US007647524B2

(12) **United States Patent**
Ide et al.

(10) **Patent No.: US 7,647,524 B2**
(45) **Date of Patent: Jan. 12, 2010**

(54) ANOMALY DETECTION

(75) Inventors: **Tsuyoshi Ide**, Kawasaki (JP); **Kunikazu Yoda**, Yamato (JP); **Hisashi Kashima**, Yamato (JP); **Hiroaki Etoh**, Kanagawa-ken (JP); **Ryo Hirade**, Miura (JP)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 52 days.

(21) Appl. No.: **11/933,270**

(22) Filed: **Oct. 31, 2007**

(65) **Prior Publication Data**

US 2009/0031176 A1 Jan. 29, 2009

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **714/4**; 714/38; 709/224

(58) **Field of Classification Search** .... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,346,803	B2 *	3/2008	Ide et al.	714/4

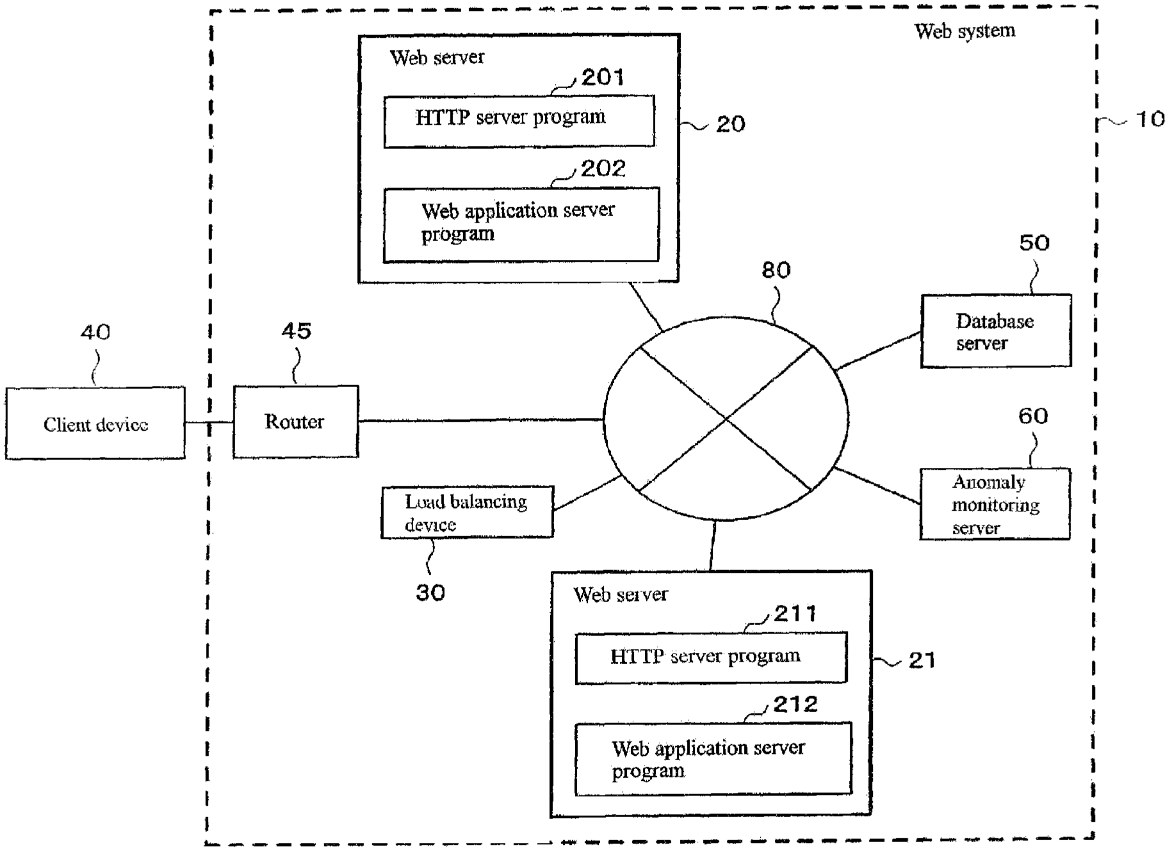
* cited by examiner

Primary Examiner—Christopher S McCarthy
(74) *Attorney, Agent, or Firm*—Vazken Alexanian

(57) **ABSTRACT**

A system such as a Web-based system in which a plurality of computers interact with each other is monitored to detect online an anomaly. Transactions of a service provided by each of a plurality of computers to another computer are collected, a matrix of correlations between nodes in the system is calculated from the transactions, and a feature vector representing anode activity balance is obtained from the matrix. The feature vector is monitored using a probability model to detect a transition to an anomalous state.

5 Claims, 9 Drawing Sheets


Web system
10
Web server
201
HTTP server program
20
202
Web application server program
50
80
Database server
40
45
Client device
Router
60
Anomaly monitoring server
Load balancing device
30
Web server
211
HTTP server program
21
212
Web application server program