

The computer program product includes instructions being operable to cause data processing apparatus to perform any of the methods described herein.

**[0010]** Any of the above examples can realize on or more of the following advantages. By using context parameters for role assignment, policy instance determination, and/or scope resolution, fewer roles are needed to handle diverse situations. Further, the same roles can be used across multiple customers in a multi-customer environment. For example, one manager role can be used for ABC Corp. and XYZ Corp. in the same computing environment because context parameters allow determination of different authorization policies for the same manager role for the two different corporations. The role-based authorization system provides for a more rich definition of authorization than is set forth as part of industry standards such as the RBAC model of the NIST, for example American National Standard ANSI INCITS 359-2004. Through inclusion of contextual considerations and actor attributes such as scope, access control, presentation, and function, the role-based authorization system enables efficient and scalable role-based authorization in a multi-customer computing environment.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0011]** The advantages of the invention described above, together with further advantages, may be better understood by referring to the following description taken in conjunction with the accompanying drawings. The details of one or more examples are set forth in the accompanying drawings and the description below. Further features, aspects, and advantages of the invention will become apparent from the description, the drawings, and the claims. The drawings are not necessarily to scale, emphasis, instead, generally being placed upon illustrating the principles of the invention.

**[0012]** FIG. 1 is an exemplary illustration of a computing system for role-based access in a multi-customer computing environment.

**[0013]** FIG. 2 is an exemplary illustration of a data structure for a role assignment record.

**[0014]** FIG. 3 illustrates a process flow diagram for role-based access in a multi-customer computing environment.

**[0015]** FIG. 4 illustrates a process flow diagram for role resolution.

**[0016]** FIG. 5 illustrates an exemplary process for policy instance determination.

**[0017]** FIG. 6 is an exemplary illustration for role-based access in a multi-customer computing environment.

**[0018]** FIG. 7 is another exemplary illustration for role-based access in a multi-customer computing environment.

#### DESCRIPTION OF THE INVENTION

**[0019]** FIG. 1 illustrates an exemplary computing system 100 for role-based access in a multi-customer computing environment. The computing system 100 performs these functions by operating on input data and generating output data. A user 110 interacts with the client device 120. The computing system 100 can include one or more client-computing devices, for example, a desktop computer 120a and/or a handheld computing device, e.g., a personal digital assistant 120b, generally 120. The client-computing device 120 is in communication with a communications network 130. The communications network device 130 enables communication between the client device 120 and an application

server 140 by, for example, transmitting data and executing instructions between the client device 120 and an application server device 140. The application server 140 receives service requests from one or more of the client devices 120 through the communications network 130. The application server 140 executes one or more application software program modules, including, for example, a role resolution program module 142a, and/or a policy instance-role mapping program module 142b, generally 142. An exemplary function of the role resolution program module 142a can be associating a role with an actor based on one or more pre-defined context parameters, and resolves the authorized scope of action for the user. An exemplary function of the policy instance-role mapping program module 142b can be assigning a policy instance to a role based on one or more pre-defined context parameters and one or more policy types. A policy type includes, for example, one or more policy elements that relate to one or more user authorizations or permissions. A policy instance is an instance of a policy type (e.g., a predetermined set of values for a predetermined set of policy elements) that applies to a user based on the role of the user and the one or more pre-defined context parameters associated with the user.

**[0020]** The application server 140 accesses one or more database servers 162 through a communications network 150. In some examples, the communications network 130 and the communications network 150 are the same network. The application server 140 serves client requests by, for example, generating the appropriate response back to the appropriate client device 120 based on outputs from the one or more application software program modules 142. The database server 162 creates, stores, organizes, and retrieves data from one or more databases. In one embodiment, databases include, for example, an actor ID-role table 164a, a role scope-role table 164b, a policy type-role table 164c, and/or any combination thereof, generally 164. In some embodiments, the one or more database servers 162 are co-located with one or more database tables 164 at repository 160. In other embodiments, the one or more database servers 162 communicate with the one or more databases and their tables 164 through a communications network (not shown).

**[0021]** Although the examples refer to a user 110 as an actor, the invention is not so limited. A user 110 is one type of actor. Other actors can include, for example, system accounts, system applications, batch processes, and/or other computing devices. The actor includes an entity that performs one or more actions, and is the target for the authorization decision regarding access to particular resources. When one or more actors are system accounts, system applications, batch processes, and/or other computing devices, the one or more actors are in communication with an application server 140 through the communications network 130. The application server 140 receives service requests from the one or more actor devices through the communications network 130. The application server 140 executes one or more application software program modules, including, for example, a role resolution module 142a, and/or a policy instance-role mapping module 142b, generally 142. The application server 140 accesses one or more servers 162 through a communications network 150. The application server 140 serves client requests by, for example, generating the appropriate response back to the appropriate