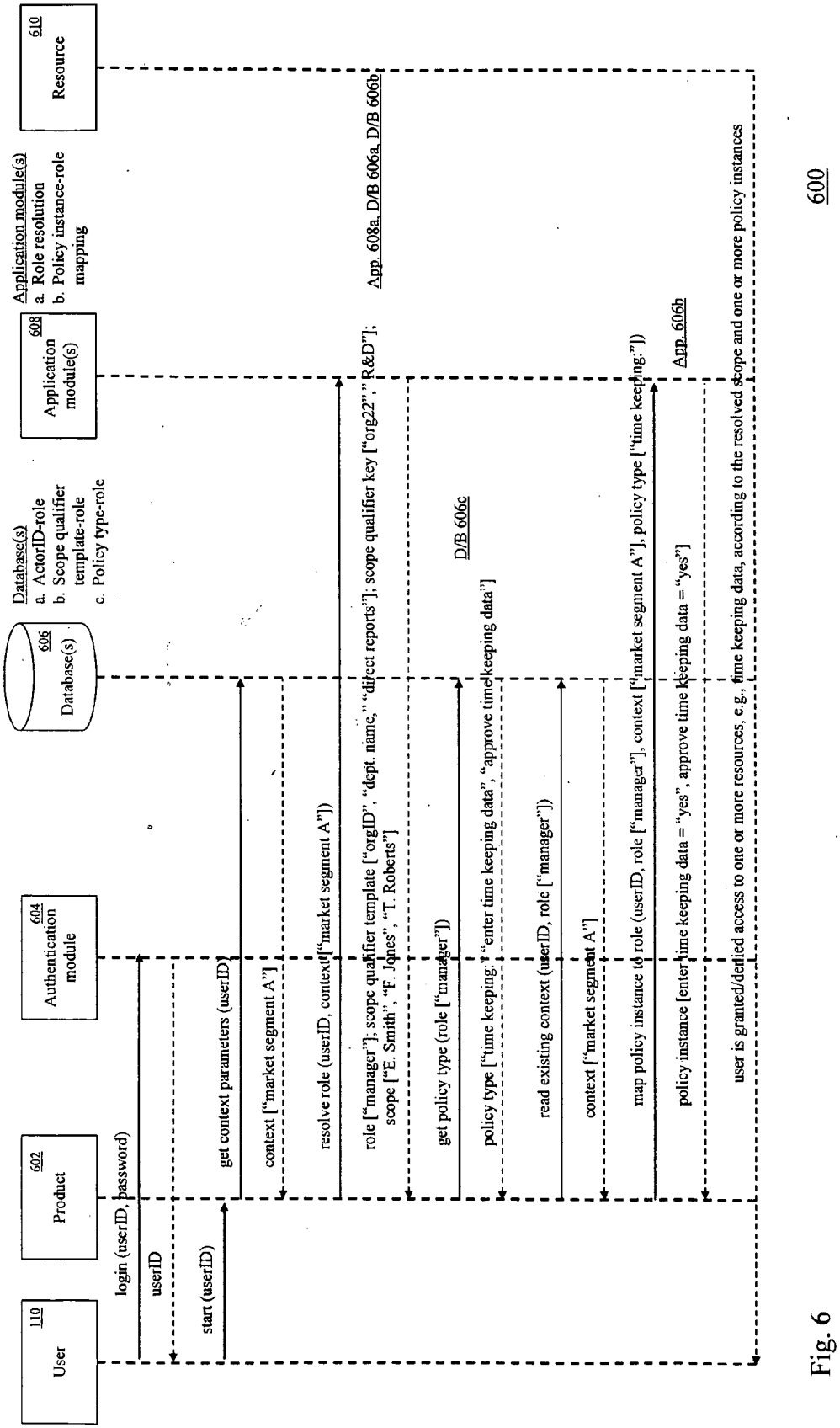
User
110
Product
602
Authentication module
604
Database(s)
606
Database(s)
a. ActorID-role
b. Scope qualifier template-role
c. Policy type-role
Application module(s)
608
Application module(s)
a. Role resolution
b. Policy instance-role mapping
Resource
610
login (userID, password)
userID
start (userID)
get context parameters (userID)
context ["market segment A"]
resolve role (userID, context["market segment A"])
role ["manager"]; scope qualifier template ["orgID", "dept. name", "direct reports"]; scope qualifier key ["org22", "R&D"];
scope ["E. Smith", "F. Jones", "T. Roberts"]
App. 608a, D/B 606a, D/B 606b
get policy type (role ["manager"])
D/B 606c
policy type ["time keeping", "enter time keeping data", "approve time keeping data"]
read existing context (userID, role ["manager"])
context ["market segment A"]
map policy instance to role (userID, role ["manager"], context ["market segment A"], policy type ["time keeping"])
App. 606b
policy instance [enter time keeping data = "yes", approve time keeping data = "yes"]
user is granted/denied access to one or more resources, e.g., time keeping data, according to the resolved scope and one or more policy instances

600

Fig. 6