US 20240214414A1

(19) **United States**

(12) **Patent Application Publication**

Chen et al.

(10) **Pub. No.: US 2024/0214414 A1**

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

(54) **INCREMENTAL CAUSAL GRAPH LEARNING FOR ATTACK FORENSICS IN COMPUTER SYSTEMS**

(71) Applicant: **NEC Laboratories America, Inc.**, Princeton, NJ (US)

(72) Inventors: **Zhengzhang Chen**, Princeton Junction, NJ (US); **Haifeng Chen**, West Windsor, NJ (US); **Dongjie Wang**, Orlando, FL (US)

(21) Appl. No.: **18/359,389**

(22) Filed: **Jul. 26, 2023**

Related U.S. Application Data

(60) Provisional application No. 63/397,955, filed on Aug. 15, 2022, provisional application No. 63/442,155, filed on Jan. 31, 2023, provisional application No. 63/450,989, filed on Mar. 9, 2023.

Publication Classification

(51) **Int. Cl.**

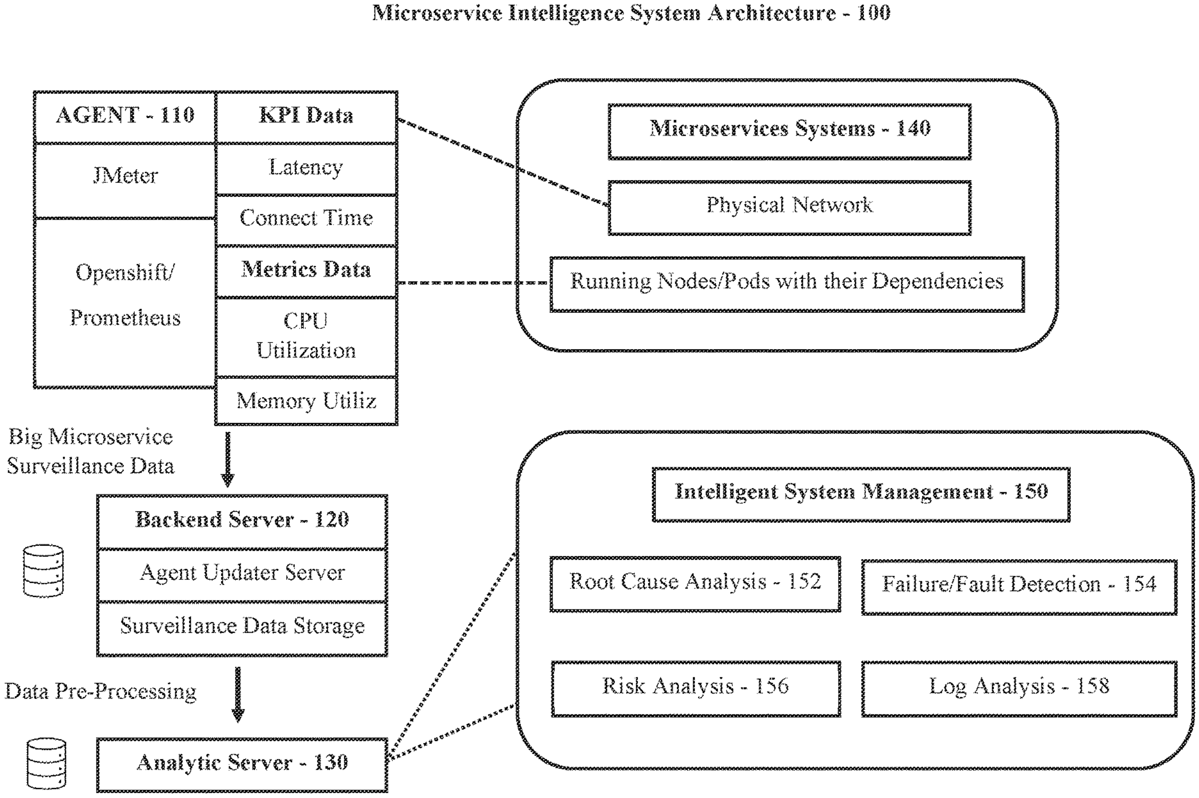
H04L 9/40	(2006.01)
H04L 41/0631	(2006.01)
H04L 41/16	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/145*** (2013.01); ***H04L 41/0631*** (2013.01); ***H04L 41/16*** (2013.01)

(57) **ABSTRACT**

A computer-implemented method for identifying attack origins is provided. The method includes detecting a trigger point from entity metrics data and key performance indicator (KPI) data, generating a learned causal graph by fusing a state-invariant causal graph with a state-dependent causal graph, backtracking from an attack detection point, via an incident backtrack and system recovery component, by using the learned causal graph to identify an attack origin when an intrusion or attack occurs, and displaying data relating to the attack origin on a visualization display for user analysis.


Microservice Intelligence System Architecture - 100
AGENT - 110
KPI Data
JMeter
Latency
Connect Time
Openshift/ Prometheus
Metrics Data
CPU Utilization
Memory Utiliz
Microservices Systems - 140
Physical Network
Running Nodes/Pods with their Dependencies
Big Microservice Surveillance Data
Backend Server - 120
Agent Updater Server
Surveillance Data Storage
Data Pre-Processing
Analytic Server - 130
Intelligent System Management - 150
Root Cause Analysis - 152
Failure/Fault Detection - 154
Risk Analysis - 156
Log Analysis - 158