (IP) address, a domain name, an e-mail address, a Uniform Resource Locator (URL), and a software file hash.

5. The method of claim 1, wherein the information related to the first security indicator comprise at least one of: an investigation result that is provided by the second user for the first security indicator, an indicator score for the first security indicator, a source for the first security indicator, and a threat actor for the first security indicator.

6. The method of claim 1, wherein a fourth user is associated with a second set user attributes that do not satisfy the first set of community attributes, comprising:

preventing the fourth user from accessing the encrypted portion of the community-based security information of the first community.

7. The method of claim 1, comprising:

identifying a second set of community attributes to be used to generate a second community on the security information sharing platform;

obtaining a second security indicator from the first user, the first user associated with a second set of user attribute that satisfy the second set of community attributes, wherein each user attribute in the second set of user attributes corresponds to a private key;

obtaining information related to the second security indicator from a fourth user of the second community;

including the second security indicator and the information related to the second security indicator in community-based security information of the second community;

encrypting at least a portion of the community-based security information of the second community with a second encryption key;

generating a second decryption key using the private key corresponding to the each user attribute in the second set of user attributes; and

authorizing a fifth user to access the encrypted portion of the community-based security information of the second community using the second decryption key, the fifth user associated with the second set of user attributes.

8. A non-transitory machine-readable storage medium comprising instructions executable by a processor of a computing device for encryption of community-based security information on a security information sharing platform, the non-transitory machine-readable storage medium comprising:

instructions to obtain a data item that is originated from a source entity;

instructions to identify a security requirement that defines at least one user that is authorized to access the data item, the security requirement comprising a set of user attributes that describe users to be authorized to access the data item;

instructions to determine an encryption mechanism to be used to encrypt the data item based on the security requirement;

instructions to generate a community on the security information sharing platform that enables sharing of security information among a plurality of communities, the community comprising the users associated with the set of user attributes; and

instructions to authorize the users of the community to access the encrypted data item using a decryption key that comprises a private key corresponding to the each user attribute of the set of user attributes.

9. The non-transitory machine-readable storage medium of claim 8, comprising:

instructions to obtain a security indicator from a first user of the community;

instructions to obtain information related to the security indicator from a second user of the community;

instructions to encrypt the security indicator and the information related to the security indicator using the encryption mechanism; and

instructions to authorize a third user of the community to access the security indicator and the information related to the security indicator using the decryption key.

10. The non-transitory machine-readable storage medium of claim 8, the security requirement comprises an identification of a user to be authorized to access the data item, or an identification of a pre-defined group of users to be authorized to access the data item.

11. The non-transitory machine-readable storage medium of claim 8, comprising:

instructions to extract the security requirement from at least one of: the data item and a user profile of the source entity.

12. The non-transitory machine-readable storage medium of claim 8, comprising:

instructions to identify a set of security key management capabilities that are available for the data item; and

instructions to determine the encryption mechanism to be used to encrypt the data item based on the security requirement and the set of security key management capabilities.

13. The non-transitory machine-readable storage medium of claim 8, wherein the set of attributes comprise an attribute related to at least one of: an industry sector of the users, a geographical region of the users, an organization that the users belong to, user reputation of the users, a citizenship status of the users, an

environmental condition, an indication of whether the users represent a threat intelligence feed vendor, a security clearance level of the users, and user status of the users in the security information sharing platform.

14. A system for encryption of community-based security information on a security information sharing platform comprising:

a processor that:

identifies a set of community attributes to be used to generate a community on the security information sharing platform that enables sharing of security information among a plurality of communities;

obtains a security indicator from a first user of the community, the first user associated with a first set of user attributes that satisfy the set of community attributes, wherein each user attribute in the first set of user attributes corresponds to a private key;

obtains information related to the security indicator from a second user of the community;

includes the security indicator and the information related to the security indicator in community-based security information of the community;

encrypts at least a portion of the community-based security information of the community; and

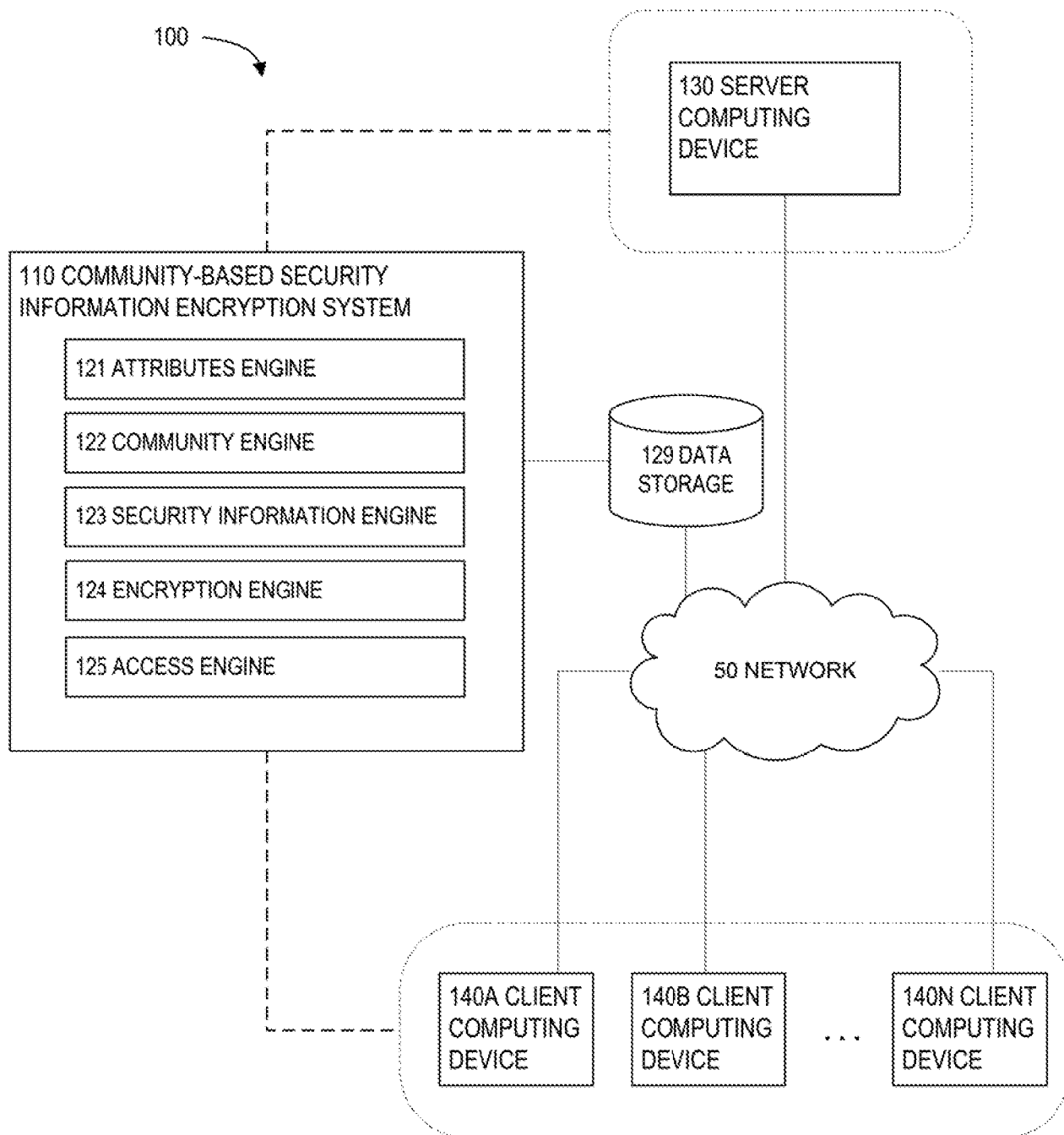
prevents a third user from accessing the encrypted portion of the community-based security information of the community, wherein the third user is associated with a second set of user attributes that do not satisfy the set of community attributes.

15. The system of claim 14, the processor that:

provides, to a fourth user associated with the first set of user attributes, a decryption key that comprises the private key corresponding to the each user attribute in the first set of user attributes; and

authorizes the fourth user to access the encrypted portion of the community-based security information of the community using the decryption key.

1/5

**FIG. 1**

2/5

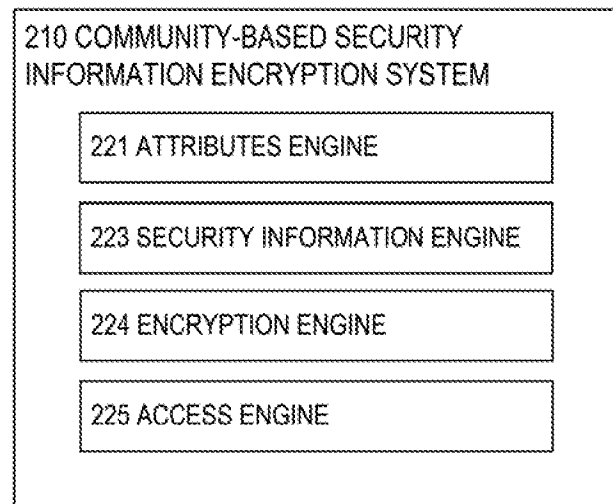
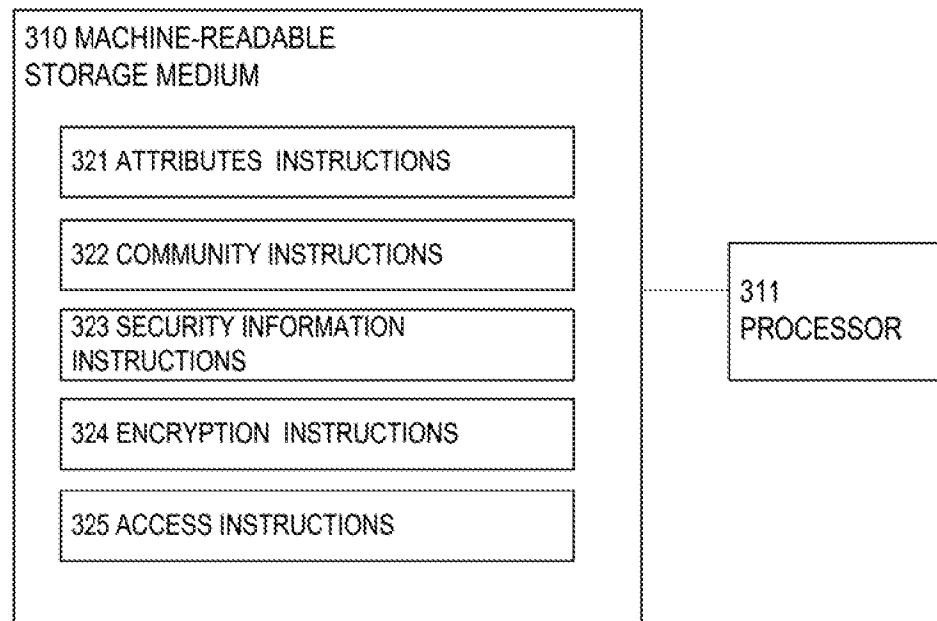
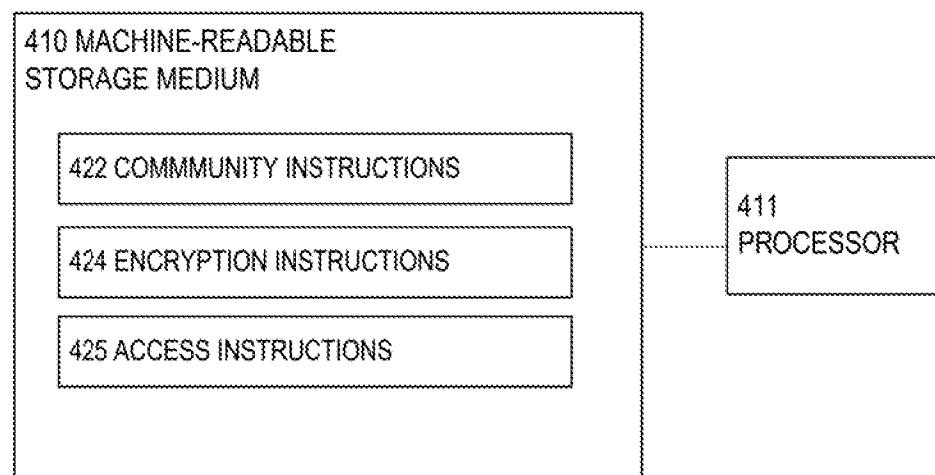


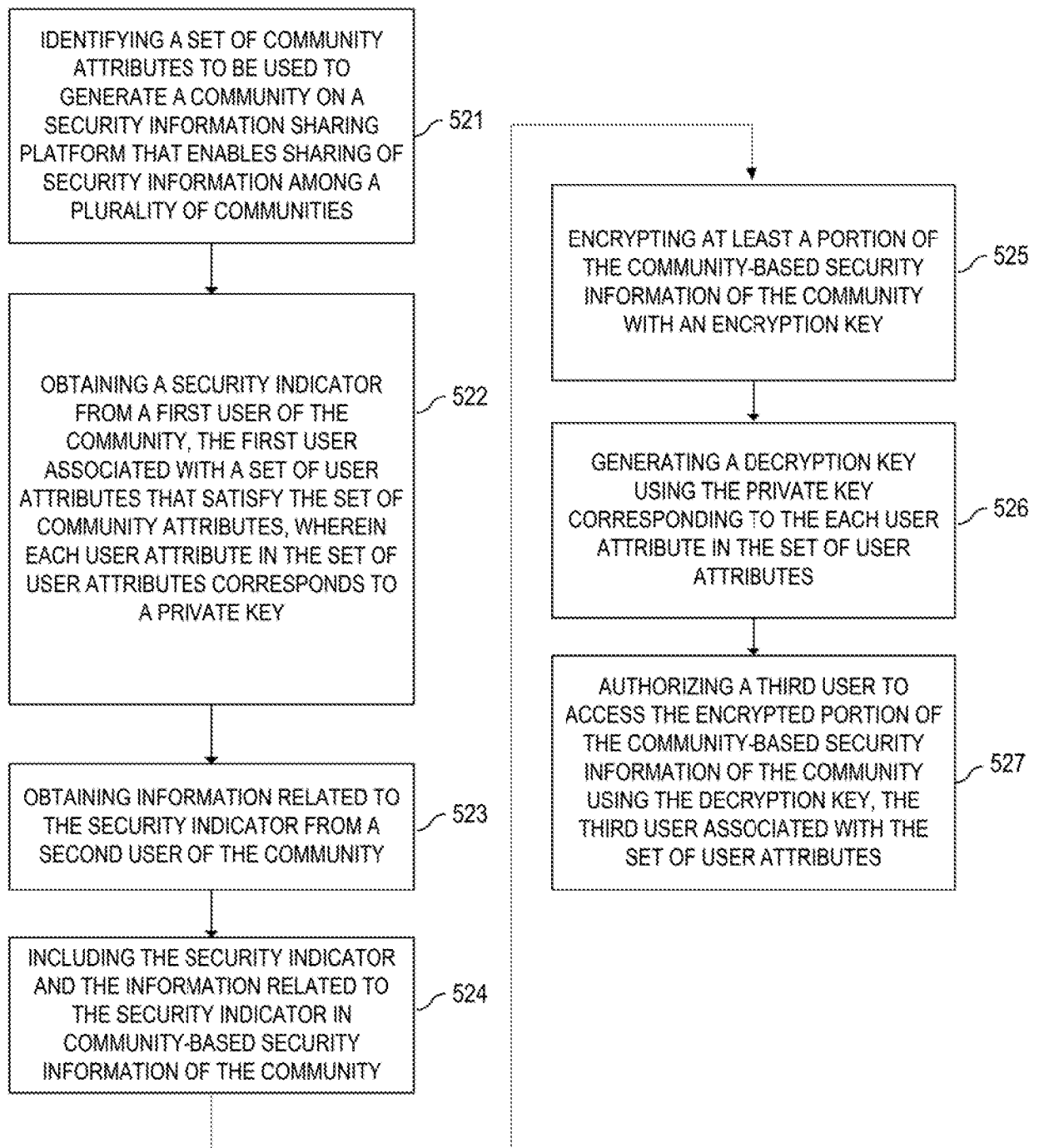
FIG. 2

3/5

**FIG. 3****FIG. 4**

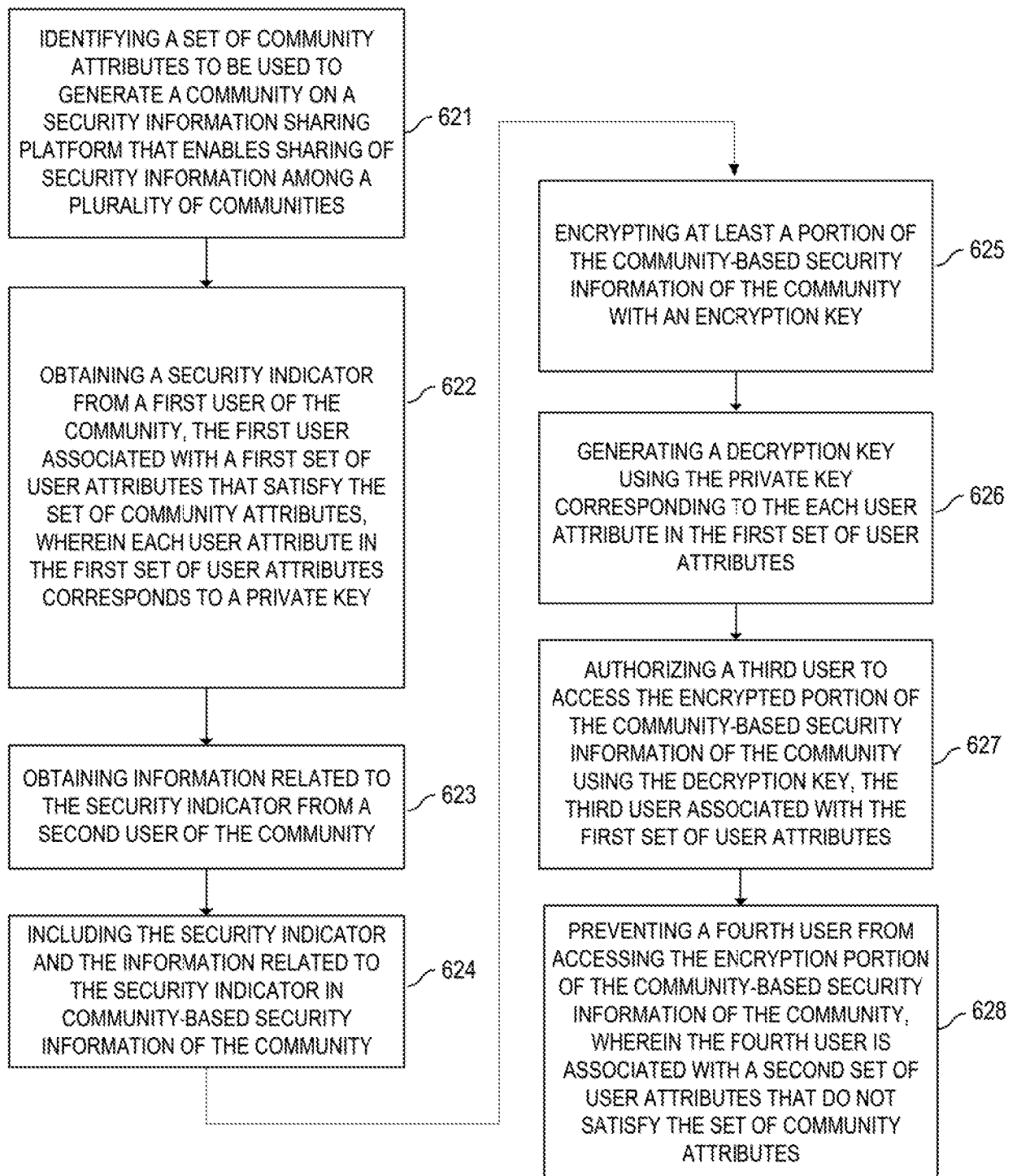
4/5

500

**FIG. 5**

5/5

600

**FIG. 6**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/015834**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/08(2006.01)i, H04L 9/32(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)

H04L 9/08; G06F 15/16; G06F 17/00; H04L 12/26; G06F 7/00; G06F 21/62; H04L 29/06; H04L 12/22; H04L 9/32

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: community, user attribute, security indicator, scoring, authorizing, encryption, decryption, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003-0158897 A1 (RON BEN-NATAN et al.) 21 August 2003 See paragraphs [0013], [0024], [0042], [0053], [0068], [0079], [0102]; claim 1; and figure 3.	1-15
Y	WO 2015-160357 A1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 22 October 2015 See paragraphs [0011], [0017], [0044]; claim 10; and figures 3, 4.	1-15
Y	US 2014-0289518 A1 (TUHIN SINHA) 25 September 2014 See paragraphs [0025], [0039]; and claim 1.	1-15
A	US 2015-0373040 A1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 24 December 2015 See paragraphs [0042]-[0044]; and figure 2.	1-15
A	US 7805415 B1 (KEVIN E. FLESHER et al.) 28 September 2010 See column 17, line 10 - column 18, line 44; and figure 12.	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

20 October 2016 (20.10.2016)

Date of mailing of the international search report

21 October 2016 (21.10.2016)

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

AHN, Jeong Hwan

Telephone No. +82-42-481-8633



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/015834

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003-0158897 A1	21/08/2003	None	
WO 2015-160357 A1	22/10/2015	None	
US 2014-0289518 A1	25/09/2014	WO 2014-146033 A1	18/09/2014
US 2015-0373040 A1	24/12/2015	WO 2014-120189 A1	07/08/2014
US 7805415 B1	28/09/2010	US 2002-0073059 A1	13/06/2002
		US 2002-0073313 A1	13/06/2002
		US 2002-0078349 A1	20/06/2002
		US 2004-0103147 A1	27/05/2004
		US 2004-0111639 A1	10/06/2004
		US 2009-0094674 A1	09/04/2009
		US 6834382 B2	21/12/2004
		US 7165060 B2	16/01/2007
		US 7293175 B2	06/11/2007
		US 7437408 B2	14/10/2008
		US 7809791 B2	05/10/2010
		WO 2005-031523 A2	07/04/2005
		WO 2005-031523 A3	19/04/2007