

include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. Data transmission and instructions can also occur over a communications network. Information carriers suitable for embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in special purpose logic circuitry.

[0060] To provide for interaction with a user, the above described processes can be implemented on a computer having a display device, e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse or a trackball, by which the user can provide input to the computer (e.g., interact with a user interface element). Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input.

[0061] The above described techniques can be implemented in a distributed computing system that includes a back-end component, e.g., as a data server, and/or a middle-ware component, e.g., an application server, and/or a front-end component, e.g., a client computer having a graphical user interface and/or a Web browser through which a user can interact with an example implementation, or any combination of such back-end, middleware, or front-end components. The components of the system can be interconnected by any form or medium of digital data communication, e.g., a communication network. Examples of communication networks include a local area network ("LAN") and a wide area network ("WAN"), e.g., the Internet, and include both wired and wireless networks.

[0062] The computing system can include clients and servers. A client and server are generally remote from each other and can interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0063] The invention has been described in terms of particular embodiments. The alternatives described herein are examples for illustration only and are not to limit the alternatives in any way. The steps of the invention can be performed in a different order and still achieve desirable results. Other embodiments are within the scope of the following claims.

What is claimed is:

1. A method for managing role-based access in a multi-customer computing environment, the method comprising:
 associating an actor with a role;
 associating a policy type with the role;
 associating a role scope with the role;
 receiving one or more values for one or more corresponding context parameters associated with the actor;
 receiving a request for access to a resource from the actor;

determining a policy instance based on the policy type and the one or more values for the one or more corresponding context parameters associated with the actor;

determining one or more actor-role scope values based on the role scope and the one or more values for the one or more corresponding context parameters associated with the actor; and

determining a response to the request based on the policy instance and the actor-role scope values.

2. The method of claim 1, wherein determining the response to the request comprises determining a resolved scope using the actor-role scope values.

3. The method of claim 1, further comprising generating a role assignment record.

4. The method of claim 3, wherein the role assignment record comprises the actor, the role, and the context parameters.

5. The method of claim 3, wherein the role assignment record comprises the one or more actor-role scope values based on the role scope.

6. The method of claim 1, wherein said resource comprises a database, a system application, a document, or any combination thereof.

7. The method of claim 1, wherein said actor comprises a user, a system account, a system application, a computing device, or any combination thereof.

8. The method of claim 1 wherein the policy type includes an access control policy element, a data view/presentation policy element, a function performance/update operation policy element, or any combination thereof.

9. The method of claim 1 wherein determining the policy instance comprises employing a hierarchical priority of the one or more of the context parameters.

10. The method of claim 1 comprising defining a default policy instance.

11. The method of claim 10 wherein determining the policy instance comprises selecting the default policy instance when there is no match with the one or more of the context parameters.

12. A system for managing role-based access in a multi-customer computing environment, the system comprising:
 one or more servers configured to:

associate an actor with a role;

associate a policy type with the role;

associate a role scope with the role;

receive one or more values for one or more corresponding context parameters associated with the actor;

receive a request for access to a resource from the actor;

determine a policy instance based on the policy type and the one or more values for the one or more corresponding context parameters associated with the actor;

determine one or more actor-role scope values based on the role scope and the one or more values for the one or more corresponding context parameters associated with the actor; and

determine a response to the request based on the policy instance and the actor-role scope values.

13. The system of claim 12, wherein the one or more servers are further configured to determine the response to the request comprises determining a resolved scope using the actor-role scope values.