US 20230231837A1

(19) **United States**
(12) **Patent Application Publication**
Islam
(10) **Pub. No.: US 2023/0231837 A1**
(43) **Pub. Date: Jul. 20, 2023**

(54) **AUTHENTICATION RISK-SCORING IN AN AUTHENTICATION SYSTEM BASED ON USER-SPECIFIC AND ORGANIZATION-SPECIFIC RISK MODELS**

(71) Applicant: **Okta, Inc.**, San Francisco, CA (US)

(72) Inventor: **Tanvir Islam**, Lake Stevens, WA (US)

(21) Appl. No.: **17/578,366**

(22) Filed: **Jan. 18, 2022**

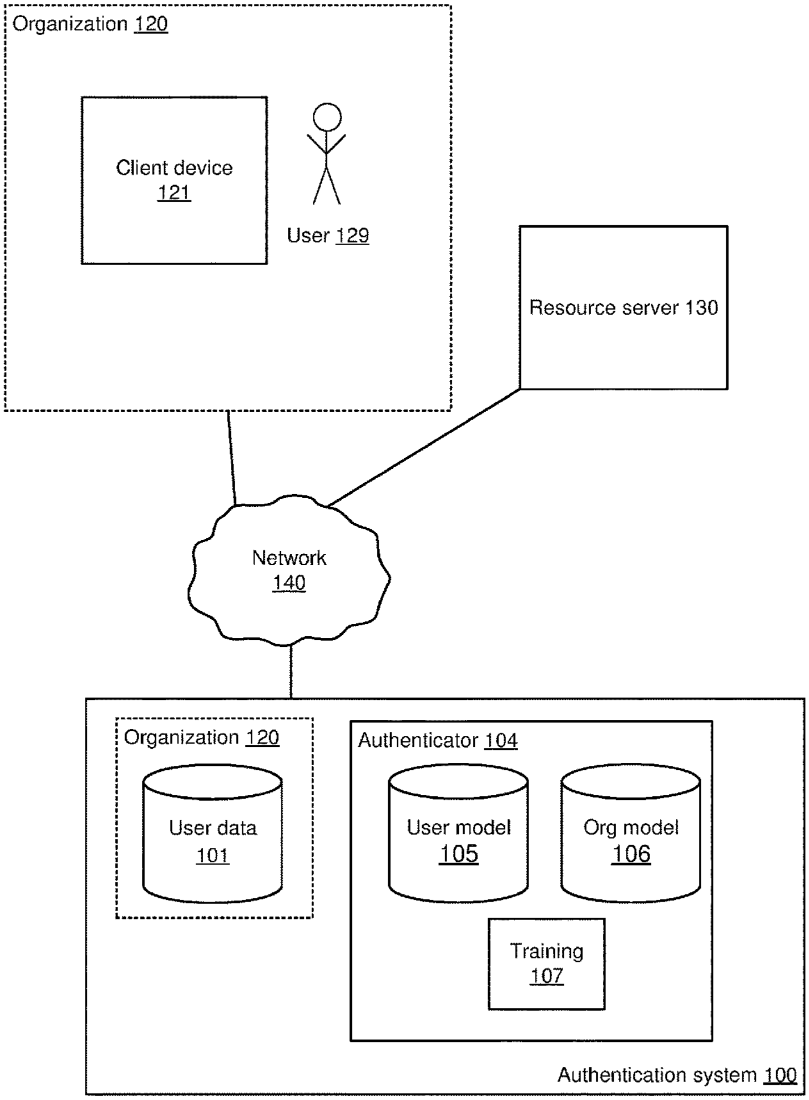
Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)
G06N 20/00 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/08*** (2013.01); ***G06N 20/00*** (2019.01); *H04L 2463/082* (2013.01)

(57) **ABSTRACT**

An authentication system uses machine learning models to quantify a degree of risk that a given request to authenticate as a particular user of an organization is not in fact originating from that user, but rather from a malicious actor attempting to gain access to the user's account. More particularly, the authentication system employs both a user model that quantifies a degree of deviation from a user context in which a particular user typically requests authentication, and an organization model that quantifies a degree of deviation of a current context of the organization from a "normal" context for that organization. The user model and the organization can be employed individually, such as the organization model providing organization administrators with insights into the current security status of the organization, or together, such as using the risk scores of both models when assessing how to respond to a particular authentication request.


Organization 120
Client device 121
User 129
Resource server 130
Network 140
Organization 120
User data 101
Authenticator 104
User model 105
Org model 106
Training 107
Authentication system 100