US008108929B2

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

(10) **Patent No.: US 8,108,929 B2**
(45) **Date of Patent: Jan. 31, 2012**

(54) **METHOD AND SYSTEM FOR DETECTING INTRUSIVE ANOMALOUS USE OF A SOFTWARE SYSTEM USING MULTIPLE DETECTION ALGORITHMS**

(75) Inventors: **Subhash C. Agrawal**, Boxboro, MA (US); **Scott M. Wimer**, Burlington, MA (US); **Jonathan H. Young**, Newton, MA (US)

(73) Assignee: **Reflex Systems, LLC**, Atlanta, GA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1844 days.

(21) Appl. No.: **10/967,945**

(22) Filed: **Oct. 19, 2004**

(65) **Prior Publication Data**

US 2006/0085854 A1 Apr. 20, 2006

(51) **Int. Cl.**
***G06F 21/00*** (2006.01)

(52) **U.S. Cl.** ..... **726/23**

(58) **Field of Classification Search** ..... 726/23
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 6,839,850 | B1 * | 1/2005 | Campbell et al. | 726/23 |
| 7,069,588 | B2 * | 6/2006 | Call et al. | 726/22 |
| 7,162,741 | B2 * | 1/2007 | Eskin et al. | 726/25 |
| 7,487,542 | B2 * | 2/2009 | Boulanger et al. | 726/23 |
| 2002/0078381 | A1 * | 6/2002 | Farley et al. | 713/201 |
| 2003/0051026 | A1 * | 3/2003 | Carter et al. | 709/224 |
| 2003/0149888 | A1 * | 8/2003 | Yadav | 713/200 |
| 2003/0188190 | A1 * | 10/2003 | Aaron et al. | 713/201 |
| 2004/0034795 | A1 * | 2/2004 | Anderson et al. | 713/201 |
| 2004/0143756 | A1 * | 7/2004 | Munson et al. | 713/200 |
| 2005/0229250 | A1 * | 10/2005 | Ring et al. | 726/23 |
| 2007/0107052 | A1 * | 5/2007 | Cangini et al. | 726/22 |

OTHER PUBLICATIONS

X. Hoang, J. Hu, and P. Bertok. "A Multi-layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls", Networks, 2003.*

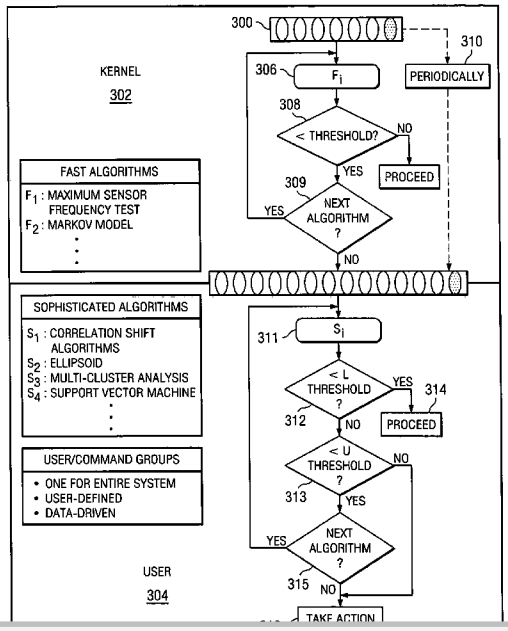
* cited by examiner

*Primary Examiner* — Gilberto Barron, Jr.
*Assistant Examiner* — Virginia T Ho
(74) *Attorney, Agent, or Firm* — David H. Judson

(57) **ABSTRACT**

A target software system is instrumented to generate behavior data representing a current observation or observation aggregate. A method then determines whether the current observation or observation aggregate warrants a second level examination; preferably, this determination is made by processing the current observation or observation aggregate through a first level detection algorithm that provides a provisional indication of a possible intrusion. If executing the first level detection algorithm indicates that the current observation or observation aggregate warrants a second level examination, the method continues by processing the current observation or observation aggregate through at least one second level detection algorithms to provide a more definite, fine grain indication of a possible intrusion. Multiple algorithms may be executed together within a single examination level, with the individual results then analyzed to obtain a composite result or output indicative of intrusive or anomalous behavior.

**23 Claims, 4 Drawing Sheets**



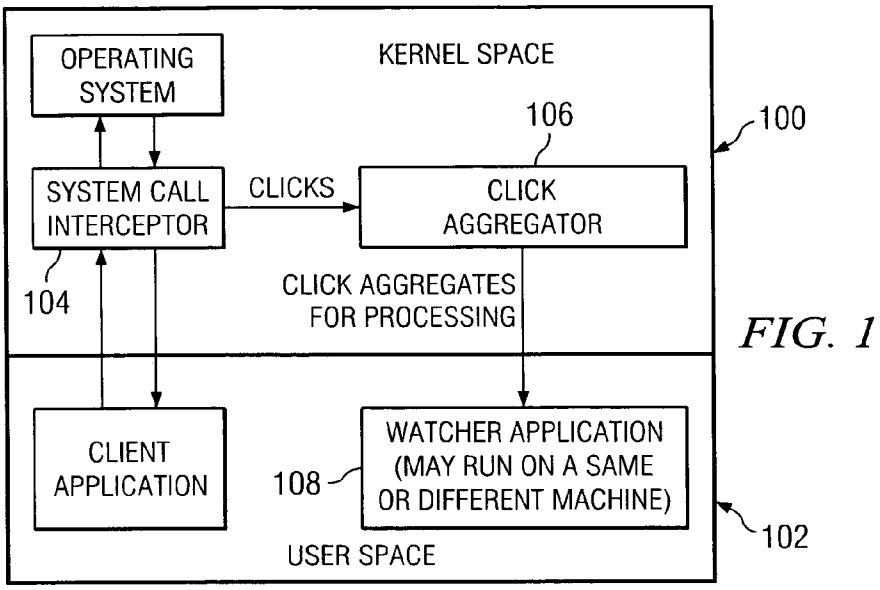



FIG. 1

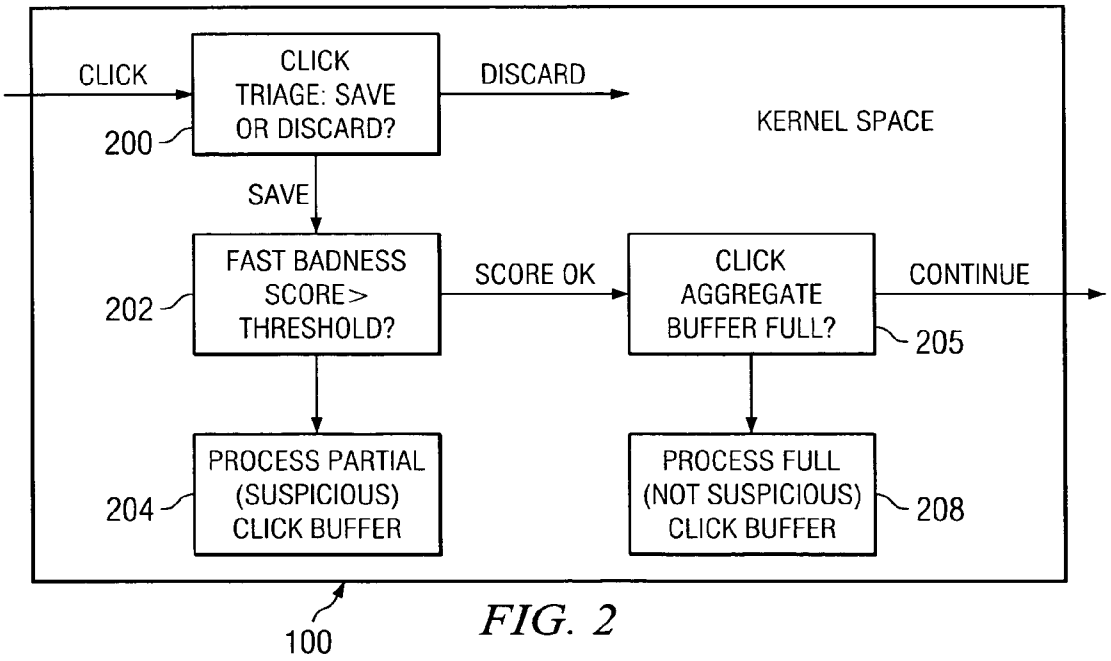



FIG. 2

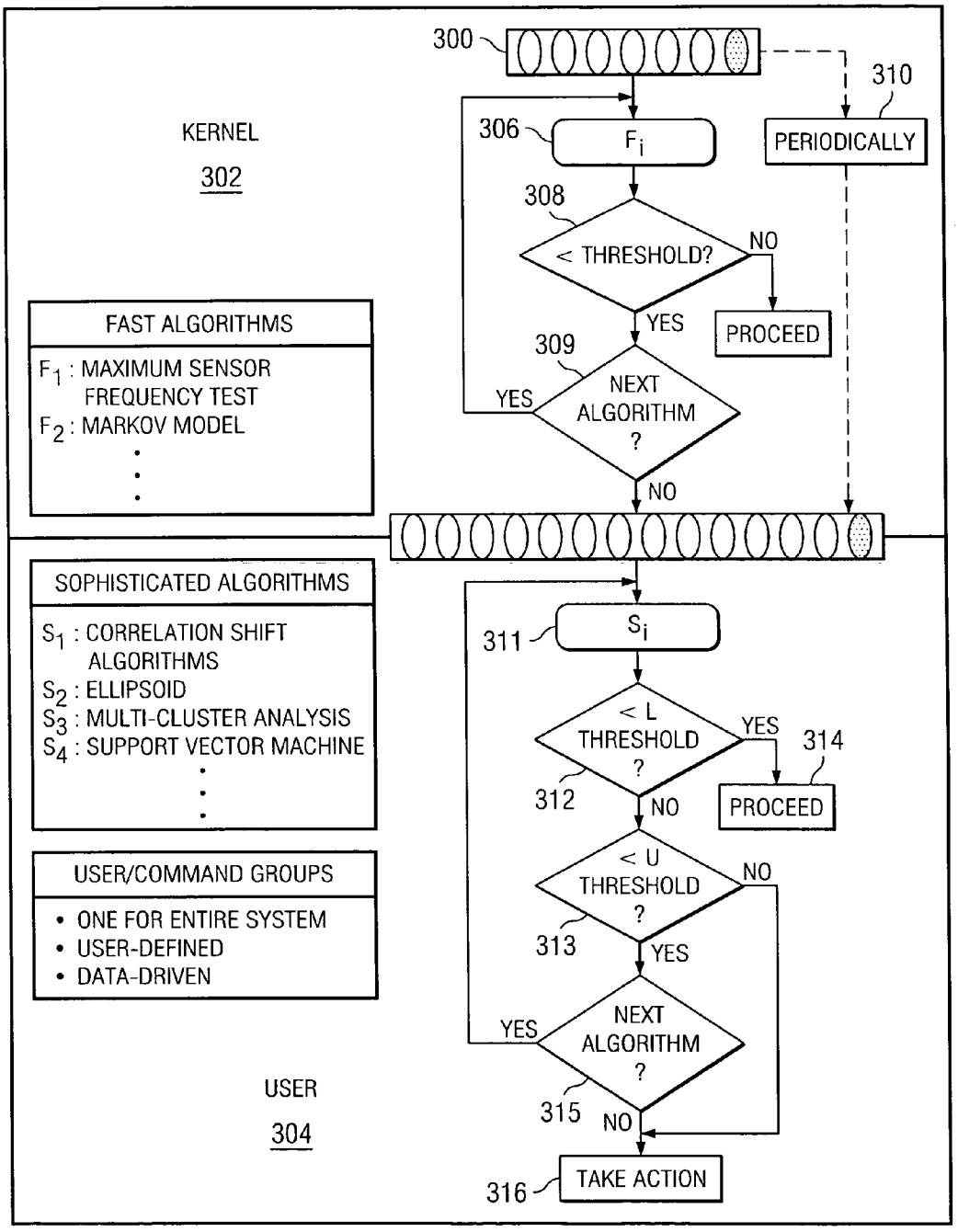



*FIG. 3*

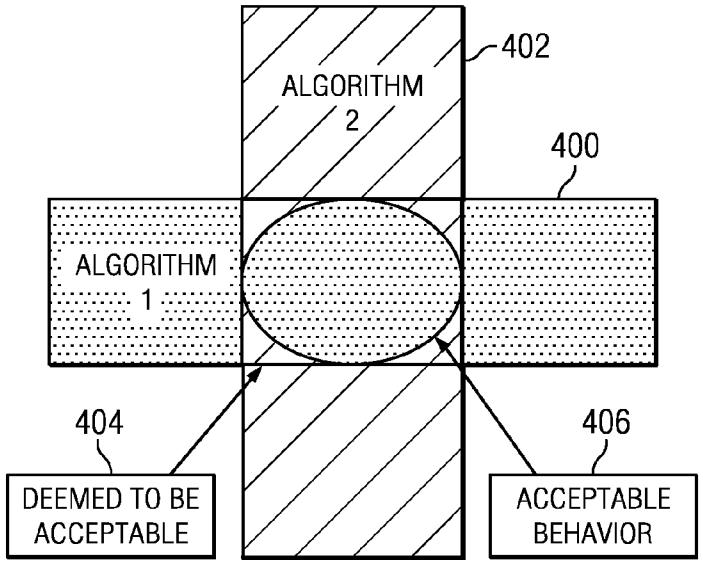



FIG. 4

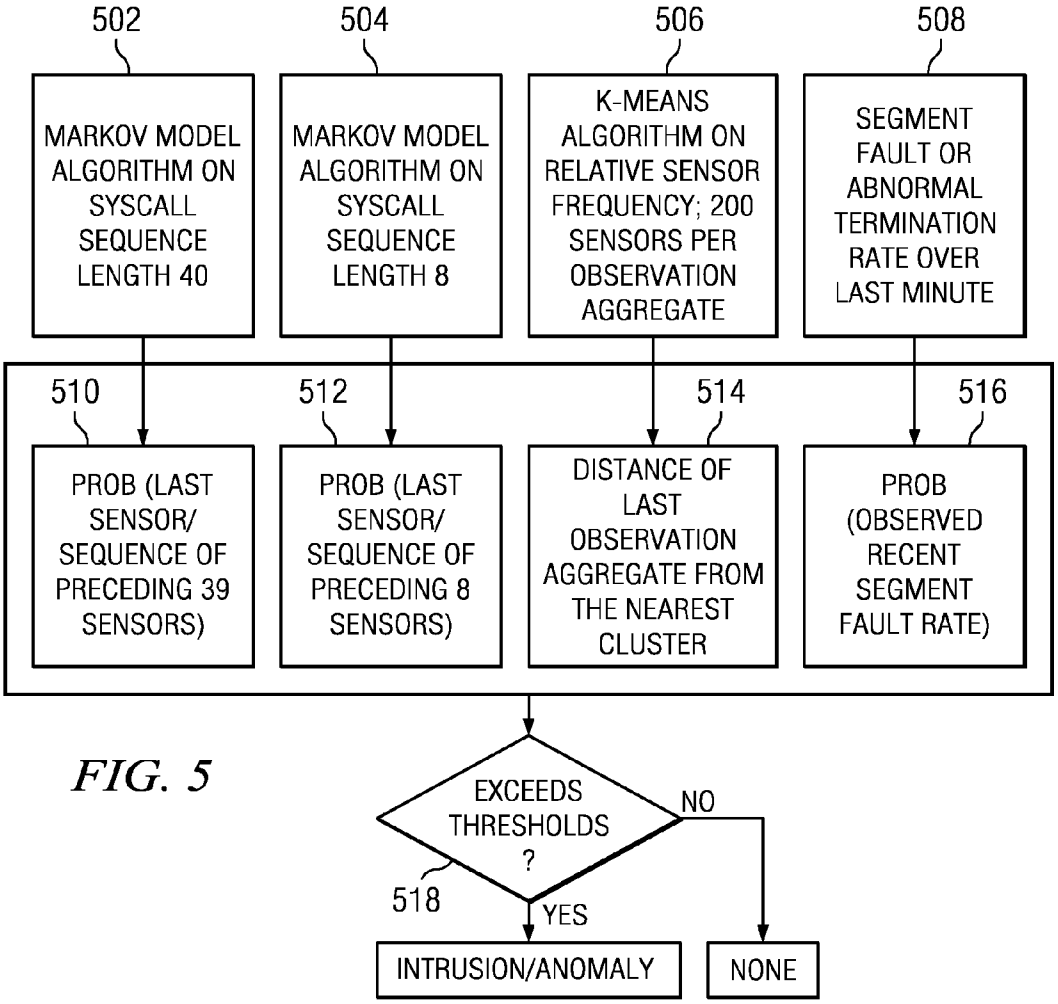



FIG. 5

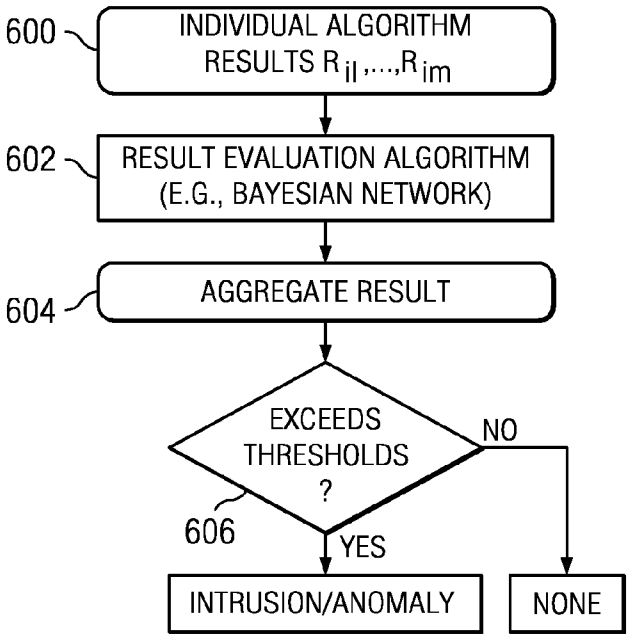



*FIG. 6*

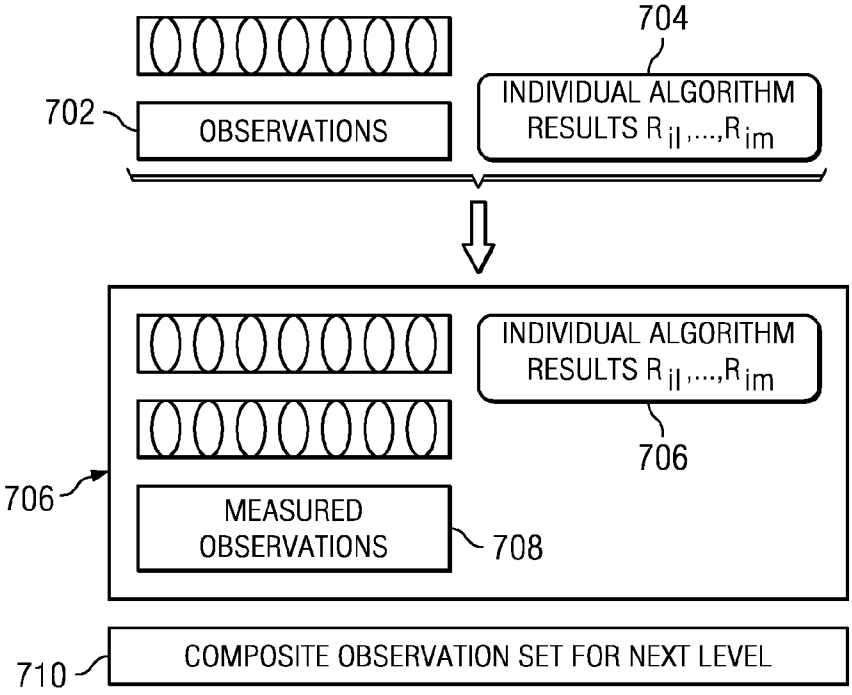



*FIG. 7*

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.