US 20190347354A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2019/0347354 A1**

Huneycutt et al. (43) **Pub. Date: Nov. 14, 2019**

(54) **SYSTEM FOR MITIGATING INTENTIONAL AND UNINTENTIONAL EXPOSURE USING SOLUTION DATA MODELLING**

(71) Applicant: **Bank of America Corporation**, Charlotte, NC (US)

(72) Inventors: **Katy Leigh Huneycutt**, Oakboro, NC (US); **Richard LeRoy Hayes**, Charlotte, NC (US); **Aaron Dion Kephart**, Denver, NC (US)

(21) Appl. No.: **15/974,351**

(22) Filed: **May 8, 2018**

Publication Classification

(51) **Int. Cl.**

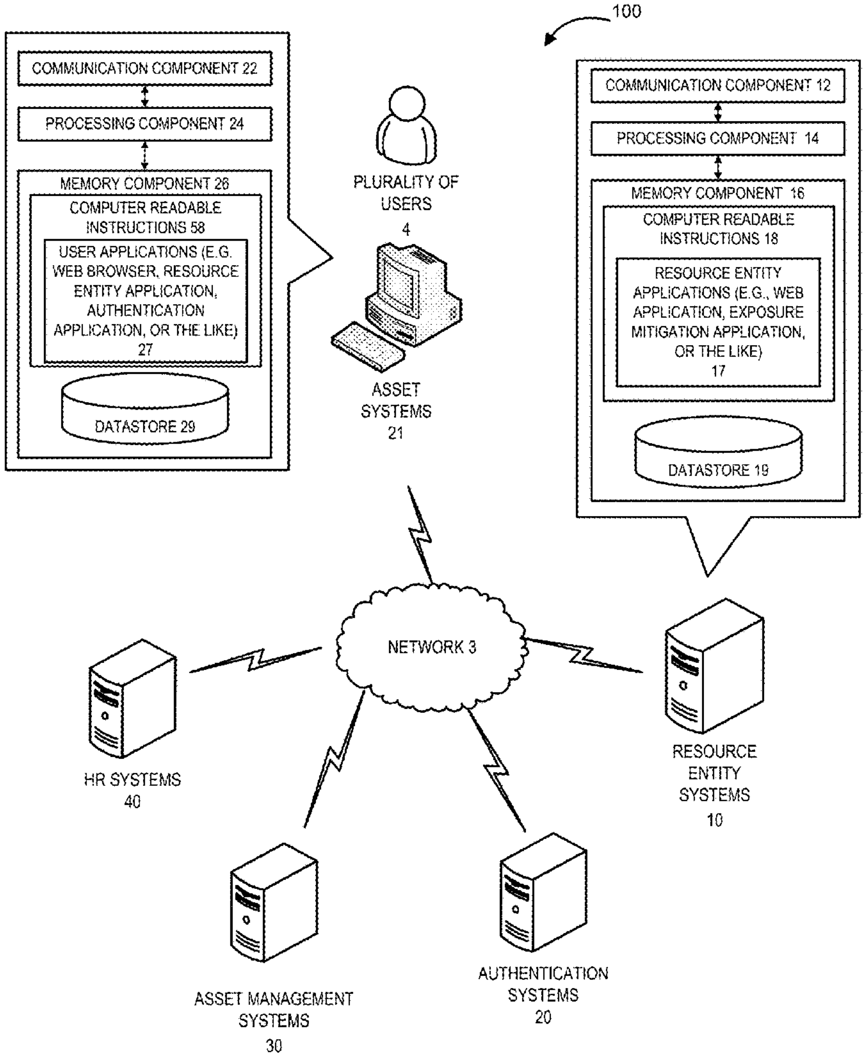
G06F 17/30	(2006.01)
H04L 29/06	(2006.01)
G06F 21/62	(2006.01)

(52) **U.S. Cl.**

CPC ***G06F 17/30604*** (2013.01); ***H04L 63/08*** (2013.01); ***H04L 63/20*** (2013.01); ***H04L 63/1425*** (2013.01); ***G06F 21/6218*** (2013.01)

(57) **ABSTRACT**

Embodiments of the present invention provide a system for mitigating intentional and unintentional exposures using solution data modelling. The system is typically configured for generating solution data models comprising a plurality of asset systems and a plurality of users, wherein each of the plurality of asset systems is associated with at least one user of the plurality of users and wherein at least a first of the plurality of asset systems is associated with at least a second of the plurality of asset systems, storing the solution data models in a model database, identifying an exposure associated with a user, accessing a solution data model associated with the user from the model database, identifying one or more relationships associated with the user from the solution data model, and implementing mitigation steps to mitigate the exposure associated with the user based on the one or more relationships.


100
COMMUNICATION COMPONENT 22
PROCESSING COMPONENT 24
MEMORY COMPONENT 26
COMPUTER READABLE INSTRUCTIONS 58
USER APPLICATIONS (E.G. WEB BROWSER, RESOURCE ENTITY APPLICATION, AUTHENTICATION APPLICATION, OR THE LIKE) 27
DATASTORE 29
PLURALITY OF USERS 4
ASSET SYSTEMS 21
COMMUNICATION COMPONENT 12
PROCESSING COMPONENT 14
MEMORY COMPONENT 16
COMPUTER READABLE INSTRUCTIONS 18
RESOURCE ENTITY APPLICATIONS (E.G., WEB APPLICATION, EXPOSURE MITIGATION APPLICATION, OR THE LIKE) 17
DATASTORE 19
NETWORK 3
HR SYSTEMS 40
RESOURCE ENTITY SYSTEMS 10
ASSET MANAGEMENT SYSTEMS 30
AUTHENTICATION SYSTEMS 20

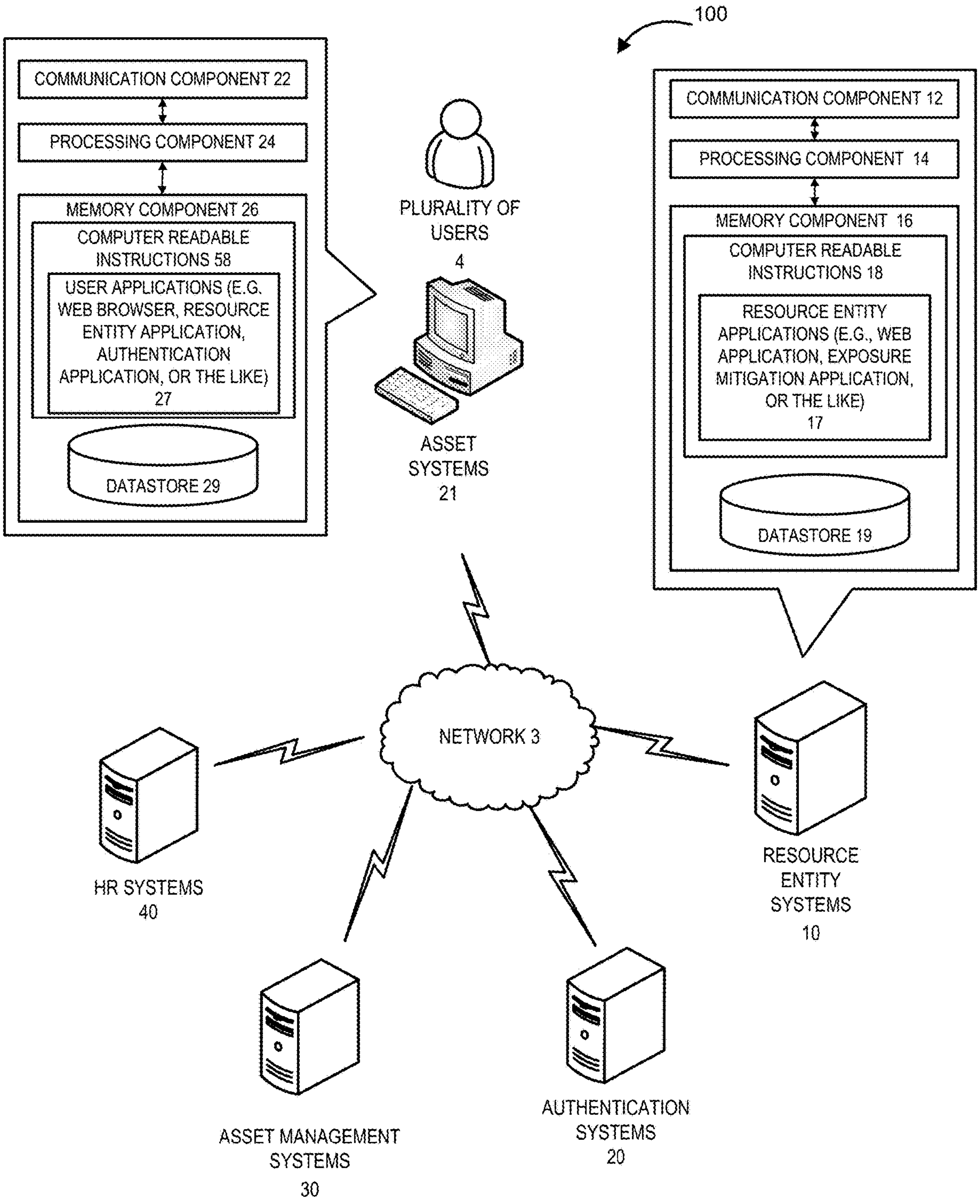

100
COMMUNICATION COMPONENT 22
PROCESSING COMPONENT 24
MEMORY COMPONENT 26
COMPUTER READABLE INSTRUCTIONS 58
USER APPLICATIONS (E.G. WEB BROWSER, RESOURCE ENTITY APPLICATION, AUTHENTICATION APPLICATION, OR THE LIKE) 27
DATASTORE 29
PLURALITY OF USERS 4
ASSET SYSTEMS 21
COMMUNICATION COMPONENT 12
PROCESSING COMPONENT 14
MEMORY COMPONENT 16
COMPUTER READABLE INSTRUCTIONS 18
RESOURCE ENTITY APPLICATIONS (E.G., WEB APPLICATION, EXPOSURE MITIGATION APPLICATION, OR THE LIKE) 17
DATASTORE 19
NETWORK 3
HR SYSTEMS 40
RESOURCE ENTITY SYSTEMS 10
ASSET MANAGEMENT SYSTEMS 30
AUTHENTICATION SYSTEMS 20

FIG. 1

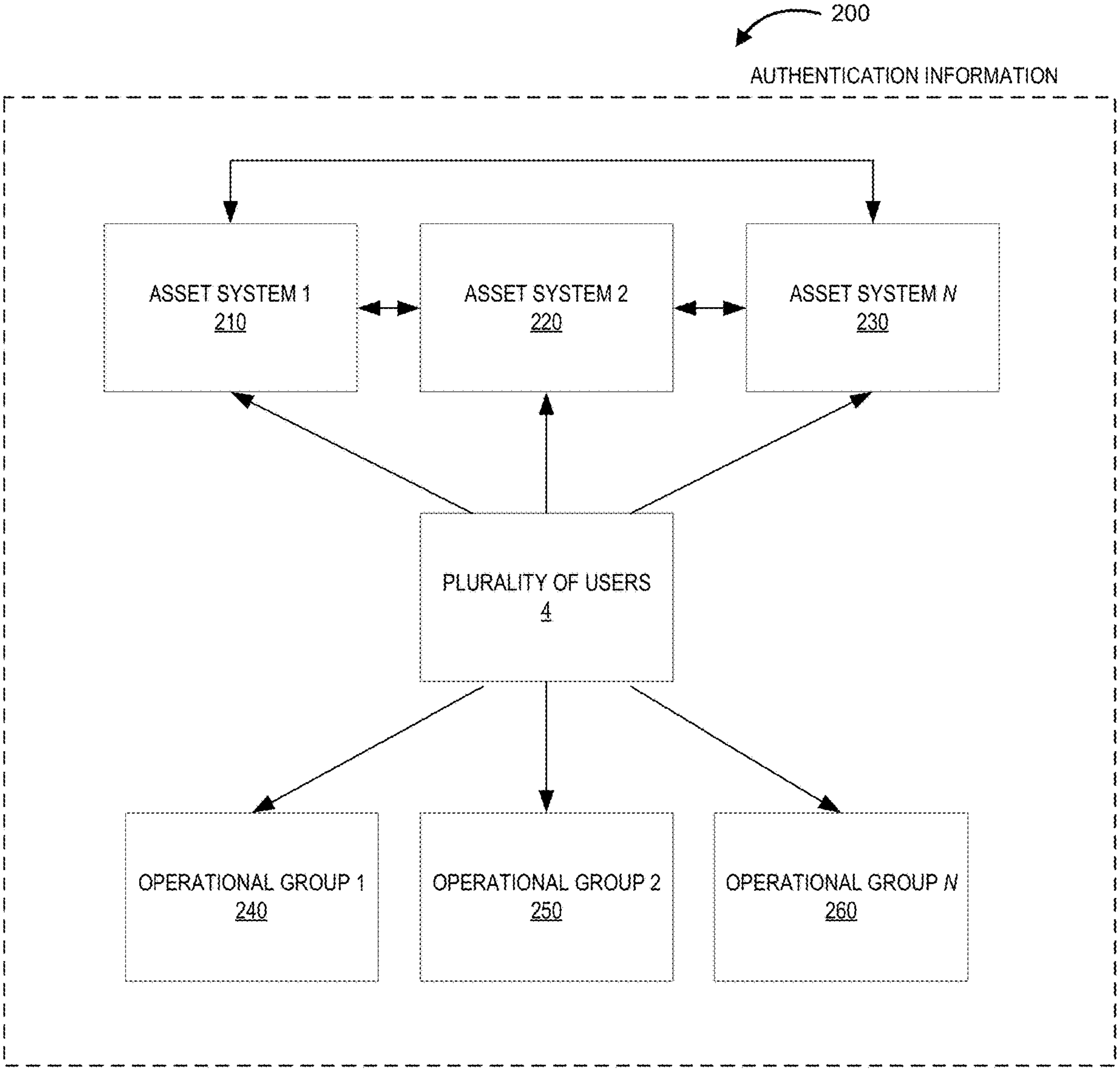

200
AUTHENTICATION INFORMATION
ASSET SYSTEM 1
210
ASSET SYSTEM 2
220
ASSET SYSTEM N
230
PLURALITY OF USERS
4
OPERATIONAL GROUP 1
240
OPERATIONAL GROUP 2
250
OPERATIONAL GROUP N
260

FIG. 2

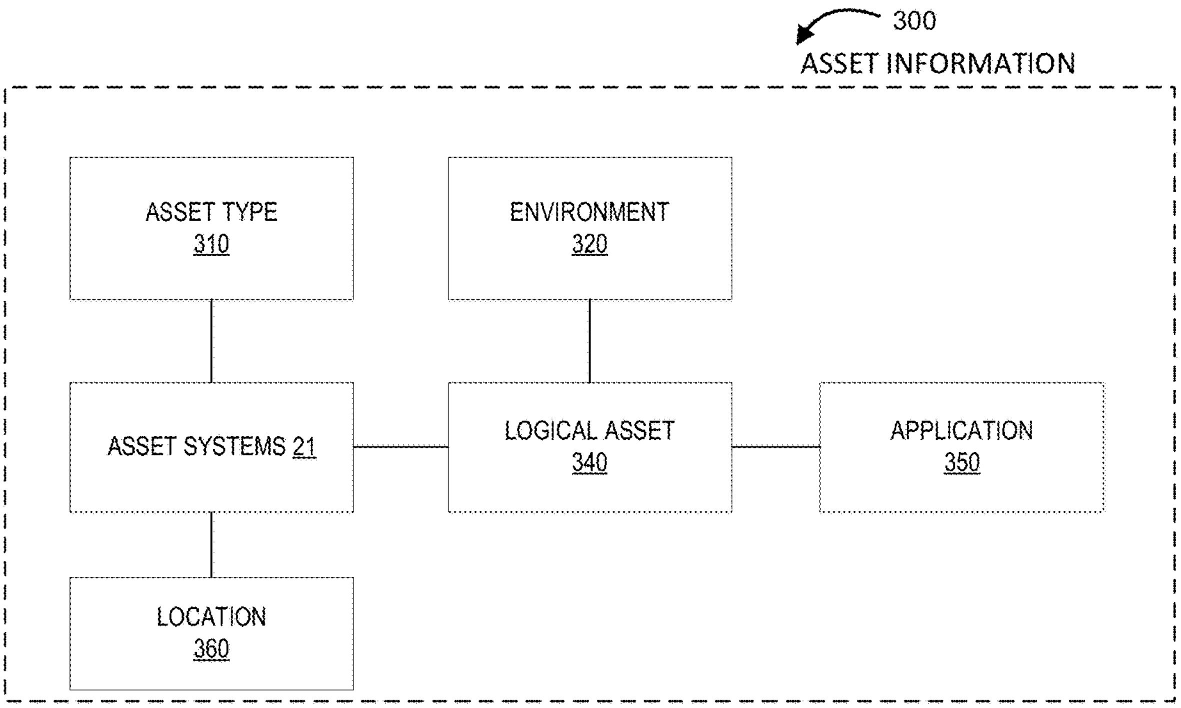

300
ASSET INFORMATION
ASSET TYPE
310
ENVIRONMENT
320
ASSET SYSTEMS 21
LOGICAL ASSET
340
APPLICATION
350
LOCATION
360

FIG. 3

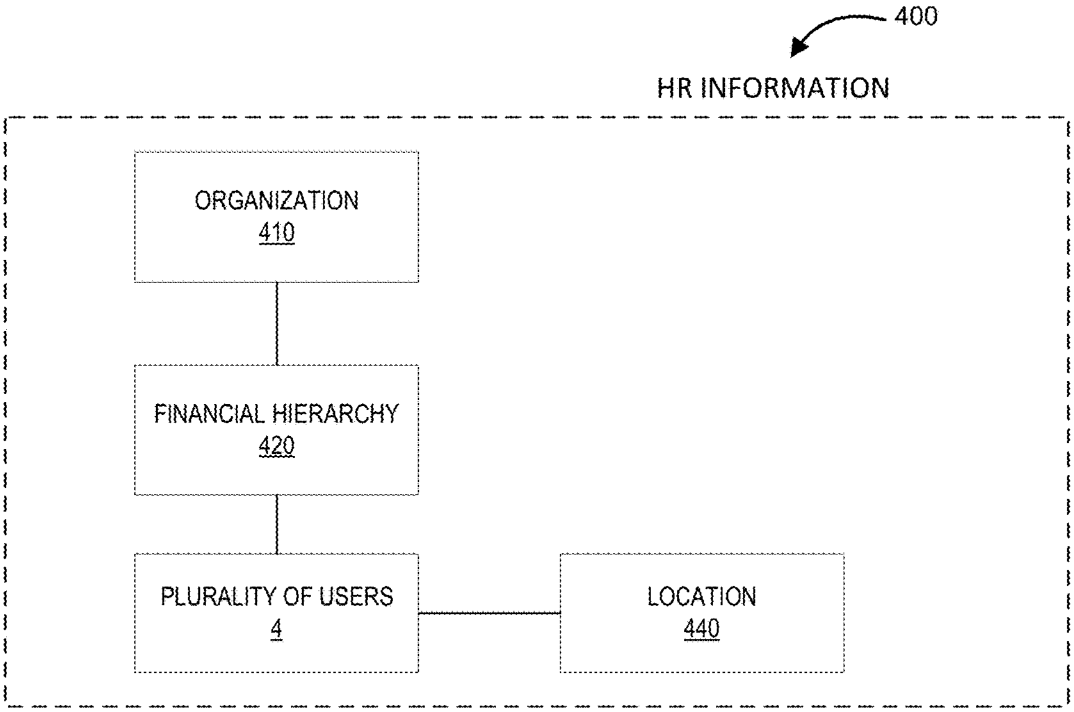

400
HR INFORMATION
ORGANIZATION
410
FINANCIAL HIERARCHY
420
PLURALITY OF USERS
4
LOCATION
440

FIG. 4

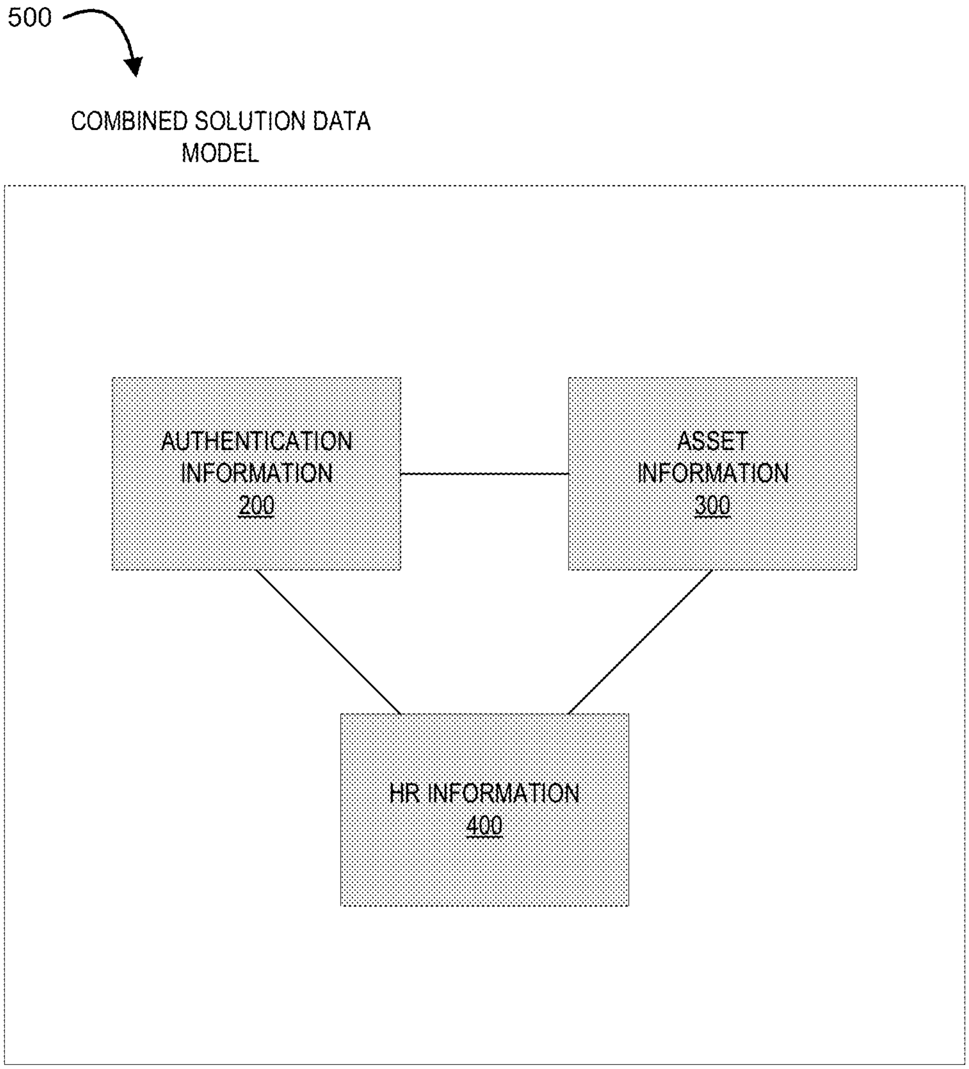

500
COMBINED SOLUTION DATA MODEL
AUTHENTICATION INFORMATION 200
ASSET INFORMATION 300
HR INFORMATION 400

FIG. 5

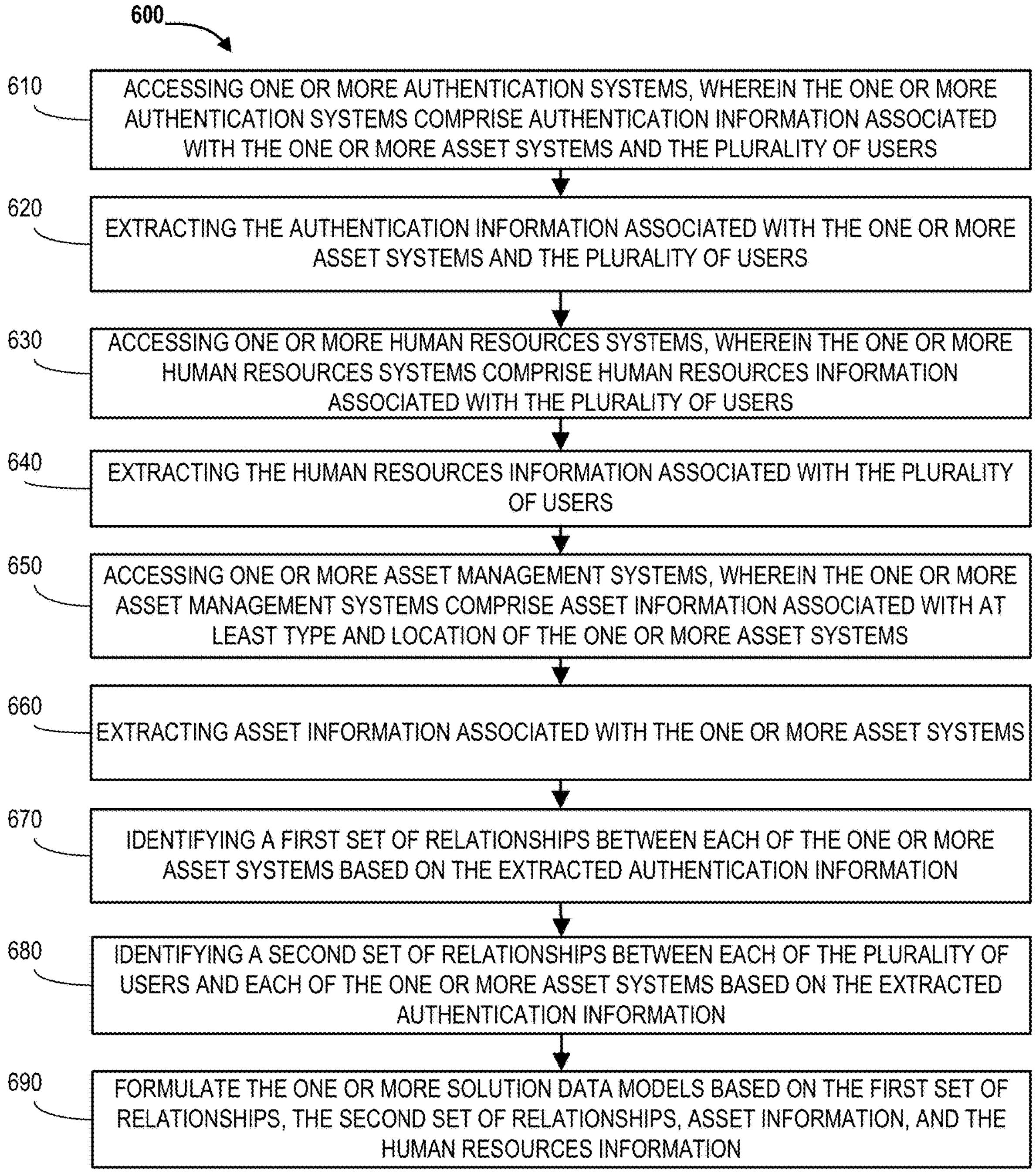

600
610
ACCESSING ONE OR MORE AUTHENTICATION SYSTEMS, WHEREIN THE ONE OR MORE AUTHENTICATION SYSTEMS COMPRISE AUTHENTICATION INFORMATION ASSOCIATED WITH THE ONE OR MORE ASSET SYSTEMS AND THE PLURALITY OF USERS
620
EXTRACTING THE AUTHENTICATION INFORMATION ASSOCIATED WITH THE ONE OR MORE ASSET SYSTEMS AND THE PLURALITY OF USERS
630
ACCESSING ONE OR MORE HUMAN RESOURCES SYSTEMS, WHEREIN THE ONE OR MORE HUMAN RESOURCES SYSTEMS COMPRISE HUMAN RESOURCES INFORMATION ASSOCIATED WITH THE PLURALITY OF USERS
640
EXTRACTING THE HUMAN RESOURCES INFORMATION ASSOCIATED WITH THE PLURALITY OF USERS
650
ACCESSING ONE OR MORE ASSET MANAGEMENT SYSTEMS, WHEREIN THE ONE OR MORE ASSET MANAGEMENT SYSTEMS COMPRISE ASSET INFORMATION ASSOCIATED WITH AT LEAST TYPE AND LOCATION OF THE ONE OR MORE ASSET SYSTEMS
660
EXTRACTING ASSET INFORMATION ASSOCIATED WITH THE ONE OR MORE ASSET SYSTEMS
670
IDENTIFYING A FIRST SET OF RELATIONSHIPS BETWEEN EACH OF THE ONE OR MORE ASSET SYSTEMS BASED ON THE EXTRACTED AUTHENTICATION INFORMATION
680
IDENTIFYING A SECOND SET OF RELATIONSHIPS BETWEEN EACH OF THE PLURALITY OF USERS AND EACH OF THE ONE OR MORE ASSET SYSTEMS BASED ON THE EXTRACTED AUTHENTICATION INFORMATION
690
FORMULATE THE ONE OR MORE SOLUTION DATA MODELS BASED ON THE FIRST SET OF RELATIONSHIPS, THE SECOND SET OF RELATIONSHIPS, ASSET INFORMATION, AND THE HUMAN RESOURCES INFORMATION

FIG. 6

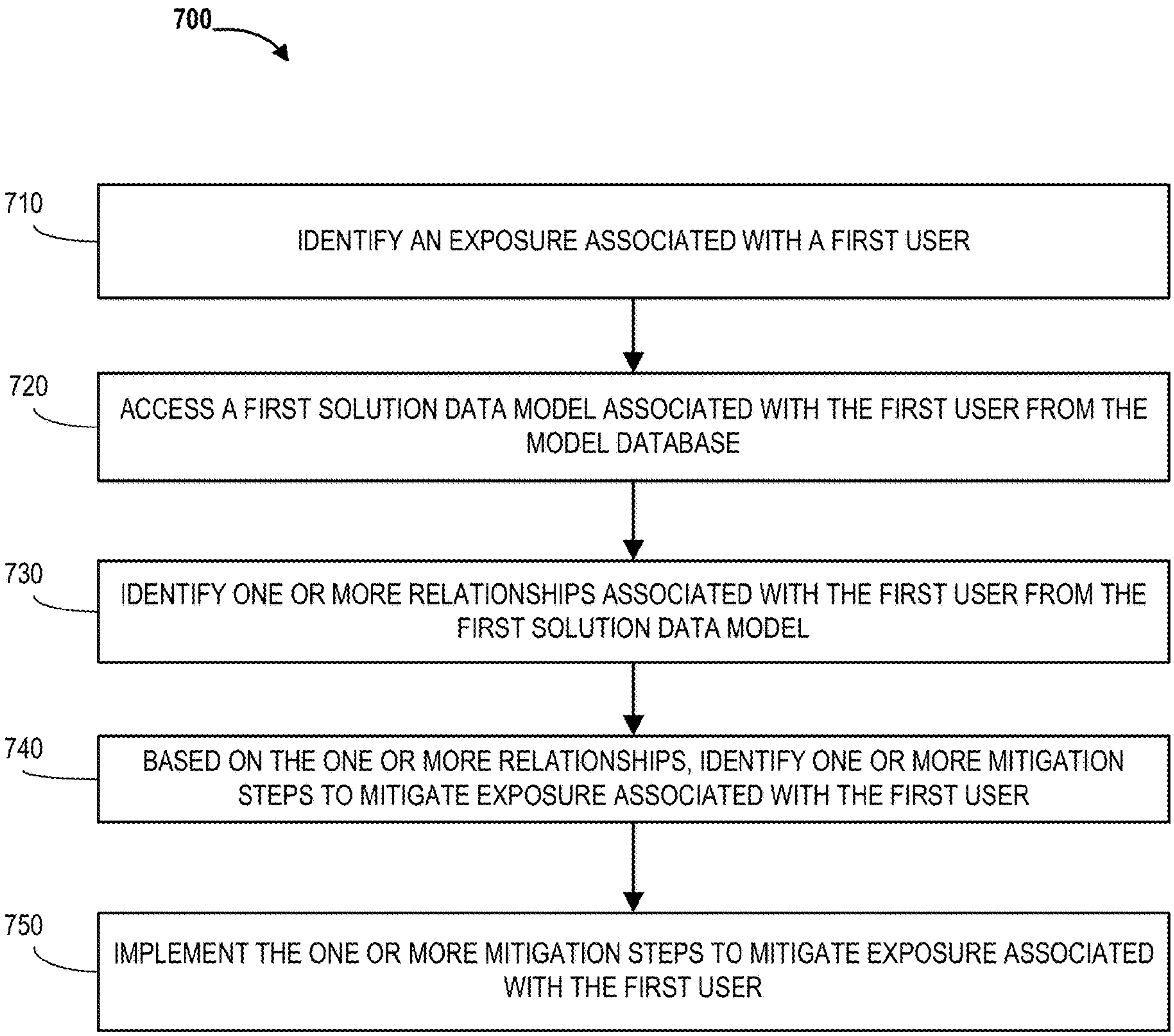

700
710
IDENTIFY AN EXPOSURE ASSOCIATED WITH A FIRST USER
720
ACCESS A FIRST SOLUTION DATA MODEL ASSOCIATED WITH THE FIRST USER FROM THE MODEL DATABASE
730
IDENTIFY ONE OR MORE RELATIONSHIPS ASSOCIATED WITH THE FIRST USER FROM THE FIRST SOLUTION DATA MODEL
740
BASED ON THE ONE OR MORE RELATIONSHIPS, IDENTIFY ONE OR MORE MITIGATION STEPS TO MITIGATE EXPOSURE ASSOCIATED WITH THE FIRST USER
750
IMPLEMENT THE ONE OR MORE MITIGATION STEPS TO MITIGATE EXPOSURE ASSOCIATED WITH THE FIRST USER

FIG. 7

SYSTEM FOR MITIGATING INTENTIONAL AND UNINTENTIONAL EXPOSURE USING SOLUTION DATA MODELLING

FIELD

[0001] The present invention relates to mitigating intentional and unintentional exposures using solution data modelling.

BACKGROUND

[0002] Present conventional systems do not have the capability to identify all existing relationships within an entity. Lack of sufficient information associated with one or more relationships within an entity makes it difficult to mitigate intentional and unintentional exposures within the entity. As such, there exists a need for a system to identify all existing relationships within the entity and to mitigate intentional and unintentional exposures arising within the entity.

SUMMARY

[0003] The following presents a simplified summary of one or more embodiments of the present invention, in order to provide a basic understanding of such embodiments. This summary is not an extensive overview of all contemplated embodiments, and is intended to neither identify key or critical elements of all embodiments nor delineate the scope of any or all embodiments. Its sole purpose is to present some concepts of one or more embodiments of the present invention in a simplified form as a prelude to the more detailed description that is presented later.

[0004] Embodiments of the present invention address the above needs and/or achieve other advantages by providing apparatuses (e.g., a system, computer program product and/or other devices) and methods for mitigating intentional and unintentional exposures using solution data modelling. The invention generates one or more solution data models comprising a plurality of asset systems and a plurality of users, wherein each of the plurality of asset systems is associated with at least one user of the plurality of users and wherein at least a first of the plurality of asset systems is associated with at least a second of the plurality of asset systems, stores the one or more solution data models in the model database, identifies an exposure associated with a first user, accesses a first solution data model associated with the first user from the model database, identifies one or more relationships associated with the first user from the first solution data model, and based on the one or more relationships, implements one or more mitigation steps to mitigate the exposure associated with the first user.

[0005] In some embodiments, the invention generates the one or more solution data models by accessing one or more authentication systems, wherein the one or more authentication systems comprise authentication information associated with the plurality of asset systems and the plurality of users, extracting the authentication information associated with the plurality of asset systems and the plurality of users, accessing one or more human resources systems, wherein the one or more human resources systems comprise human resources information associated with the plurality of users, extracting the human resources information associated with the plurality of users, accessing one or more asset management systems, wherein the one or more asset management systems comprise asset information associated with at least type and location of the plurality of asset systems, extracting the asset information associated with plurality of asset systems, identifying a first set of relationships between each of the plurality of asset systems based on the extracted authentication information, identifying a second set of relationships between each of the plurality of users and each of the plurality of asset systems based on the extracted authentication information, and formulating the one or more solution data models based on the first set of relationships, the second set of relationships, the asset information, and the human resources information.

[0006] In some embodiments, the invention identifies the exposure by monitoring the plurality of asset systems and user activity of the plurality of users and identifying abnormal activity based on monitoring the plurality of asset systems and the plurality of users, wherein the abnormal activity is identified based on a set of rules.

[0007] In some embodiments, the invention identifies the exposure based on receiving an input from a user.

[0008] In some embodiments, the invention identifies the one or more relationships associated with the first user by identifying at least one first asset associated with the first user, identifying upstream asset systems and downstream asset systems linked with the at least one first asset, identifying at least one first application associated with the first user, and identifying upstream applications and downstream applications linked with the at least one first application.

[0009] In some embodiments, the invention implements the one or more mitigation steps by identifying that at least one asset system of the upstream asset systems and the downstream asset systems comprises confidential data and restricting access to the at least one asset system.

[0010] In some embodiments, the invention implements the one or more mitigation steps by monitoring communications associated with the first user, identifying that at least one of the communications comprises confidential data, and blocking at least one of the communications comprising the confidential data.

[0011] In some embodiments, the exposure is at least one of an intentional exposure or an unintentional exposure.

[0012] The features, functions, and advantages that have been discussed may be achieved independently in various embodiments of the present invention or may be combined with yet other embodiments, further details of which can be seen with reference to the following description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Having thus described embodiments of the invention in general terms, reference will now be made to the accompanying drawings, where:

[0014] FIG. **1** presents a block diagram illustrating the exposure mitigation system environment, in accordance with embodiments of the present invention.

[0015] FIG. **2** presents a block diagram illustrating authentication information present in one or more authentication systems, in accordance with embodiments of the present invention.

[0016] FIG. **3** presents a block diagram illustrating asset information present in one or more asset management systems, in accordance with embodiments of the present invention.

[0017] FIG. **4** presents a block diagram illustrating human resources information present in one or more human resources systems, in accordance with embodiments of the present invention.

[0018] FIG. **5** presents a block diagram illustrating a combined solution data model generated by a resource entity system, in accordance with embodiments of the present invention.

[0019] FIG. **6** presents a process flow illustrating generation of combined solution data model, in accordance with embodiments of the present invention.

[0020] FIG. **7** presents a process flow for mitigating intentional and unintentional exposures, in accordance with embodiments of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0021] Embodiments of the invention will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all, embodiments of the invention are shown. Indeed, the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of one or more embodiments. It may be evident; however, that such embodiment(s) may be practiced without these specific details. Like numbers refer to like elements throughout.

[0022] Systems, methods, and computer program products are herein disclosed that provide for creating relationships between multiple asset systems, plurality of users, one or more applications, one or more logical assets, and/or the like leveraging existing data sets in one or more systems associated with a resource entity. Conventional systems utilize auto discovery tools to create the above mentioned relationships. However, the conventional auto discovery tools identify relationships between multiple asset systems by crawling into multiple systems based on a set of rules and accessing configuration files, or the like and cannot identify all existing relationships within an entity. The conventional auto discovery tools cannot identify relationships between the multiple asset systems and the one or more logical assets, one or more applications, and the plurality of users associated with the entity. Additionally, the conventional auto discovery tools are difficult to install, configure, and manage. The present system leverages already existing data within HR systems, asset management systems, and authentication systems providing authentication for the multiple asset systems, plurality of users, one or more applications, or the like to create combined solution data models comprising relationships between multiple asset systems, plurality of users, one or more applications, one or more logical assets.

[0023] Insider threats may be intentional or unintentional. Containing all insider threats or exposures can be challenging without having knowledge about a user and an application or an asset system associated with the user are linked with other asset systems, other users, and other applications within the entity. Present conventional systems do not have the capability to effectively contain insider threats and exposures. The present invention utilizes the generated solution data models to effectively identify how asset systems, applications, and users are linked with a user associated with an exposure and mitigate the exposure by performing one or more mitigation steps.

[0024] In accordance with embodiments of the invention, the terms "resource entity system" or "resource entity" may include any organization that processes financial transactions including, but not limited to, banks, credit unions, savings and loan associations, card associations, settlement associations, investment companies, stock brokerages, asset management firms, insurance companies and the like.

[0025] Many of the example embodiments and implementations described herein contemplate interactions engaged in by a user with a computing device and/or one or more communication devices and/or secondary communication devices. A "user", as referenced herein, may refer to an entity or individual that has the ability and/or authorization to access and use one or more resources or portions of a resource. In some embodiments, the "user" or "plurality of users" may be one or more associates, employees, agents, contractors, sub-contractors, third-party representatives, customers, and/or the like. Furthermore, as used herein, the term "asset systems" or "asset" may refer to mobile phones, computing devices, tablet computers, wearable devices, smart devices and/or any portable electronic device capable of receiving and/or storing data therein.

[0026] A "user interface" is any device or software that allows a user to input information, such as commands or data, into a device, or that allows the device to output information to the user. For example, the user interface include a graphical user interface (GUI) or an interface to input computer-executable instructions that direct a processing device to carry out specific functions. The user interface typically employs certain input and output devices to input data received from a user second user or output data to a user. These input and output devices may include a display, mouse, keyboard, button, touchpad, touch screen, microphone, speaker, LED, light, joystick, switch, buzzer, bell, and/or other user input/output device for communicating with one or more users.

[0027] A "system environment", as used herein, may refer to any information technology platform of an enterprise (e.g., a national or multi-national corporation) and may include a multitude of servers, machines, mainframes, personal computers, network devices, front and back end systems, database system and/or the like.

[0028] FIG. **1** illustrates a exposure mitigation system environment **100**, in accordance with embodiments of the invention. As illustrated in FIG. **1**, one or more resource entity systems **10** are operatively coupled, via a network **3**, to asset systems **21**, authentication system **20**, asset management systems **30**, and human resources (HR) systems **40**. In this way, the plurality of users **4** (e.g., one or more associates, employees, agents, contractors, sub-contractors, third-party representatives, customers, or the like), through a user application **27** (e.g., web browser, resource entity application, authentication application, or the like), may access the asset systems **21** and other resource entity applications **17** (web application, exposure mitigation application, or the like) of the asset systems **21**. In some embodiments, the exposure mitigation application may be a part of an independent exposure mitigation system. In such an embodiment, the independent exposure mitigation system is maintained and operated by the resource entity systems **10**. The independent exposure mitigation system may comprise one or more processing devices operatively coupled to the one or more memory devices and configured to execute computer readable code stored in the one or more memory devices.

[0029] The network **3** may be a global area network (GAN), such as the Internet, a wide area network (WAN), a local area network (LAN), or any other type of network or combination of networks. The network **3** may provide for wireline, wireless, or a combination of wireline and wireless communication between systems, services, components, and/or devices on the network **3**.

[0030] As illustrated in FIG. **1**, the resource entity systems **10** generally comprise one or more communication components **12**, one or more processing components **14**, and one or more memory components **16**. The one or more processing components **14** are operatively coupled to the one or more communication components **12** and the one or more memory components **16**. As used herein, the term "processing component" generally includes circuitry used for implementing the communication and/or logic functions of a particular system. For example, a processing component **14** may include a digital signal processor component, a microprocessor component, and various analog-to-digital converters, digital-to-analog converters, and other support circuits and/or combinations of the foregoing. Control and signal processing functions of the system are allocated between these processing components according to their respective capabilities. The one or more processing components **14** may include functionality to operate one or more software programs based on computer-readable instructions **18** thereof, which may be stored in the one or more memory components **16**. The authentication systems **20**, the asset management systems **30**, the human resources systems **40** may comprise similar structure and components as of the resource entity system **10** such as one or more communication components, one or more processing components, and one or more memory components.

[0031] The one or more processing components **14** use the one or more communication components **12** to communicate with the network **3** and other components on the network **3**, such as, but not limited to, the components of the asset systems **21**, the authentication systems **20**, asset management systems **30**, HR systems **40**, or other systems. As such, the one or more communication components **12** generally comprise a wireless transceiver, modem, server, electrical connection, electrical circuit, or other component for communicating with other components on the network **3**. The one or more communication components **12** may further include an interface that accepts one or more network interface cards, ports for connection of network components, Universal Serial Bus (USB) connectors and the like.

[0032] As further illustrated in FIG. **1**, the resource entity systems **10** comprise computer-readable instructions **18** stored in the memory component **16**, which in one embodiment includes the computer-readable instructions **18** of the resource entity application **17** (e.g., website application, exposure mitigation application, or the like). In some embodiments, the one or more memory components **16** include one or more data stores **19** for storing data related to the resource entity systems **10**, including, but not limited to, data created, accessed, and/or used by the resource entity application **17**. In embodiments of the present invention, the one or more data stores store the information extracted from the authentication systems **20**, asset management systems **30**, HR management systems **40**, and/or the like. In some embodiments, information associated with the one or more assets, one or more applications and logical assets, the plurality of users is gathered by the resource entity applications **17** by communicating with other resource entity systems such as HR systems **40**, asset management systems **30**, authentication systems **40**, and/or other systems associated with the resource entity. Additionally, the resource entity systems **10** comprise an artificial intelligence engine stored in the memory component **16** to generate one or more combined solution data models, in accordance with embodiments of the present invention. In embodiments of the present invention, the memory component **16** comprises a model database comprising the generated one or more combined solution data models.

[0033] As illustrated in FIG. **1**, the plurality of users **4** may access the resource entity application **17**, or other applications, through the asset systems **21**. The asset systems **21** may be a desktop, mobile device (e.g., laptop, smartphone device, PDA, tablet, or other mobile device), or any other type of computer that generally comprises one or more communication components **22**, one or more processing components **24**, and one or more memory components **26**. In some embodiments, the asset systems **21** may be servers. In some embodiments, the asset systems **21** may be cloud servers. In some embodiments, the asset systems may be repositories and/or the like.

[0034] The one or more processing components **24** are operatively coupled to the one or more communication components **22** and the one or more memory components **26**. The one or more processing components **24** use the one or more communication components **22** to communicate with the network **3** and other components on the network **3**, such as, but not limited to, the resource entity systems **10**, the authentication systems **20**, the HR systems **40**, the asset management systems **30**, and/or other systems. As such, the one or more communication components **22** generally comprise a wireless transceiver, modem, server, electrical connection, or other component for communicating with other components on the network **3**. The one or more communication components **22** may further include an interface that accepts one or more network interface cards, ports for connection of network components, Universal Serial Bus (USB) connectors and the like. Moreover, the one or more communication components **22** may include a keypad, keyboard, touch-screen, touchpad, microphone, mouse, joystick, other pointer component, button, soft key, and/or other input/output component(s) for communicating with the users **4**.

[0035] As illustrated in FIG. **1**, the asset systems **21** may have computer-readable instructions **28** stored in the one or more memory components **26**, which in one embodiment includes the computer-readable instructions **28** for user applications **27**, such as authentication application (e.g., apps, applet, or the like), other resource entity applications, a web browser or other apps that allow the plurality of users **4** to take various actions, including allowing the plurality of users **4** to access applications located on other systems, or the like. The one or more memory components **26** comprise one or more data stores **29** to store data accessed by the asset systems **21** or data required to perform one or more processes or operations assigned to the asset systems **21**. In some embodiments, the plurality of users utilizes the user applications **27**, through the asset systems **21**, to access the resource entity applications **17** to perform various day to day organizational processes. In some embodiments, plurality of users **4** may utilize a HR application to store human resources information in the HR systems **40**. In some embodiments, the plurality of users **4** may utilize asset management application to add information about new asset systems, delete information associated with old asset systems, modify location of the existing asset systems, and/or the like.

[0036] FIG. **2** presents a block diagram **200** illustrating authentication information present in one or more authentication systems **20**. The one or more authentication systems **20** are any systems which control authorizations and authentications within the resource entity. The one or more authentication systems comprise authentication information and authorization information associated with one or more asset systems **21**, plurality of users **4**, one or more applications, and/or the like. Typically one or more asset systems **21** (such asset system **1 210**, asset system **2 220**, and asset system N **230**) within an entity communicate with each other to implement multiple processes. For the one or more asset systems **21** to communicate with each other, authentication is necessary. For example, asset system **1 210** may access asset system **2 220** only after successful authentication. The one or more authentication systems **20** facilitate authentication between asset system **1 210** and asset system **2 220**, wherein the authentication between asset system **1 210** and asset system **2 220** may be unidirectional or bidirectional. In some embodiments, the one or more authentication systems **20** may receive a request from asset system **1 210** to access asset system **2 220**. Upon receiving the request, the one or more authentication systems **20** access a data store comprising approved authorizations within the resource entity, determine that the asset system **1 210** has authorization to access asset system **2 220**, and authorize asset system **1 210** to access asset system **2 220**. Approval for authorizations may be provided by a user of the plurality of users. Similarly, the one or more authentication systems provide authentication between plurality of users **4** and the one or more asset systems **21**. For example, a user of the plurality of users **4** may send a request to the one or more authentication systems to access any one of the asset systems **21**. The plurality of users **4** may belong to one or more organizational groups (organizational group **1 240**, organizational group **2 250**, operational group N **260**). Organizational group may be defined as a group with multiple users belonging to a line of business. In one example, a group of users associated with human resources department are associated with human resources organizational group. In some embodiments, the authorizations to asset systems may be based on the organizational groups of the plurality of users. For example, ‘n’ number of users associated with organization group **1 240** may have authorization to access asset system **1 210**. In some embodiments, the one or more authorization systems **20** may facilitate access between one or more applications within a resource entity. In some embodiments, the one or more authorization systems **20** may facilitate access between one or more applications within the entity and the plurality of users **4**. In some embodiments, the one or more authorization systems **20** may facilitate access between one or more applications within the entity and the one or more asset systems **21**.

[0037] FIG. **3** presents a block diagram **300** illustrating asset information present in one or more asset management systems **30**. The one or more asset management systems **30** are any systems which manage and control one or more asset systems **21** within the resource entity. The one or more asset management systems **30** comprise information associated with the one or more asset systems **21** and the one or more applications within the resource entity. The one or more applications may be any software applications owned, maintained or utilized by the resource entity. In some embodiments, the one or more asset management systems **30** comprise information associated with asset type **310**, environment **320**, logical asset **340**, application **350**, and location **360** of the one or more asset systems **21**. Asset type **310** defines the type of the one or more asset systems **21**. For example, the one or more asset management systems **30** comprise information associated with the type of asset system **1 210** shown in FIG. **2**, wherein the asset system **1 210** may be a repository. The one or more assets systems **21** may be repositories, relationship management systems, transaction systems, knowledge management systems, business intelligence systems, user systems assigned to the plurality of users **4**, and/or the like. In one embodiment, the one or more asset management systems **30** comprise information associated with environment **320** of the one or more asset systems **21**. Environment **320** may define operating system properties, physical properties, software properties, and/or the like of the one or more asset systems **21**. In one embodiment, the one or more asset management systems **30** comprise information associated with location **360** of the one or more asset systems **21**. For example, the one or more asset management systems **30** comprise physical address including country, state, city, street address, building number, floor number, cubicle location, and/or the like associated with the location of the asset system **1 210**. In one embodiment, the one or more asset management systems **30** comprise information with logical assets **340** associated with the one or more asset systems **21**. Logical asset information **340** may include logical partitions, virtual assets, and/or the like associated with each of the one or more asset systems **21**. For example, asset system **1 210** may be configured into one or more virtual assets which may be utilized by any of the plurality of users **4** from any network associated with the resource entity. In one embodiment, the one or more asset management systems **30** comprise information with applications **360** associated with the one or more asset systems **21**.

[0038] FIG. **4** presents a block diagram **400** illustrating presents a block diagram illustrating human resources information present in one or more human resources systems **40**. The one or more human resources systems **40** may be any systems utilized by the human resources organization group within the resource entity. The one or more human resources systems comprise information associated with the plurality of users **4** within the resource entity. In one embodiment, the one or more human resources systems **40** comprise information associated with organization **410** of the plurality of users **4**. The plurality of users **4** may be agents, contractors, sub-contractors, third-party representatives, and/or the like. Contractors, sub-contractors, third party representatives, may be associated with third party entities. For example, the one or more human resources systems may comprise organization information **410** associated with a first user of the plurality of users **4**. The first user may be associated with a first third party entity, wherein the third party entity provides one or more contractors to the resource entity. In one embodiment, the one or more human resources systems **40** may comprise information associated with hierarchy information **420** associated with the plurality of users **4**. For example, the one or more human resources systems **40** may comprise hierarchy information **420** associated with each of the plurality of users **4** such as one or more users reporting to a first user of the plurality of users **4**, a reporting manager associated with the first user, one or more applications managed by the first user, and/or the like. In one embodiment, the one or more human resources systems **40** may comprise information associated with location **440** of each of the plurality of users **4**. For example, the one or more human resources systems **40** comprise location information **440** associated with a first user of the plurality of users **4** such as work location address including country, state, city, street address, building number, floor number, cubicle location, and/or the like. In some embodiments, the one or more human resources systems **40** comprise all work locations associated with each of the plurality of users including the home work address, country, state, city, street address, building number, floor number, cubicle location, IP address, and/or the like.

[0039] FIG. **5** presents a block diagram **500** illustrating a combined solution data model generated by the artificial intelligence engine of the resource entity system **10**. The resource entity system **10** extracts authentication information **200** from the one or more authentication systems **20**, asset information **300** from the one or more asset management systems **30**, human resources information **400** from the one or more human resources systems **40**, and/or the like. The artificial intelligence engine intelligently applies logic to the extracted information from one or more systems and formulates a combined solution data model comprising one or more relationships between one or more assets systems **21**, the plurality of users **4**, and one or more logical assets and applications within the resource entity. In some embodiments, the combined solution data model may be stored in the form of database tables. The combined solution data models may be stored in any of available operational databases, relational databases, distribute databases, key value databases, column oriented databases, cloud database, big data, mobile database, active database, parallel database, virtual database, centralized database, navigational database, and/or the like. In some other embodiments, the combined solution data model may be stored in a data store in the form of tree data structure. In some embodiments, the combined solution data model may be split into multiple trees and each of the multiple trees may be linked with other multiples trees based on the one or more relationships. In some embodiment, the combined solution data model is in the form of a web. In some embodiments, the combined solution data model may be stored in the form of a list. In some embodiments, the combined solution data model may be stored in the form of any available data structures used to representing the one or more relationships. In some other embodiments, the combined solution data models may be stored in any graphical form in the data store of the system. In some embodiments, the combined solution data models is an integrated semantic model. In some embodiments, the combined solution data models is a schema model.

[0040] FIG. **6** presents a process flow **600** illustrating generation of combined solution data model by the artificial intelligence engine of the resource entity system **10**. As shown in block **610**, the system accesses one or more authentication systems, wherein the one or more authentication systems comprise authentication information associated with the one or more asset systems and the plurality of users **4**. The authentication information may be stored in a data store of the authentication system and the system may access the data store of the one or more authentication system. In some embodiments, the one or more authentication systems may authorize the system to access the authentication information stored in the data store of the one or more authentication systems. As shown in block **620**, the system extracts the authentication information associated with the one or more asset systems and the plurality of users. In some embodiments, the extracted information may include only active authentications present in the data store. Active authentications may be any authentication used by the plurality of users or the one or more asset systems or the one or more applications or logical assets associated with the resource entity within a predetermined amount of time. In some embodiments, the predetermined amount of time may be assigned by the resource entity. For example, the system may assign twelve months are the predetermined amount of time. In some embodiments, the system may perform routine maintenance on the one or more authentication systems **20** at regular intervals and delete all inactive forms of authentication present in the one or more authentication systems, thereby having the information ready for extraction during the process of generation of the combined solution data models. In such embodiments, the system may delete the inactive authentications only after receiving an approval from a relevant user. The relevant user may be associated with a first asset system or a first user associated with the inactive authentication. For example, the inactive authentication may be associated with a user who is not associated with the resource entity. The system may identify a reporting manager assigned to the user and may send the reporting manager a request for approval to delete the inactive authentication. In some embodiments, the authentication information may include reference identifiers associated with the plurality of users **4**, the one or more asset systems **21**, the one or more applications or logical assets, and/or the like. In some embodiments, the authentication information may include historical data logs comprising all authentications approved by the one or more authentication systems.

[0041] As shown in block **630**, the system accesses the one or more human resources systems, wherein the one or more human resources systems comprise human resources information associated with the plurality of users. Human resources information may be inputted into the one or more human resources systems **40** by one or more plurality of users associated with human resources organizational group. The human resources information may include location information, hierarchy information, organization information, personal information, and/or the like. As shown in block **640**, the system extracts the human resources information associated with the plurality of users. The system upon extracting the human resources information may sort the human resources information and store it in the data store of the system based on the human resources identifier, thereby providing easy retrieval of human resources information during the process of generation of combined solution data models.

[0042] As shown in block **650**, the system accesses the one or more asset management systems, wherein the one or more asset management system comprises asset information associated with at least the type and location of the one or more asset systems. The asset information may also include environment information, logical asset information, application information, and/or the like associated with the one or more asset systems **21**. The asset information may include information associated with whether the one or more asset systems **21** or one or more applications associated with the one or more asset systems **21** include confidential data or not. As shown in block **660**, the system extracts asset information associated with the one or more asset systems. The system, after extracting the asset information, may sort the asset information and may store it in the data store of the system based on asset reference identifier, thereby providing easy retrieval of asset information during the process of generation of combined solution data models.

[0043] As shown in block **670**, the system identifies a first set of relationships between each of the one or more asset systems based on the extracted authentication information. The first set of relationships may include all forms of active authentication records present in the extracted authentication information between each of the one or more asset systems based on the historical data log information extracted from the one or more authentication systems. For example, the system may identify all entries in the historical data log information associated with a first asset reference identifier. In some embodiments, the system, after identifying the first set of relationships, may place the first set of relationships in temporary storage of the system such as random access memory for easy retrieval. In such embodiments, the system may identify duplicate relationships from the first set of relationships and may delete the duplicate relationships before storing the first set of relationships in the data store. For example, the system may identify all entries in the historical log information associated with a first reference identifier and a second reference identifier. When a first asset system associated with the first reference identifier and a second asset system associated with the second reference identifier communicate with each other, after identifying the entries associated with the first asset system and the second asset system, the system deletes duplicate records. In some embodiments, the system, after identifying the first set of relationships, may place the first set of relationships in both temporary storage and permanent storage of the system. Additionally, in some embodiments, the system may also identify relationships between multiple applications based on the extracted authentication information. For example, an application 'A' associated with asset system **1** may be accessing an application 'B' in asset system **2** and the system identifies the relationship between application 'A' and application 'B' based on historical data log information and may place this information in the temporary storage for easy retrieval.

[0044] As shown in block **680**, the system identifies a second set of relationships between each of the one or more asset systems and each of the plurality of users based on the extracted authentication information. The second set of relationships may include all forms of active authentication present in the extracted authentication information between each of the one or more asset systems and each of the plurality of users based on the historical data log information extracted from the one or more authentication systems. For example, the system may identify all entries in the historical data log information associated with a first human resources identifier. In some embodiments, the system after identifying the second set of relationships, may place the second set of relationships in the temporary storage of the system such as random access memory for easy retrieval. In such embodiments, the system may identify duplicate relationships from the second set of relationships and may delete the duplicate relationships before storing the second set of relationships in the data store.

[0045] As shown in block **690**, the system formulates the one or more solution data models based on the first set of relationships, the second set of relationships, asset information, and the human resources information. For example, for a relationship between the first asset system and the second asset system, the system identifies and links the asset information associated with the first asset reference identifier and the second asset reference identifier with the relationship. In another example, for a second relationship between the first asset system and a first user, the system identifies and links asset information associated with the first asset reference identifier and human resources information associated with the first human resources identifier with the relationship. The system combines all relationships and generates combined solution data models, wherein the combined solution data models show one or more users associated with each of the asset systems, one or more asset systems connected with the each of the asset systems, one or more applications and logical assets associated with each of the asset systems. The combined data solution models also show lineage within an entity. In some embodiments, the system may generate one single unified data solution model. In some other embodiments, the system may generate multiple data solution models and link them with identifiers to form a combined solution data model.

[0046] FIG. **7** presents a process flow **700** for mitigating intentional and unintentional exposures within the entity, in accordance with embodiments of the present invention. As shown in block **710**, the system identifies an exposure associated with a first user. The exposure may be an intentional exposure or an unintentional exposure. Intentional exposure may be an intentional insider threat. For example, the act of sharing sensitive or confidential information with a third party intentionally is considered as an intentional exposure. Unintentional exposure may be an unintentional insider threat caused when a user loses his/her device (e.g., asset system) containing sensitive information. In some embodiments, the system identifies the exposure by monitoring the plurality of asset systems and user activity of the plurality of users and identifying abnormal activity based on monitoring the plurality of asset systems and the plurality of users, wherein the abnormal activity is identified based on a set of rules. For example, the system may monitor one or more emails communicated by the plurality of users via the plurality of asset systems and identify any abnormal activity based on monitoring the one or more emails. The set of rules may be defined by the entity, using which the system identifies abnormal activity by determining whether information being communicated from the plurality of asset systems is sensitive or not. Upon identifying that the information which is being communicated is sensitive, the system based on the set of rules determines whether the communication is an authorized communication and/or if the recipient of the communication is an authorized recipient or not. In alternate embodiments, the system identifies the exposure based on receiving an input from a user. For example, a user may identify that a first user is sharing confidential information over email or phone and may report the first user to the system. In another example, a first user may lose his/her device and may report the lost device containing sensitive information to the system.

[0047] As shown in block **720**, the system accesses a first solution data model associated with the first user from the model database. Upon identifying the exposure associated with the first user, the system accesses the first solution data model comprising information about one or more asset systems, one or more applications, and one or more users linked with the first user.

[0048] As shown in block **730**, the system identifies one or more relationships associated with the first user from the first solution data model. The system identifies the one or more relationships associated with the first user by identifying at least one first asset associated with the first user, identifying upstream asset systems and downstream asset systems linked with the at least one first asset, identifying at least one first application associated with the first user, and identifying upstream applications and downstream applications linked with the at least one first application. In other words, the system identifies all asset systems and applications that the first user may have access to.

[0049] As shown in block **740**, the system based on the one or more relationships identifies one or more mitigation steps to mitigate exposure associated with the first user. The one or more mitigation steps may include restricting access to the at least one first asset and the at least one first application, monitoring each of the communications associated with the first user, blocking communications associated with the first user, or the like. In one embodiment, the system identifies that any of the upstream asset systems of the downstream asset systems identified above comprises confidential information and restricts access of the at least one first asset system. In another embodiment, the system identifies that at least one of the communications associated with the first user comprises confidential information and blocks the at least one of the communications comprising the confidential data. In some embodiments, the system receives the one or more mitigation steps from a user. In alternate embodiments, the system automatically identifies the one or more mitigation steps using artificial intelligence and automatically implements the one or more mitigation steps. In some embodiments, the system automatically identifies the one or more mitigation steps based on historical data. For example, the system may identify that a mitigation step has been implemented to mitigate a similar exposure and implements the same mitigation step for the present exposure. As shown in block **750**, the system implements the one or more mitigation steps to mitigate exposure associated with the first user.

[0050] Although many embodiments of the present invention have just been described above, the present invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Also, it will be understood that, where possible, any of the advantages, features, functions, devices, and/or operational aspects of any of the embodiments of the present invention described and/or contemplated herein may be included in any of the other embodiments of the present invention described and/or contemplated herein, and/or vice versa. In addition, where possible, any terms expressed in the singular form herein are meant to also include the plural form and/or vice versa, unless explicitly stated otherwise. Accordingly, the terms “a” and/or “an” shall mean “one or more,” even though the phrase “one or more” is also used herein. Like numbers refer to like elements throughout.

[0051] As will be appreciated by one of ordinary skill in the art in view of this disclosure, the present invention may include and/or be embodied as an apparatus (including, for example, a system, machine, device, computer program product, and/or the like), as a method (including, for example, a business method, computer-implemented process, and/or the like), or as any combination of the foregoing. Accordingly, embodiments of the present invention may take the form of an entirely business method embodiment, an entirely software embodiment (including firmware, resident software, micro-code, stored procedures in a database, or the like), an entirely hardware embodiment, or an embodiment combining business method, software, and hardware aspects that may generally be referred to herein as a “system.” Furthermore, embodiments of the present invention may take the form of a computer program product that includes a computer-readable storage medium having one or more computer-executable program code portions stored therein. As used herein, a processor, which may include one or more processors, may be “configured to” perform a certain function in a variety of ways, including, for example, by having one or more general-purpose circuits perform the function by executing one or more computer-executable program code portions embodied in a computer-readable medium, and/or by having one or more application-specific circuits perform the function.

[0052] It will be understood that any suitable computer-readable medium may be utilized. The computer-readable medium may include, but is not limited to, a non-transitory computer-readable medium, such as a tangible electronic, magnetic, optical, electromagnetic, infrared, and/or semiconductor system, device, and/or other apparatus. For example, in some embodiments, the non-transitory computer-readable medium includes a tangible medium such as a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a compact disc read-only memory (CD-ROM), and/or some other tangible optical and/or magnetic storage device. In other embodiments of the present invention, however, the computer-readable medium may be transitory, such as, for example, a propagation signal including computer-executable program code portions embodied therein. In some embodiments, memory may include volatile memory, such as volatile random access memory (RAM) having a cache area for the temporary storage of information. Memory may also include non-volatile memory, which may be embedded and/or may be removable. The non-volatile memory may additionally or alternatively include an EEPROM, flash memory, and/or the like. The memory may store any one or more of pieces of information and data used by the system in which it resides to implement the functions of that system.

[0053] One or more computer-executable program code portions for carrying out operations of the present invention may include object-oriented, scripted, and/or unscripted programming languages, such as, for example, Java, Perl, Smalltalk, C++, SAS, SQL, Python, Objective C, JavaScript, and/or the like. In some embodiments, the one or more computer-executable program code portions for carrying out operations of embodiments of the present invention are written in conventional procedural programming languages, such as the "C" programming languages and/or similar programming languages. The computer program code may alternatively or additionally be written in one or more multi-paradigm programming languages, such as, for example, F#.

[0054] Some embodiments of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of apparatus and/or methods. It will be understood that each block included in the flowchart illustrations and/or block diagrams, and/or combinations of blocks included in the flowchart illustrations and/or block diagrams, may be implemented by one or more computer-executable program code portions. These one or more computer-executable program code portions may be provided to a processor of a general purpose computer, special purpose computer, and/or some other programmable data processing apparatus in order to produce a particular machine, such that the one or more computer-executable program code portions, which execute via the processor of the computer and/or other programmable data processing apparatus, create mechanisms for implementing the steps and/or functions represented by the flowchart(s) and/or block diagram block (s).

[0055] The one or more computer-executable program code portions may be stored in a transitory and/or non-transitory computer-readable medium (e.g., a memory or the like) that can direct, instruct, and/or cause a computer and/or other programmable data processing apparatus to function in a particular manner, such that the computer-executable program code portions stored in the computer-readable medium produce an article of manufacture including instruction mechanisms which implement the steps and/or functions specified in the flowchart(s) and/or block diagram block(s).

[0056] The one or more computer-executable program code portions may also be loaded onto a computer and/or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer and/or other programmable apparatus. In some embodiments, this produces a computer-implemented process such that the one or more computer-executable program code portions which execute on the computer and/or other programmable apparatus provide operational steps to implement the steps specified in the flowchart(s) and/or the functions specified in the block diagram block(s). Alternatively, computer-implemented steps may be combined with, and/or replaced with, operator- and/or human-implemented steps in order to carry out an embodiment of the present invention.

[0057] While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other changes, combinations, omissions, modifications and substitutions, in addition to those set forth in the above paragraphs, are possible. Those skilled in the art will appreciate that various adaptations, modifications, and combinations of the just described embodiments can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

INCORPORATION BY REFERENCE

[0058] To supplement the present disclosure, this application further incorporates entirely by reference the following commonly assigned patent applications:

Docket Number	U.S. patent application Ser. No.	Title	Filed On
8015US1.014033.3109	15/814,028	SYSTEM FOR TECHNOLOGY ANOMALY DETECTION, TRIAGE AND RESPONSE USING SOLUTION DATA MODELING	Nov. 15, 2017
8016US1.014033.3110	15/814,038	IMPLEMENTING A CONTINUITY PLAN GENERATED USING SOLUTION DATA MODELING BASED ON PREDICTED FUTURE EVENT SIMULATION TESTING	Nov. 15, 2017
8017US1.014033.3111	15/814,044	SYSTEM FOR REROUTING ELECTRONIC DATA TRANSMISSIONS BASED ON GENERATED SOLUTION DATA MODELS	Nov. 15, 2017
8371US1.014033.3198	To be assigned	SYSTEM FOR MITIGATING EXPOSURE ASSOCIATED WITH IDENTIFIED IMPACTS OF TECHNOLOGICAL SYSTEM CHANGES BASED ON SOLUTION DATA MODELLING	Concurrently herewith
8372US1.014033.3199	To be assigned	SYSTEM FOR MITIGATING EXPOSURE ASSOCIATED WITH IDENTIFIED UNMANAGED DEVICES IN A NETWORK USING SOLUTION DATA MODELLING	Concurrently herewith

-continued

Docket Number	U.S. patent application Ser. No.	Title	Filed On
8374US1.014033.3201	To be assigned	SYSTEM FOR DECOMMISSIONING INFORMATION TECHNOLOGY ASSETS USING SOLUTION DATA MODELLING	Concurrently herewith

What is claimed is:

1. A system for mitigating intentional and unintentional exposures using solution data modelling, the system comprising:

one or more memory devices having computer readable code stored thereon; wherein the one or more memory devices comprises a plurality of databases comprising a model database and an incident database;

one or more processing devices operatively coupled to the one or more memory devices, wherein the one or more processing devices are configured to execute the computer readable code to:

generate one or more solution data models comprising a plurality of asset systems and a plurality of users, wherein each of the plurality of asset systems is associated with at least one user of the plurality of users and wherein at least a first of the plurality of asset systems is associated with at least a second of the plurality of asset systems;

store the one or more solution data models in the model database;

identify an exposure associated with a first user;

access a first solution data model associated with the first user from the model database;

identify one or more relationships associated with the first user from the first solution data model; and

based on the one or more relationships, implement one or more mitigation steps to mitigate the exposure associated with the first user.

2. The system of claim **1**, wherein generating the one or more solution data models comprises:

accessing one or more authentication systems, wherein the one or more authentication systems comprise authentication information associated with the plurality of asset systems and the plurality of users;

extracting the authentication information associated with the plurality of asset systems and the plurality of users;

accessing one or more human resources systems, wherein the one or more human resources systems comprise human resources information associated with the plurality of users;

extracting the human resources information associated with the plurality of users;

accessing one or more asset management systems, wherein the one or more asset management systems comprise asset information associated with at least type and location of the plurality of asset systems;

extracting the asset information associated with plurality of asset systems;

identifying a first set of relationships between each of the plurality of asset systems based on the extracted authentication information;

identifying a second set of relationships between each of the plurality of users and each of the plurality of asset systems based on the extracted authentication information; and

formulating the one or more solution data models based on the first set of relationships, the second set of relationships, the asset information, and the human resources information.

3. The system of claim **1**, wherein identifying the exposure comprises:

monitoring the plurality of asset systems and user activity of the plurality of users; and

identifying abnormal activity based on monitoring the plurality of asset systems and the plurality of users, wherein the abnormal activity is identified based on a set of rules.

4. The system of claim **1**, wherein the one or more processing devices are configured to execute the computer readable code to identify the exposure based on receiving an input from a user.

5. The system of claim **1**, wherein identifying the one or more relationships associated with the first user comprises:

identifying at least one first asset associated with the first user;

identifying upstream asset systems and downstream asset systems linked with the at least one first asset;

identifying at least one first application associated with the first user; and

identifying upstream applications and downstream applications linked with the at least one first application.

6. The system of claim **5**, wherein implementing the one or more mitigation steps comprises:

identifying that at least one asset system of the upstream asset systems and the downstream asset systems comprises confidential data; and

restricting access to the at least one asset system.

7. The system of claim **1**, wherein implementing the one or more mitigation steps comprises:

monitoring communications associated with the first user;

identifying that at least one of the communications comprises confidential data; and

blocking at least one of the communications comprising the confidential data.

8. The system of claim **1**, wherein the exposure is at least one of an intentional exposure or an unintentional exposure.

9. A computer program product for mitigating intentional and unintentional exposures using solution data modelling, the computer program product comprising at least one non-transitory computer-readable medium having computer-readable program code portions embodied therein, the computer-readable program code portions comprises one or more executable portions for:

generating one or more solution data models comprising a plurality of asset systems and a plurality of users, wherein each of the plurality of asset systems is associated with at least one user of the plurality of users and wherein at least a first of the plurality of asset systems is associated with at least a second of the plurality of asset systems;

storing the one or more solution data models in a model database;

identifying an exposure associated with a first user;

accessing a first solution data model associated with the first user from the model database;

identifying one or more relationships associated with the first user from the first solution data model; and

based on the one or more relationships, implementing one or more mitigation steps to mitigate the exposure associated with the first user.

10. The computer program product of claim **9**, wherein generating the one or more solution data models comprises:

accessing one or more authentication systems, wherein the one or more authentication systems comprise authentication information associated with the plurality of asset systems and the plurality of users;

extracting the authentication information associated with the plurality of asset systems and the plurality of users;

accessing one or more human resources systems, wherein the one or more human resources systems comprise human resources information associated with the plurality of users;

extracting the human resources information associated with the plurality of users;

accessing one or more asset management systems, wherein the one or more asset management systems comprise asset information associated with at least type and location of the plurality of asset systems;

extracting the asset information associated with plurality of asset systems;

identifying a first set of relationships between each of the plurality of asset systems based on the extracted authentication information;

identifying a second set of relationships between each of the plurality of users and each of the plurality of asset systems based on the extracted authentication information; and

formulating the one or more solution data models based on the first set of relationships, the second set of relationships, the asset information, and the human resources information.

11. The computer program product of claim **9**, wherein identifying the exposure comprises:

monitoring the plurality of asset systems and user activity of the plurality of users; and

identifying abnormal activity based on monitoring the plurality of asset systems and the plurality of users, wherein the abnormal activity is identified based on a set of rules.

12. The computer program product of claim **9**, wherein the computer-readable program code portions comprises one or more executable portions for identifying the exposure based on receiving an input from a user.

13. The computer program product of claim **9**, wherein identifying the one or more relationships associated with the first user comprises:

identifying at least one first asset associated with the first user;

identifying upstream asset systems and downstream asset systems linked with the at least one first asset;

identifying at least one first application associated with the first user; and

identifying upstream applications and downstream applications linked with the at least one first application.

14. The computer program product of claim **13**, wherein implementing the one or more mitigation steps comprises:

identifying that at least one asset system of the upstream asset systems and the downstream asset systems comprises confidential data; and

restricting access to the at least one asset system.

15. The computer program product of claim **9**, wherein implementing the one or more mitigation steps comprises:

monitoring communications associated with the first user;

identifying that at least one of the communications comprises confidential data; and

blocking at least one of the communications comprising the confidential data.

16. A computer implemented method for mitigating intentional and unintentional exposures using solution data modelling, the method comprising:

generating one or more solution data models comprising a plurality of asset systems and a plurality of users, wherein each of the plurality of asset systems is associated with at least one user of the plurality of users and wherein at least a first of the plurality of asset systems is associated with at least a second of the plurality of asset systems;

storing the one or more solution data models in a model database;

identifying an exposure associated with a first user;

accessing a first solution data model associated with the first user from the model database;

identifying one or more relationships associated with the first user from the first solution data model; and

based on the one or more relationships, implementing one or more mitigation steps to mitigate the exposure associated with the first user.

17. The computer implemented method of claim **16**, wherein generating the one or more solution data models comprises:

accessing one or more authentication systems, wherein the one or more authentication systems comprise authentication information associated with the plurality of asset systems and the plurality of users;

extracting the authentication information associated with the plurality of asset systems and the plurality of users;

accessing one or more human resources systems, wherein the one or more human resources systems comprise human resources information associated with the plurality of users;

extracting the human resources information associated with the plurality of users;

accessing one or more asset management systems, wherein the one or more asset management systems comprise asset information associated with at least type and location of the plurality of asset systems;

extracting the asset information associated with plurality of asset systems;

identifying a first set of relationships between each of the plurality of asset systems based on the extracted authentication information;

identifying a second set of relationships between each of the plurality of users and each of the plurality of asset systems based on the extracted authentication information; and

formulating the one or more solution data models based on the first set of relationships, the second set of relationships, the asset information, and the human resources information.

18. The computer implemented method of claim **16**, wherein identifying the exposure comprises:

monitoring the plurality of asset systems and user activity of the plurality of users; and

identifying abnormal activity based on monitoring the plurality of asset systems and the plurality of users, wherein the abnormal activity is identified based on a set of rules.

19. The computer implemented method of claim **16**, wherein the method further comprises identifying the exposure based on receiving an input from a user.

20. The computer implemented method of claim **16**, wherein identifying the one or more relationships associated with the first user comprises:

identifying at least one first asset associated with the first user;

identifying upstream asset systems and downstream asset systems linked with the at least one first asset;

identifying at least one first application associated with the first user; and

identifying upstream applications and downstream applications linked with the at least one first application.

* * * * *