Abstract: This disclosure describes techniques for defining security measures of a secure data corridor that enables data feeds to transmit from an ingress point to an egress point, while maintaining a desired security protection. This disclosure further describes techniques to quantify the desired security protection by determining and further associating a data sensitivity rating with individual data feeds in transit through the secure data corridor. In some examples, the data sensitivity rating of the secure data corridor may be locked at a default rating that is commensurate with access permissions of a subject or a data sensitivity rating of an adjoining secure data container. Alternatively, the data sensitivity rating may be dynamically set based on data feeds transmitting through the secure data corridor or set based on the data sensitivity rating of data feeds at an ingress point or egress point of the secure data corridor.
DISTRIBUTED BIG DATA SECURITY ARCHITECTURE

RELATED APPLICATIONS


BACKGROUND

[0002] Traditional information technology (IT) architecture have relied on centralized computing structures, whereby all or most of the processing and computing is performed on a central server. Centralized computing can enable the deployment of central server computing resources, administration, and management. Typically, computational processing involves the extraction, transformation and loading of a resultant data feeds by the centralized computing structure.

[0003] However, cost and performance inefficiencies of centralized computing structures have steered IT architectures towards decentralized computing structures, whereby data feeds are extracted, uploaded to a decentralized computing platform and then transformed. Doing so provides cost and performance efficiencies since the infrastructure to perform the computational processing can be outsourced to an entity that specializes in such.

[0004] As decentralized computing develops, both the velocity and diversity of data can cause some security measures to have an impact on latency, scalability, and recovery performance. Thus, security can be viewed as a service constraint. Thus there is a need to
balance security constraints with other competing service constraints when optimizing operation requirements of a platform.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0005] The detailed description is set forth with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items or features.

[0006] FIG. 1 illustrates a schematic view of a computing environment 100 that facilitates a subject establishing a secure session between a subject and a secure data container via a secure data corridor.

[0007] FIG. 2A illustrates a block diagram of an informational graph that describes the relationship between data objects, data elements, and data feeds within a use-case and/or secure data container. FIG. 2B illustrates a block diagram of a diagraph that represents subject permissions to a specific control and a specific data feed.

[0008] FIG. 3A illustrates a block diagram of an exemplary permission lattice associated with granting access privileges to a subject. FIG. 3B illustrates a data sensitivity lattice for classifying control to for the control level of data feeds.

[0009] FIG. 4 illustrates a block diagram of a resource management platform that can establish a communicative connection between a subject device and a secure data container via a secure data corridor.

[0010] FIG. 5 illustrates a flow diagram that describes a process of establishing a session between a subject and a secure data container using a secure data corridor.

[0011] FIG. 6 illustrates a flow diagram that describes a process of dynamically setting a data sensitivity rating of a secure data corridor based at least in part on the data sensitivity of data feeds.
DETAILED DESCRIPTION

[0012] This disclosure describes techniques for defining security measures of a "secure data corridor" that enables data feeds to transmit from an ingress point to an egress point, while maintaining a desired security protection. The term "secure data corridor" as used herein may describe a communication channels used to transmit data feeds from a source location (i.e., ingress point) to a destination location (i.e., egress point). The techniques described herein further associate a secure data corridor with security measures that mandate confidentiality protection and data integrity protection that is commensurate with the nature of the data feed. For example, a data feed that relates to proprietary vendor data that is preferentially withheld from public dissemination may be associated with a less sensitive security measure when compared with a data feed that that relates to personal consumer information that must be withheld from public dissemination. In various examples, security measures may be defined, and enforced by explicit, read, write, import and export provisions expressly associated with data feeds. Further, any other regime that is definable by a developer or an administrator, may be used to define security measures.

[0013] In various examples, data items may be classified by use-case, and risk controls may be applied based on the sensitivity of data that is maintained within each use case. Each use case may be classified and assigned to "data sensitivity rating." The term "data sensitivity rating" is used herein to describe a rating, or score, given to a data feed that quantifies the security measure that mandates confidentiality protection and data integrity protection. Using the above mentioned example, a data feed that is associated with personal consumer information to be withheld from public dissemination is likely to be assigned a more sensitive, that is higher, data sensitivity rating, relative to a data feed that relates to proprietary vendor data that is preferentially withheld from public dissemination.
Each data sensitivity rating may prompt one or more control parameters that protect the confidentiality and integrity of the data feed. The one or more control parameters may include principles such as no read-up, no write-down, tranquility, explicit read-in, and explicit write-out. The 'no read-up' principle refers to a condition whereby a subject at a given security level may not read a data feed at a high security level. A 'no write-down' principle refers to a condition whereby a subject at a given security level may not write to a data feed to a less sensitive security level. The term "subject" as used herein describes a user, a non-user entity, a secure data container, or any other data structure requesting access permissions to data feeds within a secure data container, and via a secure data corridor.

In various examples, the classification of a "data sensitivity rating" may be associated directly with data elements, and set by predetermined rules. In some examples, a default data sensitivity rating may be assigned to a secure data corridor. In other examples, the data sensitivity rating may be based on access privileges associated with the subject. Further, the data sensitivity rating of the secure data corridor may be dynamically set by interrogating the nature of the data feed that is transmitting through the secure data corridor. In some examples, the data sensitivity rating may be set in substantially real-time.

The term "data feed" as used herein describes a mechanism by which data can be transferred from a source location. A data feed may include one or more data elements, which in turn are associated with data objects. A data feed may be assigned a default control parameter that applies to all data elements in the feed. A data feed may have default controls and acquired controls. Acquired controls may supersede default controls. The ability to set default controls on a data feed may facilitate loading data into the cluster that requires transformation after loading, but still requires protection.
The term "data element" as used herein describes the physical and logical characteristics of an associated data type. Further, a data element may define a data type as a string, integer, float, or object. The data elements map to data objects, which in turn store the data value at a particular storage location.

In some examples, the control parameters are assigned to the data objects. The data elements that map to the data objects inherit control parameters from the data objects. Further, the data feed that maps to the data elements inherit the control parameters from the data elements, and ultimately from the data objects. The level of control parameters is dependent on the use case. Thus, the security model may be customized for different use cases. In other words, a use case may be associated with a specific data sensitivity rating, and all data objects associated with the use case may be assigned that same, specific data sensitivity rating. Thus, a subject with access to a use case may have access to all data and services that are assigned to the use case provided that the subject retains the requisite access permissions.

Each use case, may have its own namespace, which can be enforced by a resource management platform. Privileges and permission are attached to the namespace. The term 'namespace' is used herein to describe a set of symbols that are used to organize objects of various kinds, so that these objects may be referred to by name. In a non-limiting example, a namespace may include file systems, programming languages, and computer networks and distributed systems. Further, a namespace may also include a secure data container.

In various examples, a subject may be added to an Access Control List (ACL) on the authentication service principals in order to gain access to a secure data corridor. Generally, a subject assigned to a given data sensitivity rating may access all data within that same classification.
[0021] This disclosure further describes techniques that illustrate multiple layers of authentication, authorization, and auditing of separate platform levels. Thus, a single point of attack (SPOA) in the security trust chain can be avoided as any successful attack would need to be of a synchronized multi-point nature. Elements of a defense in depth may include controlling access to the resource management platform by an authentication server entry. Authentication may be performed by an Active Directory whereby a subject may provide a set of credentials that confirm their identity. In a non-limiting example, the credentials may include a username, password, or other biometric identifier. Further, authorization to access a secure data container, via secure data corridor is dependent on the assigned access privileges and the data sensitivity rating of an associated use case and data feed within the secure data container.

[0022] A secure data corridor may comprise of a secure data container and trust chain vertices. A trust chain is created by a directed graph of vertices between SDC. The traversal of a given trust chain not only verifies the integrity of the chain, but also enables an audit mechanism. The secure data container is, in essence, embedded within the data corridor. The trust chain vertices define logical input and output pathways to the embedded data container. In other words, a secure data corridor connotes a transport mechanism and in its basic pathway operates as a migration pathway of physical data.

[0023] In various examples, the secure data corridor may correspond to a link layer, a network layer, a transport layer, or an application layer of a transmission control protocol (TCP) and internet protocol (IP). In a non-limiting example, a secure data corridor may include one input, one output, and one container. In a second non-limiting example, a secure data corridor may include one container with one input and no outputs. In this example, the SDC can acts as a secure sink where data of an unknown sensitivity rating can be staged prior to being class-rated into other containers, and other secure data
corridors. In a third non-limiting example, the secure data corridor may include a secure data container with multiple outputs and no input. In this example, the secure data corridor input may be disconnected once data has been migrated. The multiple outputs, that is vertices, may connect to several other secure data corridors.

[0024] The term "data container," as used herein, describes a data structure that includes data items associated with the operation of a particular application. For example, a data container of a particular application and its dependencies may include an operating system, one or more data item libraries, configuration files, application binaries, and other parts of a technology stack used for execution of the particular application. Unlike a traditional virtual machine, a data container may hold its application and any dependencies, however a same operating system kernel and libraries can be shared between multiple containers running in a host environment.

[0025] The principles described herein may be applicable to any distributed computing environment. Historical protection techniques include network (IP address), firewall (Ports, Services), platform (Folder, Share) and data (Schema, Table) segmentation.

[0026] The term "techniques," as used herein, may refer to system(s), method(s), computer-readable instructions, module(s), algorithms, hardware logic, and/or operation(s) as permitted by the context described above and throughout the document.

[0027] FIG. 1 illustrates a schematic view of a computing environment 100 that facilitates a subject establishing a secure session between a subject and a secure data container via a secure data corridor.

[0028] In the illustrated example, the subject 102 may transmit an access request 104 to an authentication server 106. In some examples, the authentication server 106 may perform authentication by an Active Directory whereby the subject 102 may provide a set
of credentials that confirm their identity. In a non-limiting example, the credentials may include a username, password, or other biometric identifier associated with the subject.

[0029] In various examples, the subject 102 may correspond to a user, a non-user entity, a secure data corridor, or any other data structure that is capable of requesting access permissions to data feeds within a secure data container.

[0030] The subject 102 may interface with the authentication server 106 via any sort of electronic device, such as a cellular phone, a smart phone, a tablet computer, an electronic reader, a media player, a gaming device, a personal computer (PC), a laptop computer, etc. Further, the electronic device of the subject 102 may include a subscriber identity module (SEVI), such as an eSIM, to identify the electronic device of the subject 102 to a telecommunication service provider network (also referred to herein as "telecommunication network").

[0031] In the illustrated example, in response to authenticating the subject 102, a session 108 is initiated via the authentication server 106 between the subject 102, through one or more staging server(s) 110. The goal of a decentralized cluster security policy must be to balance the need to provide scalable aggregation while still maintaining isolation based on security classifications. Isolation may be based on authorization and via the one or more staging server(s) 110.

[0032] Further, the one or more staging server(s) 110 are communicatively connected to a resource management platform 112. The resource management platform 112 may establish a communicative connection between a subject 102 and one or more secure data container(s) 114(1), 114(2), or 114(N), via a secure data corridor 116(1), 116(2), and 116(N) respectively. In various examples, the secure data corridor 116(1), 116(2), and 116(N) correspond to a link layer, a network layer, a transport layer, or an application layer of a transmission control protocol (TCP) and internet protocol (IP). In a non-limiting
example, a secure data corridor may include one input, one output, and one container. In a second non-limiting example, a secure data corridor may include one container with one input and no outputs. The one or more secure data containers 114(1), 114(2), or 114(N) may be stored within a decentralized computing platform 118. The one or more secure data containers 116(1), 116(2), or 116(N) may include a data structure that includes data items associated with the operation of a particular application. For example, a data container of a particular application and its dependencies may include an operating system, one or more data item libraries, configuration files, application binaries, and other parts of a technology stack used for execution of the particular application.

[0033] The one or more staging server(s) 110 and the decentralized computing platform 118 may operate on one or more distributed computing resource(s), respectively. The one or more distributed computing resource(s) may include one or more computing device(s) 120 and 122, respectively, that operate in a cluster or other configuration to share resources, balance load, increase performance, provide fail-over support or redundancy, or for other purposes. The one or more computing device(s) 120 and 122 may include one or more interfaces that enable communications with electronic device(s), such as an electronic device associated with the subject 102, via one or more network(s) 124.

[0034] In the illustrated example, the one or more network(s) 142 may include public networks such as the Internet, private networks such as an institutional and/or personal intranet, or some combination of private and public networks. The one or more network(s) 124 can also include any type of wired and/or wireless network, including but not limited to local area network (LANs), wide area networks (WANs), satellite networks, cable networks, Wi-Fi networks, Wi-Max networks, mobile communications networks (e.g., 3G, 4G, and so forth), or any combination thereof.
FIG. 2A illustrates a block diagram of an informational graph 200 that
describes the relationship between data objects, data elements, and data feeds within a use-case and/or secure data container. In the illustrated example, control parameters 202, 204, and 206 may be assigned to data objects 208, 210, and 212 respectively. The control parameters may include principles such as no read-up, no write-down, tranquility, explicit read-in, and explicit write-out. The 'no read-up' principle refers to a condition whereby a subject at a given security level may not read a data feed at a high security level. A 'no write-down' principle refers to a condition whereby a subject at a given security level may not write to a data feed to a less sensitive security level.

In the illustrated example, the data elements 214, 216, and 218 may map to the
data objects 208, 210, and 212 and inherit the respective control parameters 202, 204, and 206 of the data objects 208, 210, and 212. A data element may define the physical and logical characteristics of an associated data type. For example, a data element may define a data type as a string, integer, float, or object. Further, a data element may further define a risk rating or a generic sensitivity rating of the associated data. In some examples, sensitivity may change over time. Sensitivity may also change to reflect a directed or explicit sensitivity policy. Further, a data element may define a data type as a string, integer, float, or object. The data elements map to data objects, which in turn store the data value at a particular storage location.

In the illustrated example, the data feeds 220 and 222 that maps to the data elements inherit the control parameters from the data elements 214, 216, and 218, and ultimately from the data objects 208, 210, and 212.

FIG. 2B illustrates a block diagram of a diagraph that represents subject permissions to specific control parameters 224 and a specific data feed 226. In the illustrated example, permissions associated with the subject 228 are bound to specific
control parameters 224 and stored in a list of triples 230 (i.e., subject, control, and data feed) that tie the subject 228 to specific controls, and correspondingly the subject to the data feeds that are tagged by the specific controls. In some examples, the subject 228 may be granted access permissions to data feeds, whereby the nature of access is governed by the specific control parameters specified in the list of triples 230. The data feeds 226 and specific control parameters 224 may be explicitly assigned. Alternatively, or additionally, the subject 228 may be granted access to all data elements that are qualified by a specific control parameter.

[0039] Further, the resource management platform may interrogate the list of triples 230 associated with the subject to determine privileged data feeds as well as the controls that determine the access rights to those data feeds. The control parameters 224 may be expressed as a data sensitivity lattice of varying levels as further described in FIG. 3.

[0040] FIG. 3A illustrates a block diagram of an exemplary, data sensitivity lattice 300 associated with granting access permissions to a subject. In various examples, a subject may correspond to a user, a non-user entity, a secure data container, or any other data structure requesting access privileges. Particularly, FIG. 3A illustrates a block diagram of a data sensitivity lattice 300. In some examples, the data sensitivity lattice 300 may include a first data sensitivity layer 302 and a second data sensitivity layer 304. In the illustrated example, the first data sensitivity layer 302 may be associated with a first set of data items that mandate the least security measures for data confidentiality and data integrity protection. In a non-limiting example, the first set of data items may correspond to proprietary vendor data that is preferentially withheld from public distribution. Comparatively, the second data sensitivity layer 304 may be associated with a second set of data items that mandate more data security measures relative to the first data sensitivity layer 302, for data confidentiality and data integrity protection. In a non-limiting example,
the second set of data items may correspond to personal consumer information that must be withheld from public distribution. For illustrative purposes only, FIGS. 3A and 3B present a two-layer, data sensitivity lattice 300. It is noteworthy that the data sensitivity lattice 300 may be defined to include any number of layers favored by a developer or administrator.

[0041] Further, FIG. 3A illustrates the relative flow of read and write permissions between the first data sensitivity layer 302 and the second data sensitivity layer 304. It is noteworthy, that although FIG. 3A describes read and write permissions, permissions may further include import permissions, export permissions, or any other permission regime definable by a developer or administrator. In the illustrated example, a subject with access permission to the first data sensitivity layer 302 may write data items to the second data sensitivity layer 304, however the subject may not read data items within the second data sensitivity layer 304. In other words, the subject may add (i.e., write) data items to the more sensitive, second data sensitivity layer 304, however the subject may not access, that is read, data items within the more sensitive, second data sensitivity layer 304.

[0042] FIG. 3A further illustrates that a subject with access permission to the second data sensitivity layer 304 may read data items within the first data sensitivity layer 302, however the subject may not write data items within the first data sensitivity layer 302. In other words, the subject may read data items within the less sensitive, first data sensitivity layer 302, however the subject may not add (i.e., write) data items to the less sensitive, first data sensitivity layer 302.

[0043] It is noteworthy that a subject with access permission to the first data sensitivity layer 302 may read data items and write data items within the first data sensitivity layer 302. Similarly, a subject with access permission to the second data sensitivity layer 304 may read data items and write data items within the second data
sensitivity layer 304. Note that the terms data sensitivity layer and data sensitivity rating may be used interchangeably to describe the data sensitivity of a data item. Further the term data item may be used interchangeably to describe data feed.

[0044] FIG. 3B illustrates a data sensitivity lattice 306 that associates control parameters with data feeds. The control parameters are tied to data feeds. The control parameters may include read, write, export, and import parameters. In a non-limiting example, consider a subject with access permission to the second data sensitivity layer 304. As illustrated in FIG. 3A, the subject may read data items within the first data sensitivity layer 302, but may not add (i.e., write) data items to the first data sensitivity layer 302. The write limitation ensures that the subject may avoid inadvertently having more sensitive data items from the second data sensitivity layer 304 being added to the less sensitive, first data sensitivity layer 302. The data sensitivity lattice 306 of FIG. 3B reflects the same, except access permissions are presented from the perspective of the data feed, rather than the subject.

[0045] For example, FIG. 3A illustrates the second data sensitivity layer 304 as the most data sensitivity layer. Thus, the second data sensitivity layer 304 can only interact downward with the first data sensitivity layer 302. In FIG. 3B, the interaction of the second data sensitivity layer 304 with the first data sensitivity layer 302 is reflected in the 'down' column of the data sensitivity lattice 306. The 'down' column indicates a capability to read down (i.e., T in the read - down cell), and an inability to write down (i.e., '0' in the write - down cell).

[0046] Similarly, as shown FIG. 3A, a subject with access permissions to first data sensitivity layer 302 may not read data contained within the second data sensitivity layer 304, because the more sensitivity of the second data sensitivity layer 304 represents more sensitively classified data. Using the previous example of proprietary vendor data and
consumer personal data, a subject with permission access to proprietary vendor data (i.e., classified as first data sensitivity layer 302) cannot read the consumer personal data (i.e., classified as the second data sensitivity layer 304).

[0047] FIG. 4 illustrates a block diagram of a resource management platform 402 that can establish a communicative connection between a subject and a secure data container via a secure data corridor. The secure data corridor may be configured with a data sensitivity rating that is substantially similar to a data sensitivity rating of an adjoining secure data container. In some examples, the subject may correspond to a user device, a non-user entity device, or another adjoining secure data container.

[0048] In the illustrated example, the resource management platform 402 may correspond to resource management platform 112. Further, the resource management platform 402 may include one or more processor(s) 404 that are operably connected to memory 406. In at least one example, the one or more processor(s) 404 may be a central processing unit(s) (CPU), graphics processing unit(s) (GPU), a both a CPU and GPU, or any other sort of processing unit(s). Each of the one or more processor(s) 404 may have numerous arithmetic logic units (ALUs) that perform arithmetic and logical operations as well as one or more control units (CUs) that extract instructions and stored content from processor cache memory, and then executes these instructions by calling on the ALUs, as necessary during program execution. The one or more processor(s) 404 may also be responsible for executing all computer applications stored in the memory, which can be associated with common types of volatile (RAM) and/or nonvolatile (ROM) memory.

[0049] In some examples, memory 406 may include system memory, which may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.) or some combination of the two. The memory may also include additional data storage devices
(removable ad/or non-removable) such as, for example, magnetic disks, optical disks, or tape.

[0050] The memory 406 may further include non-transitory computer-readable media, such as volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. System memory, removable storage and non-removable storage are all examples of non-transitory computer-readable media. Examples of non-transitory computer-readable media include, but are not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium which can be used to store the desired information.

[0051] In the illustrated example, the memory 406 may include an operating system 408, a data sensitivity module 410, a secure data corridor module 412, and an audit module 414. The operating system 408 may be used to implement the data sensitivity module 410 and the secure data corridor module 412. The operating system 408 may be any operating system capable of managing computer hardware and software resources. The data sensitivity module 410, the secure data corridor module 412, and audit module 414 may include routines, program instructions, objects, and/or data structures that perform particular tasks or implement particular abstract data types.

[0052] In the illustrated example, the data sensitivity module 410 may determine the data sensitivity rating to assign to a secure data corridor. In some example, the data sensitivity module 410 may detect a data sensitivity rating at an ingress and egress point of a secure data corridor. The ingress and egress points may interchangeably correspond to a subject and a secure data container, depending on the flow of data feeds. Thus, the data
sensitivity module 410 may further assign a data sensitivity rating to the secure data corridor that corresponds with the determined data sensitivity rating at the ingress and egress points.

[0053] In a non-limiting example, the data sensitivity module 410 may quantify a data sensitivity rating of secure data corridor based on access permissions associated with a subject. For example, the data sensitivity module 410 may detect that access permissions associated with the subject may limit the data sensitivity rating of data feeds that the subject may access. For example, if a subject is permitted to access data feeds with a first data sensitivity rating, whereby the first data sensitivity rating is less sensitive (i.e., mandates less data security measures for data confidentiality and data integrity protection) than a second data sensitivity rating, the data sensitivity module 410 may associate the first data sensitivity rating to a secure data corridor that establishes a session link between a secure data container and the subject. Doing so ensures that data feeds that egress from the secure container to the subject comply with access permissions of the subject and do not include data feeds that may be more sensitive (i.e., mandate more data security measures for data confidentiality and data integrity protection) than permitted by the subject access permissions.

[0054] In another non-limiting example, the data sensitivity module 410 may quantify a data sensitivity rating of the secure data corridor based on the data sensitivity rating of incoming data feeds that ingress from the subject to a secure data container. In other words, the data sensitivity rating of the secure data corridor may be based on the data sensitivity rating of incoming data feeds that are transmitting into the secure data container, rather than data feeds being accessed by the subject from the secure data container. In this example, the data sensitivity module 410 may quantify a data sensitivity rating for incoming data feeds and associate that data sensitivity rating to the secure data
corridor that establishes a session link between the subject and the secure data container. Doing so ensures that incoming data feeds transmitting from the subject to the secure data container are protected while transmitting through the secure data corridor.

[0055] Further, in another non-limiting example, the data sensitivity module 410 may quantify a data sensitivity rating of the secure data corridor based on the data sensitivity rating of data feeds that transmit through the secure data corridor. In other words, the data sensitivity module 410 may detect the data sensitivity rating of data feeds transmitting through the secure data corridor, and dynamically set a substantially similar data sensitivity rating for the secure data corridor. A benefit of this approach is that in some instances, data feeds may have an unknown data sensitivity rating. As a precautionary measure, these data feeds tend to be assigned a high data sensitivity rating until determined otherwise. Thus to avoid assigning a secure data corridor with an arbitrary, and unnecessarily high data sensitivity rating that is based on data feed with unknown data sensitivity ratings transmitting through the secure data corridors, the data sensitivity module 410 may progressively adjust the data sensitivity rating of the secure data corridor in response to progressively quantifying the unknown data sensitivity ratings of the data feeds.

[0056] Additionally, the data sensitivity module 410 may lock the data sensitivity rating of a secure data corridor based at least in part on the data sensitivity rating of the adjoining secure data container. For example, a secure data container may have assigned a particular data sensitivity rating based at least in part on an associated use case. Thus, by locking the data sensitivity rating of the secure data corridor, the data sensitivity module 410 may ensure that data feeds that transmit through the secure data corridor comply with the data sensitivity rating of the use case.
In the illustrated example, the secure data corridor module 412 may establish a secure data corridor between a subject device and a secure data container. In various examples, the secure data corridor may correspond to a link layer, a network layer, a transport layer, or an application layer of a transmission control protocol (TCP) and internet protocol (IP). Further, secure data corridor module 412 may assign the secure data corridor with a data sensitivity rating that is determined by the data sensitivity module 410.

In the illustrated example, the audit module 414 facilitate a developer or administrator to audit an operation of the resource management platform. The audit module 414 may identify access permissions associated with a subject and compare the access permissions with control parameters of the data feeds. Further, the audit module 414 may interrogate data sensitivity ratings associated with established secure data corridors, secure data containers, and use cases associated with secure data containers. Additionally, the audit module may ensure that each of the secure data corridors and secure data containers comply with the control parameters of the transmitting data feeds.

In the illustrated example, the resource management platform 402 may further include input/output interface(s) 416. The input/output interface(s) 416 may include any type of output interface known in the art, such as a display (e.g., a liquid crystal display), speakers, a vibrating mechanism, or a tactile feedback mechanism. Input/output interface(s) 416 also include ports for one or more peripheral devices, such as headphones, peripheral speakers, or a peripheral display. Further, the input/output interface(s) 416 may further include a camera, a microphone, a keyboard/keypad, or a touch-sensitive display. A keyboard/keypad may be a push button numerical dialing pad (such as on a typical telecommunication device), a multi-key keyboard (such as a conventional QWERTY
keyboard), or one or more other types of keys or buttons, and may also include a joystick-like controller and/or designated navigation buttons, or the like.

[0060] In the illustrated example, the resource management platform 402 may further include one or more network interface(s) 418. The one or more network interface(s) 418 may include any sort of transceiver known in the art. For example, the one or more network interface(s) 418 may include a radio transceiver that performs the function of transmitting and receiving radio frequency communications via an antenna. In addition, the one or more network interface(s) 418 may also include a wireless communication transceiver and a near field antenna for communicating over unlicensed wireless Internet Protocol (IP) networks, such as local wireless data networks and personal area networks (e.g., Bluetooth or near field communication (NFC) networks). Further, the one or more network interface(s) 418 may include wired communication components, such as an Ethernet port or a Universal Serial Bus (USB).

[0061] FIGS. 5 and 6 present illustrative processes 500 and 600 for establishing a session between a subject and a secure data container using a secure data corridor, and dynamically setting a data sensitivity rating of a secure data corridor based at least in part on the data sensitivity ratings of data feeds. Each of processes 500 and 600 illustrate a collection of blocks in a logical flow chart, which represents a sequence of operations that can be implemented in hardware, software, or a combination thereof. In the context of software, the blocks represent computer-executable instructions that, when executed by one or more processors, perform the recited operations. Generally, computer-executable instructions may include routines, programs, objects, components, data structures, and the like that perform particular functions or implement particular abstract data types. The order in which the operations are described is not intended to be construed as a limitation, and any number of the described blocks can be combined in any order and/or in parallel to
implement the process. For discussion purposes, the processes 500 and 600 are described with reference to the environment 100 of FIG. 1.

[0062] FIG. 5 illustrates a flow diagram that describes a process of establishing a session between a subject and a particular secure data container using a secure data corridor. In various examples, the subject may correspond to a user, a non-user entity, or another secure data corridor that requests permission to access data feeds within the particular secure data corridor. At 502, a resource management platform may receive a request from a subject to access data items within a secure data container. In some examples, the secure data container may be associated with a use case, whereby all data feeds within the secure data container retain a particular data sensitivity rating.

[0063] At 504, the resource management platform may authenticate an identity of the subject and determine whether access permissions to the secure data container have been granted. In some examples, access permissions may be associated with control parameters associated with data feeds. Further, permissions may be bound to specific control parameters stored in a list of triples that tie the subject to control parameters of data feeds. In other examples, access permissions may be tied to a use-case of the secure data container, such that the subject is permitted access to all data feeds associated with the use-case and/or the secure data container.

[0064] At 506, the resource management platform may determine that access permissions associated with the subject are sufficient to allow the subject access to the secure data container. The determination may be based at least in part on a comparison of the access permissions to the control parameters associate with data feeds within the secure data containers.

[0065] At 508, the resource management platform may establish a session link between the subject and the secure data container via secure data corridor. In various
examples, the secure data corridor may be assigned a data sensitivity rating that is based on a data sensitivity rating of data feeds within the secure data container. Alternatively, the data sensitivity rating may be locked by an administrator based at least in part on use-case for the secure data container.

[0066] FIG. 6 illustrates a flow diagram that describes a process of auto-leveling the data sensitivity rating of a secure data corridor based at least in part on the data sensitivity of transmitting data feeds. In other words, the resource management platform may detect the data sensitivity rating of data feeds that transmitting through the secure data corridor, and dynamically set a substantially similar data sensitivity rating for the secure data corridor.

[0067] At 602, the resource management platform may detect a data feed at an ingress point of a secure data corridor. In a non-limiting example, the ingress point may correspond to an endpoint at the subject, whereby the incoming data feed may be intended to transmit from the subject, via the secure data corridor, and to an adjoining secure data container. In another non-limiting example, the ingress point may correspond to the secure data container, whereby the incoming data feed may be intended to transmit from the secure data container, via the secure data corridor, and to the subject.

[0068] At 604, the resource management platform may determine that a data sensitivity rating of the data feed is more sensitive than the data sensitivity rating of the secure data corridor. In other words, the data feed may mandate more data security measures to maintain sufficient data confidentiality and data integrity than what is provided by the data sensitivity rating of the secure data corridor.

[0069] At 606, the resource management platform may dynamically set a data sensitivity rating for the secure data corridor that is substantially similar to that of the data feed. In
doing so, the confidentiality and the integrity of the data feed may not be compromised while transmitting through the secure data corridor.

CONCLUSION

[0070] Although the subject matter has been described in language specific to features and methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described herein. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claims.
WHAT IS CLAIMED:

1. A system of a resource management platform, comprising:
   one or more processors;
   memory coupled to the one or more processors, the memory including one or more modules that are executable by the one or more processors to:
   receive a message that includes a request from a subject to access a set of data items associated with a secure data container;
   identify a set of permissions associated with the subject based at least in part on the message, the message including a set of access permissions that authorize the subject to access the set of data items having a first data sensitivity rating;
   determine that the subject is authorized to access the secure data container based on a comparison of the set of access permissions and a second data sensitivity rating associated with the secure data container; and
   establish a secure data corridor between the subject and the secure data container, the secure data corridor having a third data sensitivity rating that is based at least in part on the first data sensitivity rating and the second data sensitivity rating.

2. The system of claim 1, wherein the set of data items is a first set of data items and the message is a first message, wherein the first message further includes a request for ingress of a second set of data items into the secure data container, and wherein the one or more modules are further executable by the one or more processors to:
   determine an additional data sensitivity rating associated with the second set of data items;
determine that the additional data sensitivity rating is more sensitive in comparison to the second data sensitivity rating of the secure data container, the second data sensitivity rating being a maximum threshold of sensitivity for ingress of the second set of data items into the secure data container; and

dynamically set the third data sensitivity rating of the secure data corridor to be substantially equivalent to the additional data sensitivity rating.

3. The system of claim 1, wherein the set of data items is a first set of data items and the message is a first message, wherein the first message further includes a request for ingress of a second set of data items into the secure data container, and wherein the one or more modules are further executable by the one or more processors to:

determine an additional data sensitivity rating associated with the second set of data items;

determine that the additional data sensitivity rating is more sensitive in comparison to the second data sensitivity rating of the secure data container, the second data sensitivity rating being a maximum threshold of sensitivity for ingress of the second set of data items into the secure data container;

determine that the third data sensitivity rating of the secure data corridor is locked; and

transmit a second message to the subject indicating that the second set of data items cannot securely transmit through the secure data corridor.

4. The system of claim 1, wherein the second data sensitivity rating associated with the secure data corridor is dynamically set to be at least substantially similar to the first data sensitivity rating associated with the secure data container.
5. The system of claim 1, wherein the second data sensitivity rating associated with the secure data corridor is based at least in part on individual control parameters associated with individual data feeds at an ingress point or an egress point of the secure data corridor, the individual control parameters including at least one of an explicit read provision, an explicit write provision, an explicit import provision, or explicit export provision.

6. The system of claim 5, wherein the individual control parameters are initially assigned to one or more data objects, wherein individual data objects of the one or more data objects are linked to one or more data elements, and the one or more data elements being further linked to the individual data feeds via a diagraph of connectivity.

7. The system of claim 1, wherein the set of data items is a first set of data items, and wherein the one or more modules are further executable by the one or more processors to:

   determine that the first data sensitivity rating associated with the subject is less sensitive in comparison to the second data sensitivity rating associated with the secure data container;

   determine that the subject is unauthorized to read data items within the secure data container, based at least in part on the first data sensitivity rating and the second data sensitivity rating; and

   configure the secure data corridor to prevent the secure data corridor from transmitting the first set of data items from the secure data container to the subject.
8. The system of claim 1, wherein the set of data items is a first set of data items and the message is a first message, wherein the first message further includes a request for ingress of a second set of data items to the secure data container, and wherein the one or more modules are further executable by the one or more processors to:

determine that the first data sensitivity rating associated with the subject is less sensitive in comparison to the second data sensitivity rating associated with the secure data container;

determine that the subject is authorized to write data items to the secure data container, based at least in part on comparing the first data sensitivity rating and the second data sensitivity rating; and

configure the secure data corridor to transmit the second set of data items from the subject to the secure data corridor.

9. A computer-implemented method, comprising:

under control of one or more processors:

receiving a request to from a subject to access a set of data items associated with a use case, the use case being associated with a secure data container;

determining that the subject is authorized to access the set of data items, based at least in part on access privileges of the subject and a first data sensitivity rating associated with the use case; and

establishing a secure data corridor between the subject and the secure data container, the secure data corridor having a second data sensitivity rating that is at least substantially similar to the first data sensitivity rating.
10. The computer-implemented method of claim 9, further comprising:

determining, via a scheduling algorithm, the second data sensitivity rating based at least in part on the first data sensitivity rating associated with the use case;

identifying control parameters associated with individual data items of the set of data items;

determining individual data sensitivity ratings for the individual data items, based at least in part on the control parameters;

determining that the individual data sensitivity ratings of a portion of the individual data items are at least substantially similar to the second data sensitivity rating of the secure data corridor, based at least in part on the control parameters associated with the portion of the individual data items; and

coming, the portion of the individual data items to transmit through the secure data corridor based at least in part on the individual data sensitivity ratings.

11. The computer-implemented method of claim 10, wherein the portion of the individual data items is a first portion of the individual data items, and further comprising:

determining that the individual data sensitivity ratings of a second portion of the individual data items are greater than the second data sensitivity rating of the secure data corridor; and

dynamically setting the second data sensitivity rating of the secure data corridor to be at least substantially similar to the individual data sensitivity ratings of the second portion of the individual data items.

12. The computer-implemented method of claim 10, wherein the portion of the individual data items is a first portion of the individual data items, and further comprising:
determining that the individual data sensitivity ratings of a second portion of the individual data items is more sensitive than the second data sensitivity rating of the secure data corridor, the second data sensitivity rating being a maximum threshold of sensitivity for transmission of data items through the secure data corridor; and

transmitting an indication to the subject indicating that content of the second portion of the individual data items cannot be securely transmitted through the secure data corridor.

13. One or more non-transitory computer-readable media storing computer-executable instructions, that when executed on one or more processors, causes the one or more processors to perform acts comprising:

receiving a request from a subject to access data feeds associated with a use case, the use case having a first data sensitivity rating;

determining that the subject is authorized to access data items associated with the use case; and

establishing, via a scheduling algorithm, a secure data corridor between the subject and a secure data container associated with the use case, the secure data corridor having a second data sensitivity rating that is greater than or equal to the first data sensitivity rating.

14. The one or more non-transitory computer-readable media of claim 14, further comprising:

generating a security label for individual data feeds that associate the individual data feeds with corresponding data elements, corresponding data objects, and assigned control parameters;
generating a linkage map-set of the individual data feeds that include a plurality of entries, wherein individual entries of the plurality of entries correspond to the security labels of the individual data feeds; and

auditing a data sensitivity of the individual data feeds being transmitted through the secure data corridor, the data sensitivity being based at least in part on security labels within the linkage map-set.

15. The one or more non-transitory computer-readable media of claim 14, wherein an assigned control parameter of the assigned control parameters corresponds to a particular data sensitivity rating, the assigned control parameter further comprising of a permission lattice of an explicit read provision, an explicit write provision, an explicit import provision, and an explicit export provision that corresponds to the particular data sensitivity rating relative to other data sensitivity ratings.
FIG. 2B
FIG. 3A

<table>
<thead>
<tr>
<th>Control</th>
<th>Up</th>
<th>Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Write</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

FIG. 3B
FIG. 4
RECEIVE A REQUEST FROM A SUBJECT TO ACCESS DATA ITEMS WITHIN A SECURE DATA CONTAINER ASSOCIATED WITH A USE CASE 502

AUTHENTICATE SUBJECT AND DETERMINE WHETHER ACCESS PERMISSIONS TO THE SECURE DATA CONTAINER HAVE BEEN GRANTED 504

DETERMINE THAT THE ACCESS PERMISSIONS ASSOCIATED WITH THE SUBJECT ARE SUFFICIENT TO GRANT THE SUBJECT ACCESS TO THE SECURE DATA CONTAINER 506

ESTABLISH A SESSION BETWEEN THE SUBJECT AND SECURE DATA CONTAINER VIA A SECURE DATA CORRIDOR 508

FIG. 5
Detect a data feed at an ingress point of a secure data corridor

Determine that the data sensitivity rating of the set of data elements is less sensitive to the data sensitivity rating of the secure data corridor

Dynamically change data sensitivity rating of the secure data corridor to match or exceed the data sensitivity rating associated with the first set of data elements

FIG. 6
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i, G06F 21/62(2013.01)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)

G06F 21/60; G06F 5/00; G06K 7/01; G06F 17/00; H04N 1/00; H04L 29/06; G06F 21/34; G06F 21/62; 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: request, access permission, authorize, secure data corridor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 8938775 B1 (GREGORY M. ROTH et al.) 20 January 2015 See column 2, line 3 - column 5, line 53; column 7, line 31 - column 9, line 42; claims 1-7, 15-16; and figures 1, 4.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>US 2006-0232826 A1 (HAGAI BAR-EL) 19 October 2006 See paragraphs [0072]-[0104]; and figures 2-3.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>US 8285983 B2 (MAGNUS HALLENSL et al.) 09 October 2012 See column 5, line 9 - column 6, line 13; claim V, and figures 2-3.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>US 8322610 B2 (SCOTT M. GUTHERY) 04 December 2012 See column 5, line 66 - column 7, line 64; and figure 2.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>WO 2014-130920 A1 (ACTIVIDENTITY, INC.) 28 August 2014 See page 16, line 29 - page 17, line 7; and figure 5.</td>
<td>1-15</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

Date of the actual completion of the international search
11 January 2017 (11.01.2017)

Date of mailing of the international search report
11 January 2017 (11.01.2017)

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
CHIN, Sang Burn
Telephone No. +82-42-481-8398

Form PCT/ISA/210 (second sheet) (January 2015)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 8938775 Bl</td>
<td>20/01/2015</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2006-109307 A3</td>
<td>14/06/2007</td>
</tr>
<tr>
<td>US 8285983 B2</td>
<td>09/10/2012</td>
<td>EP 2030400 Al</td>
<td>04/03/2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2030400 Bl</td>
<td>23/09/2015</td>
</tr>
<tr>
<td>US 8322610 B2</td>
<td>04/12/2012</td>
<td>EP 2406718 Al</td>
<td>18/01/2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2406718 A4</td>
<td>15/08/2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010-0230490 Al</td>
<td>16/09/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2010-105259 Al</td>
<td>16/09/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2959421 A4</td>
<td>02/11/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2016-0014116 Al</td>
<td>14/01/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2014-130920 A8</td>
<td>17/09/2015</td>
</tr>
</tbody>
</table>