



US 20240214398A1

(19) **United States**

(12) **Patent Application Publication**
LIDGI et al.

(10) **Pub. No.: US 2024/0214398 A1**

(43) **Pub. Date: Jun. 27, 2024**

(54) **SYSTEM AND METHOD FOR DETECTING SENSITIVE DATA IN ACTIVE INSPECTION OF CLOUD COMPUTING RESOURCES**

(52) **U.S. Cl.**
CPC **H04L 63/1416** (2013.01)

(71) Applicant: **Wiz, Inc.**, New York, NY (US)

(57) **ABSTRACT**

(72) Inventors: **Matilda LIDGI**, Tel Aviv (IL); **Shai KEREN**, Tel Aviv (IL); **Raaz HERZBERG**, Tel Aviv (IL); **Avi Tal LICHTENSTEIN**, Tel Aviv (IL); **Ami LUTTWAK**, Binyamina (IL); **Roy REZNIK**, Tel Aviv (IL)

A system and method for performing active inspection of a cloud computing environment to detect exposed sensitive data. The method also includes receiving at least one network path to access a first resource, where the first resource is a cloud object deployed in the cloud computing environment, and potentially accessible from a network which is external to the cloud computing environment; and generating a first instruction to access the first resource based on a plurality of reachability parameters designated in the at least one network path; causing execution of the generated first instruction to access the first resource; receiving an output, the output generated in response to execution of the generated first instruction; detecting in the output a predetermined sensitive data indicator; and initiating a mitigation action in response to detecting the sensitive data indicator in the output.

(73) Assignee: **Wiz, Inc.**, New York, NY (US)

(21) Appl. No.: **18/146,670**

(22) Filed: **Dec. 27, 2022**

Publication Classification

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

