(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년10월23일
(11) 등록번호 10-1320386
(24) 등록일자 2013년10월15일

(51) 국제특허분류(Int. Cl.)
G06F 11/34 (2006.01) *G06F 15/16* (2006.01)
G06F 15/18 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2012-0022880
(22) 출원일자 2012년03월06일
심사청구일자 2012년03월06일
(65) 공개번호 10-2013-0101832
(43) 공개일자 2013년09월16일
(56) 선행기술조사문헌
논문 1 (2012.02)
논문 2 (2007)
논문 3 (2007)

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 효자동 산31 포항공과대학교내
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
정재윤
경상북도 포항시 남구 효자동 포항공과대학교 리스트 4동 4405호
홍원기
경상북도 포항시 남구 지곡동 지곡그린빌라 328-304
(뒷면에 계속)
(74) 대리인
리앤목특허법인

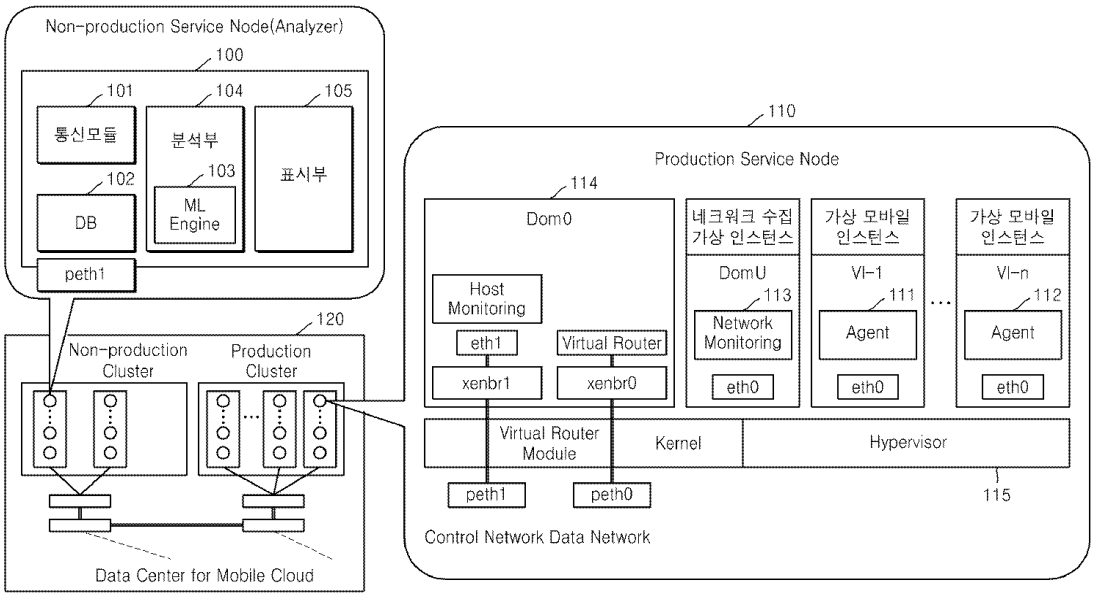
전체 청구항 수 : 총 18 항 심사관 : 임동재

(54) 발명의 명칭 **클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법**

(57) 요 약

본원 발명은 클라우드 인프라를 사용하여 모바일 단말을 가상화하는 모바일 클라우드 서비스에서 가상화 환경을 고려하여 모바일 클라우드에 할당된 가상 모바일 인스턴스들의 행동을 모니터링 하고 비정상 행동을 탐지하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법을 제공하는 것이다.

대 표 도



(72) 발명자

유재형

서울특별시 송파구 잠실2동 잠실엘스아파트 160-2102

한승희

대전광역시 동구 가양동 655-1 대주파크빌 107-205

황찬규

대전광역시 서구 둔산2동 녹원아파트 108-1205

최영락

경상북도 포항시 남구 효자동 산32 RIST 4F 정보전자융합공학부

특허청구의 범위

청구항 1

적어도 하나 이상의 상황 정보(context)의 기계 학습을 통하여 가상 인스턴스 (VI : Virtual Instance)의 상태를 분석하는 분석부로서, 상기 상황 정보는 상기 가상 인스턴스의 호스트 상황 정보 및 상기 가상 인스턴스를 포함하여 클라우드 서비스를 제공하는 서버의 네트워크 상황 정보를 포함하는, 분석부;

상기 가상 인스턴스의 상태를 표시하는 표시부;및

상기 서버의 유저 도메인 영역에 상기 네트워크 상황 정보를 수집하는 분석용 가상 인스턴스;를 포함하고,

상기 가상 인스턴스에서 발생하는 트래픽(traffic)의 상기 분석용 가상 인스턴스에 미러링(Mirroring) 방법으로 상기 네트워크 상황 정보를 수집하고, 상기 분석용 가상 인스턴스는 포트 미러링 결과 IP header, TCP/UDP header, payload를 포함한 모든 트래픽 정보를 획득하여 분석을 수행하는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 2

제 1 항에 있어서, 상기 상황 정보는

클라우드 서비스를 제공하는 서버에서 수집되는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 3

제 2 항에 있어서,

상기 서버로부터 상기 상황 정보를 수신하는 수신부;를 더 포함하는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 4

제 1 항에 있어서, 상기 분석부는

기계 학습 알고리즘을 통하여 상기 기계 학습을 수행하는 기계 학습 엔진(Machine Learning Engine)을 포함하는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 5

제 4 항에 있어서, 상기 기계 학습 알고리즘은

SVM(Support Vector Machine), Random Forest 또는 베이시안 네트워크(Bayesian Network) 중 어느 하나인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 6

삭제

청구항 7

제 1 항에 있어서,

상기 가상 인스턴스는 복수개인것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 8

제 7 항에 있어서,상기 호스트 상황 정보는

각각의 상기 가상 인스턴스에 포함된 에이전트(agent)에 의해 수집되고 동시에 상기 서버의 자원 관리 도메인 영역의 에이피아이(API : Application Programming Interface)를 통하여 수집되는 것을 특징으로 하는 클라우

드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 9

삭제

청구항 10

제 1 항에 있어서, 상기 호스트 상황 정보는

상기 가상 인스턴스의 CPU 유저 사용량, 상기 가상 인스턴스의 CPU 시스템 사용량, 상기 가상 인스턴스의 사용 메모리량, 상기 가상 인스턴스의 미사용 메모리량, 상기 가상 인스턴스의 anonymous 메모리량, 상기 가상 인스턴스의 동작 프로세스 수 및 상기 가상 인스턴스의 프로세스 생성 횟수 중 적어도 어느 하나 이상인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 11

제 1 항에 있어서, 상기 네트워크 상황 정보는

상기 가상 인스턴스가 접속한 원격 호스트 수, 상기 가상 인스턴스가 발생시긴 플로우(flow) 수, 상기 가상 인스턴스가 발생시킨 패킷 양, 상기 가상 인스턴스가 발생시킨 트래픽의 양, 상기 가상 인스턴스가 특정 포트로 발생시킨 트래픽의 양, 상기 가상 인스턴스가 Well-known 포트로 발생시킨 트래픽의 양 및 상기 가상 인스턴스가 상기 Well-known 포트가 아닌 포트로 발생시킨 트래픽의 양 중 적어도 어느 하나 이상인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 12

제 2 항에 있어서, 상기 가상 인스턴스는

모바일 가상 인스턴스이며, 상기 클라우드 서비스는 모바일 클라우드 서비스인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치.

청구항 13

클라우드 서비스를 제공하는 서버에서 수집된 적어도 하나 이상의 상황 정보 (context)를 수신하는 상황정보 수신단계;

분석부에서 상기 상황 정보(context)의 기계 학습을 통하여 가상 인스턴스 (VI : Virtual Instance)의 상태를 분석하는 분석 단계로, 상기 상황 정보는상기 가상 인스턴스의 호스트 상황 정보 및 상기 가상 인스턴스를 포함하여 클라우드 서비스를 제공하는 서버의 네트워크 상황 정보를 포함하는 분석단계;

표시부에서 상기 가상 인스턴스의 상태를 표시하는 표시 단계; 및

분석용 가상 인스턴스에서 상기 서버의 유저 도메인 영역에 상기 네트워크 상황 정보를 수집하는 단계;를 포함하고,

상기 가상 인스턴스에서 발생하는 트래픽(traffic)의 상기 분석용 가상 인스턴스에 미러링(Mirroring) 방법으로 상기 네트워크 상황 정보를 수집하고, 상기 분석용 가상 인스턴스는 포트 미러링 결과 IP header, TCP/UDP header, payload를 포함한 모든 트래픽 정보를 획득하여 분석을 수행하는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 14

제 13 항에 있어서, 상기 분석 단계는

기계 학습 알고리즘을 통하여 상기 기계 학습을 수행하는 기계 학습 엔진(Machine Learning Engine)을 포함하는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 15

제 14 항에 있어서, 상기 기계 학습 알고리즘은

SVM(Support Vector Machine), Random Forest 또는 베이시안 네트워크(Bayesian Network) 중 어느 하나인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 16

삭제

청구항 17

제 13 항에 있어서,

상기 가상 인스턴스는 복수개인것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 18

제 17 항에 있어서,상기 호스트 상황 정보는

각각의 상기 가상 인스턴스에 포함된 에이전트(agent)에 의해 수집되고 동시에 상기 서버의 자원 관리 도메인 영역의 에이피아이(API : Application Programming Interface)를 통하여 수집되는 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 19

삭제

청구항 20

제 13 항에 있어서, 상기 호스트 상황 정보는

상기 가상 인스턴스의 CPU 유저 사용량, 상기 가상 인스턴스의 CPU 시스템 사용량, 상기 가상 인스턴스의 사용 메모리량, 상기 가상 인스턴스의 미사용 메모리량, 상기 가상 인스턴스의 anonymous 메모리량, 상기 가상 인스턴스의 동작 프로세스 수 및 상기 가상 인스턴스의 프로세스 생성 횟수 중 적어도 어느 하나 이상인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 21

제 13 항에 있어서, 상기 네트워크 상황 정보는

상기 가상 인스턴스가 접속한 원격 호스트 수, 상기 가상 인스턴스가 발생시긴 플로우(flow) 수, 상기 가상 인스턴스가 발생시킨 패킷 양, 상기 가상 인스턴스가 발생시킨 트래픽의 양, 상기 가상 인스턴스가 특정 포트로 발생시킨 트래픽의 양, 상기 가상 인스턴스가 Well-known 포트로 발생시킨 트래픽의 양 및 상기 가상 인스턴스가 상기 Well-known 포트가 아닌 포트로 발생시킨 트래픽의 양 중 적어도 어느 하나 이상인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

청구항 22

제 13 항에 있어서, 상기 가상 인스턴스는

모바일 가상 인스턴스이며, 상기 클라우드 서비스는 모바일 클라우드 서비스인 것을 특징으로 하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법.

명 세 서

기 술 분 야

[0001] 본원 발명은 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법에 관한 것으로, 보다 상세하게는 모바일 클라우드 서비스의 가상 모바일 인스턴스의 행동 또는 상태를 모니터링 하고 비정상적인(abnormal) 행동을 탐지 또는 분석하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 스토리지, 컴퓨팅 등의 자원을 빌려주고 사용한 만큼 비용을 지불하는 클라우드 서비스가 주목 받고 있다.

[0003] 클라우드 인프라와 가상화 기술의 발전으로 가상 데스크탑(VD : Virtual Desk) 서비스도 점차 증가하는 추세이다.

[0004] 가상 데스크탑 서비스는 thin client를 사용하여 서버에 집중된 가상화 자원을 사용하는 것으로 클라우드 서비스와 마찬가지로 자원 할당의 신축성과 사용 비용 측면에서 상대적으로 유리하다고 알려져 있다.

[0005] 또한 최근 급격히 팽창한 모바일 시장과 클라우드 서비스를 결합함으로써 모바일 클라우드 서비스라는 용어가 등장하기 시작했다.

[0006] 모바일 클라우드 서비스는 모바일 단말을 클라우드 인프라에 가상화(virtualization)하여 제공하는 것이다.

[0007] 사용자는 클라우드의 가상화 단말에 접속하여 게임, 동영상 재생, 웹 서핑 등 기존의 모바일 서비스뿐만 아니라 고사양 3D 게임, 복잡한 연산, 대용량 스토리지 사용 등 클라우드의 장점을 활용한 서비스도 제공 받을 수 있다.

[0008] 모바일 클라우드 서비스는 모든 자원을 서비스 제공자가 사용자에게 사용한 만큼 할당하는 방식이기 때문에 서비스 제공자가 사용자의 정보를 더욱 안전하게 보호해야만 한다.

[0009] 모바일 클라우드 서비스 제공자는 안전한 서비스를 제공하기 위하여 사용자의 자원 사용을 정확하게 모니터링 해야 할 뿐 아니라 비정상적인 행동을 탐지하여 보안을 강화해야 한다.

[0010] 모바일 클라우드의 보안은 단말, 네트워크, 클라우드 인프라를 아우르는 전체 영역에서 이루어져야만 한다.

발명의 내용

해결하려는 과제

[0011] 본 발명의 실시예가 이루고자 하는 기술적 과제는, 클라우드 인프라를 사용하여 모바일 단말을 가상화하는 모바일 클라우드 서비스에서 가상화 환경을 고려하여 모바일 클라우드에 할당된 가상 모바일 인스턴스들의 행동을 모니터링 하고 비정상 행동을 탐지하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0012] 상기 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치는, 적어도 하나 이상의 상황 정보(context)의 기계 학습을 통하여 가상 인스턴스 (VI : Virtual Instance)의 상태를 분석하는 분석부; 및 상기 가상 인스턴스의 상태를 표시하는 표시부;를 포함하는 것을 특징으로 한다.

[0013] 바람직하게는 상기 상황 정보는 클라우드 서비스를 제공하는 서버에서 수집되는 것을 특징으로 한다.

[0014] 바람직하게는 상기 서버로부터 상기 상황 정보를 수신하는 수신부;를 더 포함하는 것을 특징으로 한다.

[0015] 바람직하게는 상기 분석부는 소정의 기계 학습 알고리즘을 통하여 상기 기계 학습을 수행하는 기계 학습 엔진(Machine Learning Engine)을 포함하는 것을 특징으로 한다.

[0016] 바람직하게는 상기 기계 학습 알고리즘은 SVM(Support Vector Machine), Random Forest 또는 베이시안 네트워크(Bayesian Network) 중 어느 하나인 것을 특징으로 한다.

[0017] 바람직하게는 상기 상황 정보는 상기 가상 인스턴스의 호스트 상황 정보 및 상기 가상 인스턴스를 포함하여 클라우드 서비스를 제공하는 서버의 네트워크 상황 정보를 포함하는 것을 특징으로 한다.

[0018] 바람직하게는 상기 가상 인스턴스는 복수개인것을 특징으로 한다.

[0019] 바람직하게는 상기 호스트 상황 정보는 각각의 상기 가상 인스턴스에 포함된 에이전트(agent)에 의해 수집되고 동시에 상기 서버의 자원 관리 도메인 영역의 에이피아이(API : Application Programming Interface)를 통하여 수집되는 것을 특징으로 한다.

[0020] 바람직하게는 상기 서버의 유저 도메인 영역에 상기 네트워크 상황 정보를 수집하는 분석용 가상 인스턴스;를 더 포함하고, 상기 가상 인스턴스에서 발생하는 트래픽(traffic)의 상기 분석용 가상 인스턴스에 미러링(Mirroring) 방법으로 상기 네트워크 상황 정보를 수집하는 것을 특징으로 한다.

[0021] 바람직하게는 상기 호스트 상황 정보는 상기 가상 인스턴스의 CPU 유저 사용량, 상기 가상 인스턴스의 CPU 시스템 사용량, 상기 가상 인스턴스의 사용 메모리량, 상기 가상 인스턴스의 미사용 메모리량, 상기 가상 인스턴스의 anonymous 메모리량, 상기 가상 인스턴스의 동작 프로세스 수 및 상기 가상 인스턴스의 프로세스 생성 횟수 중 적어도 어느 하나 이상인 것을 특징으로 한다.

[0022] 바람직하게는 상기 네트워크 상황 정보는 상기 가상 인스턴스가 접속한 원격 호스트 수, 상기 가상 인스턴스가 발생시긴 플로우(flow) 수, 상기 가상 인스턴스가 발생시킨 패킷 양, 상기 가상 인스턴스가 발생시킨 트래픽의 양, 상기 가상 인스턴스가 특정 포트로 발생시킨 트래픽의 양, 상기 가상 인스턴스가 Well-known 포트로 발생시킨 트래픽의 양 및 상기 가상 인스턴스가 상기 Well-known 포트가 아닌 포트로 발생시킨 트래픽의 양 중 적어도 어느 하나 이상인 것을 특징으로 한다.

[0023] 바람직하게는 상기 가상 인스턴스는 모바일 가상 인스턴스이며, 상기 클라우드 서비스는 모바일 클라우드 서비스인 것을 특징으로 한다.

[0024] 상기 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법은, 클라우드 서비스를 제공하는 서버에서 수집된 적어도 하나 이상의 상황 정보 (context)를 수신하는 상황정보 수신단계; 상기 상황 정보(context)의 기계 학습을 통하여 가상 인스턴스 (VI : Virtual Instance)의 상태를 분석하는 분석 단계; 및 상기 가상 인스턴스의 상태를 표시하는 표시 단계;를 포함하는 것을 특징으로 한다.

[0025] 바람직하게는 상기 분석 단계는 소정의 기계 학습 알고리즘을 통하여 상기 기계 학습을 수행하는 기계 학습 엔진(Machine Learning Engine)을 포함하는 것을 특징으로 한다.

[0026] 바람직하게는 상기 기계 학습 알고리즘은 SVM(Support Vector Machine), Random Forest 또는 베이시안 네트워크(Bayesian Network) 중 어느 하나인 것을 특징으로 한다.

[0027] 바람직하게는 상기 상황 정보는 상기 가상 인스턴스의 호스트 상황 정보 및 상기 가상 인스턴스를 포함하여 클라우드 서비스를 제공하는 서버의 네트워크 상황 정보를 포함하는 것을 특징으로 한다.

[0028] 바람직하게는 상기 가상 인스턴스는 복수개인것을 특징으로 한다.

[0029] 바람직하게는 상기 호스트 상황 정보는 각각의 상기 가상 인스턴스에 포함된 에이전트(agent)에 의해 수집되고 동시에 상기 서버의 자원 관리 도메인 영역의 에이피아이(API : Application Programming Interface)를 통하여 수집되는 것을 특징으로 한다.

[0030] 바람직하게는 상기 서버의 유저 도메인 영역에 상기 네트워크 상황 정보를 수집하는 분석용 가상 인스턴스;를 더 포함하고, 상기 가상 인스턴스에서 발생하는 트래픽(traffic)의 상기 분석용 가상 인스턴스에 미러링(Mirroring) 방법으로 상기 네트워크 상황 정보를 수집하는 것을 특징으로 한다.

[0031] 바람직하게는 상기 호스트 상황 정보는 상기 가상 인스턴스의 CPU 유저 사용량, 상기 가상 인스턴스의 CPU 시스템 사용량, 상기 가상 인스턴스의 사용 메모리량, 상기 가상 인스턴스의 미사용 메모리량, 상기 가상 인스턴스의 anonymous 메모리량, 상기 가상 인스턴스의 동작 프로세스 수 및 상기 가상 인스턴스의 프로세스 생성 횟수 중 적어도 어느 하나 이상인 것을 특징으로 한다.

[0032] 바람직하게는 상기 네트워크 상황 정보는 상기 가상 인스턴스가 접속한 원격 호스트 수, 상기 가상 인스턴스가 발생시긴 플로우(flow) 수, 상기 가상 인스턴스가 발생시킨 패킷 양, 상기 가상 인스턴스가 발생시킨 트래픽의 양, 상기 가상 인스턴스가 특정 포트로 발생시킨 트래픽의 양, 상기 가상 인스턴스가 Well-known 포트로 발생시킨 트래픽의 양 및 상기 가상 인스턴스가 상기 Well-known 포트가 아닌 포트로 발생시킨 트래픽의 양 중 적어도 어느 하나 이상인 것을 특징으로 한다.

[0033] 바람직하게는 상기 가상 인스턴스는 모바일 가상 인스턴스이며, 상기 클라우드 서비스는 모바일 클라우드 서비

스인 것을 특징으로 한다.

발명의 효과

[0034] 본 발명에 의한 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법에 의하면, 클라우드 인프라를 사용하여 모바일 단말을 가상화하는 모바일 클라우드 서비스에서 가상화 환경을 고려하여 모바일 클라우드에 할당된 가상 모바일 인스턴스들의 행동을 모니터링 하고 비정상 행동을 탐지할 수 있다.

[0035] 본 발명에 의한 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법에 의하면, 모바일 클라우드 서비스 제공자는 사용자의 자원 사용을 정확하게 모니터링 하고 또한 비정상적인 행동을 탐지하여 보안을 강화하고 안전한 서비스를 제공할 수 있는 효과가 있다.

도면의 간단한 설명

[0036] 도 1 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 를 포함한 시스템 구성을 보여주는 도면이다.

도 2는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 에이전트를 활용한 호스트 상황정보 수집 과정을 보여주는 도면이다.

도 3은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 Introspection을 통한 호스트 상황정보 수집 과정을 보여주는 도면이다.

도 4 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 네트워크 상황정보 수집 과정을 보여주는 도면이다.

도 5 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 구성을 보여주는 도면이다.

도 6 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 기계 학습(ML)을 위한 트레이닝 데이터의 일 실시예를 보여주는 도면이다.

도 7 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말의 트래픽 생성량의 결과를 보여주는 도면이다.

도 8 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말의 context switch의 결과를 보여주는 도면이다.

도 9 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말의 User CPU의 결과를 보여주는 도면이다.

도 10 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말이 접속한 remote host 수 결과를 보여주는 도면이다.

도 11 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 행동 분석 결과를 보여주는 도면이다.

도 12 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법의 흐름도를 보여주는 도면이다.

도 13은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 에이전트를 활용한 호스트 상황정보를 보여주는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0037] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 도면에 기재된 내용을 참조하여야 한다.

[0038] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

[0039] 본원 발명은 클라우드 인프라를 사용하여 모바일 단말을 가상화하는 모바일 클라우드 서비스에서 가상화 환경을 고려하여 모바일 클라우드에 할당된 가상 모바일 인스턴스들의 행동을 모니터링 하고 비정상 행동을 탐지하는 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 및 방법을 제공하는 것이다.

[0040] 본원 발명은 목적 달성을 위하여 1) 가상 모바일 인스턴스의 호스트 정보 수집 과정 2) 인프라 내 네트워크 정보 수집 과정 3) 수집된 호스트 정보와 네트워크 정보를 수신, 분석과정을 통하여 비정상 행동을 탐지하는 단계를 포함하여 이루어진다.

[0041] 본원 발명은 1) 원활한 클라우드 서비스 제공을 위하여 호스트 정보 및 네트워크 상황 정보를 수집하는 서버(production server)에 구별된 별도의 행동 분석 서버(non-production server)를 두어 가상 인스턴스의 행동을 분석 2) 행동 분석의 신뢰성을 높이기 위하여 에이전트 방식에 의한 호스트 정보 수집과 introspection 방식에 의한 호스트 정보 수집을 동시에 활용하는 점 3) 호스트 상황 정보(context)와 네트워크 상황 정보의 각 데이터를 기초로 기계 학습(machine learning)을 통한 행동 분석을 수행 4) 네트워크 상황 정보 수집을 위하여 가상 인스턴스를 유저 도메인 영역에 생성 5) 네트워크 상황 정보 수집을 위한 가상 인스턴스에서 미러링 방법을 활용한 점에서 특징이 있다.

[0042] 도 1 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치 를 포함한 시스템 구성을 보여주는 도면이다.

[0043] 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치를 포함한 시스템은 호스트 상황 정보 및 네트워크 상황 정보를 수집하는 상황정보 수집 장치(110), 행동 분석 장치(100)를 포함하여 이루어진다.

[0044] 상황 정보 수집 장치(110)와 행동 분석 장치(100)는 각각 별도의 서버로 구성되어지며, 행동 분석 장치(100)의 통신 모듈(101)을 통하여 상황 정보 수집 장치(110)에서 수집된 상황정보(context) 데이터의 수신이 가능하다.

[0045] 본원 발명의 행동 분석 장치(100)는 분석부(104) 및 표시부(105)를 포함하여 구성된다.

[0046] 분석부(104)는 적어도 하나 이상의 상황 정보(context)의 기계 학습을 통하여 가상 인스턴스 (VI : Virtual Instance)의 상태를 분석한다.

[0047] 표시부(105)는 분석부(104)의 결과인 가상 인스턴스의 상태를 표시한다.

[0048] 호스트 상황 정보 및 네트워크 상황 정보를 수집하는 상황 정보 수집 장치(110)는 행동 분석 장치와는 별도의 서버로서 클라우드 서비스를 가입자에 제공하는 서버이다.

[0049] 도 1 의 분석 장치(100)의 통신 모듈(101)내 수신부는 상황 정보 수집 장치(110)에서 수집된 상황 정보를 수신한다.

[0050] 분석부(104)는 소정의 기계 학습 알고리즘을 통하여 상기 기계 학습을 수행하는 기계 학습 엔진(Machine Learning Engine)(103)을 포함한다.

[0051] 기계 학습 알고리즘은 SVM(Support Vector Machine), Random Forest 또는 베이시안 네트워크(Bayesian Network) 중 어느 하나로 이루어진다.

[0052] 가상 인스턴스의 행동 분석을 위한 상황 정보는 가상 인스턴스의 호스트 상황 정보 및 클라우드 서비스를 제공하는 서버의 네트워크 상황 정보를 포함한다.

[0053] 본원 발명에서의 가상 인스턴스 행동 분석 장치는 복수개의 가상 인스턴스 행동을 동시에 분석할 수 있다.

[0054] 호스트 상황 정보는 각각의 가상 인스턴스에 포함된 에이전트(agent)에 의해 수집되거나 상황 정보 수집 서버(110)의 자원 관리 도메인 영역(Dom 0 : 114)의 에이피아이(API : Application Programming Interface)를 통하여 수집된다.

[0055] 본원 발명의 가상 인스턴스 행동 분석을 위한 호스트 상황 정보는 가상 인스턴스의 CPU 유저 사용량, 가상 인스턴스의 CPU 시스템 사용량, 가상 인스턴스의 사용 메모리량, 가상 인스턴스의 미사용 메모리량, 가상 인스턴스의 anonymous 메모리량, 가상 인스턴스의 동작 프로세스 수 및 가상 인스턴스의 프로세스 생성 횟수 중 적어도 어느 하나 이상이 될 수 있다.

[0056] 자원 관리 도메인 영역의 에이피아이(API)를 통한 호스트 상황 정보 수집은 서버(110)의 유저 영역이외에 가상화 인프라에서 Introspection을 지원하는 API(Application Programming Interface)를 활용한 구조이다.

[0057] 네트워크 상황 정보는 상황 정보 수집 서버(110)의 유저 도메인 영역(Dom U)에 네트워크 상황 정보를 수집하는 분석용 가상 인스턴스(113)에서 수행되며, 가상 인스턴스(111,112)에서 발생하는 트래픽(traffic)의 분석용 가상 인스턴스(113)에 미러링(Mirroring) 방법으로 네트워크 상황 정보를 수집한다.

[0058] 네트워크 상황 정보는 가상 인스턴스가 접속한 원격 호스트 수, 가상 인스턴스가 발생시긴 플로우(flow) 수, 가상 인스턴스가 발생시킨 패킷 양, 가상 인스턴스가 발생시킨 트래픽의 양, 가상 인스턴스가 특정 포트로 발생시킨 트래픽의 양, 가상 인스턴스가 Well-known 포트로 발생시킨 트래픽의 양 및 가상 인스턴스가 상기 Well-known 포트가 아닌 포트로 발생시킨 트래픽의 양 중 적어도 어느 하나 이상이 될 수 있다.

[0059] 본원 발명의 가상 인스턴스는 클라우드 서비스에서의 모바일 단말을 가상화한 가상 머신이며, 클라우드 서비스는 모바일 클라우드 서비스를 의미한다.

[0060] 도 2는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 에이전트를 활용한 호스트 상황정보 수집 과정을 보여주는 도면이다.

[0061] 본원 발명의 가상 인스턴스 행동 분석 시스템은 상황 정보 수집서버(110)와 분석 서버(100)를 포함하여 이루어진다.

[0062] 상황 정보 수집 서버(110)에서의 호스트 상황정보를 수집하는 방법은 에이전트를 활용한 방법과 서버 자원 관리 도메인 영역(Dom 0 : 114)에서의 Introspection을 지원하는 API(Application Programming Interface)를 활용한 방법을 동시에 이용한다.

[0063] 도 2에서의 에이전트를 활용한 호스트 상황 정보 수집은 Production 노드(110)내 각 가상 인스턴스에 설치되는 에이전트에서 수행되며,Non-production 노드(100)내 설치되어 각 가상 인스턴스에서 모니터링한 호스트 정보를 전송받아 분석하는 부분으로 나누어져 이루어진다.

[0064] Production 노드(110)라 함은 모바일 클라우드 서비스를 제공하는 역할을 담당하는 모바일 클라우드 인프라 상의 컴퓨팅 노드를 의미하고, Non-production 노드(100)라 함은 모바일 클라우드 서비스를 직접 제공하지 않고 Production 노드의 컴퓨팅을 뒷받침하거나 Production 노드의 장애 발생시 교체 가능한 노드들을 의미한다.

[0065] 클라우드에 할당된 가상 모바일 인스턴스의 호스트 상황 정보 수집은 에이전트 방식을 이용한 방법과 Introspection을 지원하는 API(Application Programming Interface)를 활용한 방법으로 크게 두 가지로 나눌 수 있다.

[0066] 첫째, 가상 인스턴스에 에이전트 방식(111,112)의 모니터링 프로그램을 설치하여 해당 프로그램으로부터 인스턴스 상황 정보를 수집하는 방법이고 둘째, 가상화 영역에서 Introspection을 지원하는 API(Application Programming Interface)를 활용한 방법(115)으로 가상 인스턴스의 상황 정보를 수집하는 방법이다.

[0067] 에이전트를 사용한 모니터링은 가상 모바일 인스턴스의 상태를 자세하게 모니터링 할 수 있다는 장점이 있으나 공격자가 에이전트를 변조하여 에이전트를 무력화 시킬 수 있다는 단점이 있다.

[0068] 가상화 영역에서의 Introspection을 통한 상황 정보(115) 수집 방법은 얻을 수 있는 정보가 제한적이고 방법이 복잡하며 가상화 핵심 역할을 수행하는 하이퍼바이저의 역할을 최대한 단순하게 가져가야 한다는 제약 조건이 있다.

[0069] 하지만 하이퍼바이저(115)가 공격 당하지 않는다면 가상 모바일 인스턴스에서는 자신이 모니터링 되고 있음을 인지할 수 없으며 정보를 조작할 수도 없다.

[0070] 본원 발명은 에이전트 방식을 이용한 방법과 Introspection을 지원하는 API(Application Programming Interface)를 활용한 방법,두 가지 세부 방식의 호스트 상황정보 수집한다.

[0071] 본원 발명의 가상 인스턴스 행동 분석 장치는 호스트 상황 정보 뿐만 아니라네트워크 상황 정보를 수집하여 클라우드의 가상 모바일 인스턴스를 모니터링 하고 비정상 행동을 탐지하는 시스템이다.

[0072] 가상 단말에 설치된 에이전트로부터, CPU, memory, 프로세스 호스트 상황정보 등을 수집하고 가상화 영역에서 수집한 호스트 상황 정보를 통해 상호 보완적으로 호스트 모니터링을 수행한다.

[0073] 또한 네트워크 상황 정보는 각 가상 단말에 대한 네트워크 정보를 수집하기 위해 가상 스위치의 기능을 사용하고, 이를 분석하는 가상화 자원(분석용 가상 인스턴스(113))을 할당하여 하이퍼바이저가 복잡한 연산을 수행하지 않도록 한다.

[0074] 도 13은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 에이전트를 활용한 호스트 상황정보를 보여주는 도면이다.

[0075] 도 13 에서 제시된 호스트 상황 정보는 가상 단말에 설치된 에이전트의 Data Collector(111-1)에서 CPU, memory, 프로세스 호스트 상황정보 등을 수집한다.

[0076] 수집된 상황 정보는 1차 가공을 통하여 데이터 베이스(DB :111-2)에 저장된다.

[0077] 또한 에이전트에 의해 수집된 상황 정보는 통신 모듈(111-4)를 통하여 분석 장치, Non-production service node의 분석 장치(100)로 전송된다.

[0078] 도 3은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 Introspection을 통한 호스트 상황 정보 수집 과정을 보여주는 도면이다.

[0079] Introspection을 통한 호스트 상황 정보 수집은 가상화 인프라에서 Introspection을 지원하는 API (Application Programming Interface)를 활용한 구조하에서 이루어진다.

[0080] 가상 모바일 인스턴스 내 에이전트를 통한 모니터링 방식만은 해당 인스턴스의 시스템 상태를 구체적으로 파악 가능하지만, 해당 에이전트에 조작 및 변조된 정보가 모니터링되는지에 대한 여부를 확인할 수 없는 문제점이 있는바 이를 보완하기 위하여 Introspection을 통한 호스트 상황 정보 수집을 수행하는 것이다.

[0081] 상황 정보 수집 서버(110)에서의 서버 자원 관리 도메인 영역(Dom 0 : 114)에서의 Introspection을 지원하는 API(Application Programming Interface)를 활용한다.

[0082] 가상화 레벨에서 호스트 정보를 수집하는 Introspection 방식은 가상 모바일 인스턴스에 보안 침해가 발생하더라도 정확한 모니터링이 가능하고, 해당 수집된 호스트 데이터와 에이전트에서 수집된 호스트 데이터와의 비교를 통해 보다 강화된 모바일 가상 인스턴스의 보안을 제공하는 장점이 있다.

[0083] 도 4 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 네트워크 상황정보 수집 과정을 보여주는 도면이다.

[0084] 종래의 가상화된 인스턴스에 대한 네트워크 상황 정보 수집 방법은 각 가상 단말에서 에이전트를 활용한 직접적인 네트워크 정보 수집과 가상화를 담당하는 하이퍼바이저를 통한 네트워크 정보 수집 방식이 있다.

[0085] 위 두 방식 중, 전자는 호스트 모니터링을 하는 에이전트 및 각 모바일 가상 단말에 많은 부담을 주는 단점이 있다.

[0086] 그리고 후자는 가상화 전반을 담당하는 하이퍼바이저에 부담을 주어 가상 모바일 단말 전체 서비스에 악영향을 미치는 단점을 안고 있다.

[0087] 본원 발명은 종래의 문제점을 해결하기 위하여 모바일 가상 인스턴스에 대한 네트워크 모니터링 방식은 모바일 가상 인스턴스에 최소한의 부하를 주기 위해 노드 내 네트워크 정보 수집을 담당하는 별도의 가상 인스턴스(113)를 생성하고, 각 모바일 가상 인스턴스에서 발생하는 트래픽을 분석용 가상 인스턴스에 미러링하는 방법을 사용한다.

[0088] 가상화 환경에서 타 가상 인스턴스에 대한 트래픽을 특정 가상 인스턴스로 미러링하는 기법은 하이퍼바이저에 트래픽 미러링을 담당하는 가상 라우터를 적용함으로써 가능하다.

[0089] 미러링(Mirroring) 방식은 하이퍼바이저에 최소한의 모듈만을 설치하여 가상화 전반적인 기능에 부담을 최소화한다.

[0090] 네트워크 상황 정보는 상황 정보 수집 서버(110)의 유저 도메인 영역(Dom U)에 네트워크 상황 정보를 수집하는 분석용 가상 인스턴스(113)에서 수행되며, 가상 인스턴스(111,112)에서 발생하는 트래픽(traffic)의 분석용 가상 인스턴스(113)에 미러링(Mirroring) 방법으로 네트워크 상황 정보를 수집한다.

[0091] 뿐만 아니라, 분석용 가상 인스턴스에서는 포트 미러링 결과 IP header, TCP/UDP header, payload를 포함한 모든 트래픽 정보를 얻을 수 있기 때문에 추후 여러가지 분석 기능을 추가 할 때 활용할 수 있다.

[0092] 분석용 가상 인스턴스(113)에서는 Netflow나 sFlow 등의 정형화된 (formatted) 플로우 정보를 사용하여 네트워크 데이터 정보 수집이 가능하다.

[0093] 트래픽 정보는 각 가상 인스턴스의 행동을 파악할 수 있는 주요한 요소이며 5-tuple flow 정보를 기본으로

한다.

[0094] 수집된 flow 정보는 각 가상 인스턴스 단위로 다시 정리되어 네트워크 데이터를 수집한다.

[0095] 다음은 위 방법을 적용하였을 때 수집 가능한 네트워크 정보 항목에 대한 예시이다.

[0096] (1) 가상 인스턴스가 접속한 remote host의 수, (2) 가상 인스턴스가 발생시킨 flow 양, (3)가상 인스턴스가 발생시킨 패킷 양, (4)가상 인스턴스가 발생시긴 트래픽의 양, (5)가상 인스턴스가 53 포트로 발생시킨 트래픽의 양, (6)가상 인스턴스가 80 포트로 발생시킨 트래픽의 양, (7)가상 인스턴스가 443 포트로 발생시킨 트래픽의 양,(8) 가상 인스턴스가 well-known 포트로 발생시킨 트래픽의 양, (9)가상 인스턴스가 well-known이 아닌 포트로 발생시킨 트래픽의 양이 일 실시예가 될 수 있다.

[0097] 도 5 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 구성을 보여주는 도면이다.

[0098] 비정상 활동을 분석하기 위해 행동 분석 장치(100)는 상황 정보를 전송받는 통신 모듈(101), DB(102)과 호스트 상황 정보 및 네트워크 상황 정보를 주기적으로 분석하여 비정상을 탐지하는 분석부(104)를 포함하여 이루어진다.

[0099] 본원 발명의 가상 인스턴스 행동 분석 시스템은 상황 정보 수집 장치(collector :110)와 분석 장치(analyzer:100)로 구분되어 구성된다.

[0100] 이는 도1 에서 도시된 바와 같이 별도의 서버로 구현됨으로써 클라우드 서비스 제공시 추가적인 트래픽 발생으로 인한 서비스 지연등의 문제점이 발생하지 않는 장점이 있다.

[0101] 상황 정보 수집 장치(collector :110)는 각 가상 모바일 단말로부터 매 분마다 호스트 상황 정보를 에이전트 또는 인트로스펙션(introspection) 결과로부터 수집한다.

[0102] 또한 각 node의 가상 모바일 인스턴스들의 네트워크 상황 정보를 수집한다.

[0103] 상황 정보 수집 장치(collector :110)는 전송 받은 호스트 모니터링 정보와 네트워크 모니터링 정보를 해독하여 데이터베이스(111-2)에 저장한다.

[0104] 분석 장치(analyzer:100)는 실제 데이터베이스에 저장된 정보를 사용하여 기계 학습 (ML, Machine Learning) 알고리즘으로 비정상 활동을 훈련 및 탐지한다.

[0105] 일정 주기마다 기존 전송되었던 데이터를 테스트 데이터로 추출하고 기계 학습 모듈(103)로 넘겨준다.

[0106] 대표적인 기계 학습 모듈로는, Weka가 있다.

[0107] Weka의 알고리즘은 기존에 training된 데이터 모델을 바탕으로 테스트 데이터에서 비정상 데이터를 찾아낸다.

[0108] 본원 발명의 특징 중 하나는 호스트 상황 정보 및 네트워크 상황 정보를 이용하여 모바일 가상 머신 또는 가상 인스턴스의 상태를 기계 학습 방법을 사용하여 비정상 행동을 탐지한다.

[0109] 본원 발명의 분석부(104)에서의 기계 학습 엔진(103)에서는 SVM, Random Forest, Bayesian Network 등의 기계 학습 알고리즘이 사용될 수 있다.

[0110] 본원 발명의 분석부(104)에서의 기계 학습을 통한 가상 모바일 인스턴스의 정상 행동과 비정상 행동을 구분하기 위해 정상 행동을 하는 상태의 데이터와 비정상 행동을 할때의 데이터를 수집해야 한다.

[0111] 이를 위해 정상인 상태를 Active와 Inactive class로 나누었고 비정상 활동은 Abnormal class를 갖는다.

[0112] (1) Inactive: 사용자가 가상 모바일 인스턴스를 사용하지 않는 상태. 트위터나 Facebook등 몇 개의 어플리케이션이 백그라운드에서 실행 중

[0113] (2) Active: 사용자가 가상 모바일 인스턴스를 사용하고 있는 상태. 웹서핑, 게임 등

[0114] (3) Abnormal: 비정상 어플리케이션이 동작하고 있는 상태. 지속적으로 정보를 빼가려 하거나 특정 도메인에 접속하려고 하는 상태로 정의된다.

[0115] 비정상 활동 분석은 수집된 Inactive 데이터 및 Active 데이터를 기반으로 이루어진다.

[0116] 비정상 데이터는 실제 배포된 악성코드 또는 malware 등을 활용해 수집 가능하다.

[0117] 모바일 단말 인스턴스에 감염 가능한 악성 프로그램들은 공격자가 모바일 단말을 좀비화 하는 것 등을 목표로

하고 있다.

[0118] 도 6 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 기계 학습(ML)을 위한 트레이닝 데이터의 일 실시예를 보여주는 도면이다.

[0119] 기계학습 (ML)의 데이터는 학습을 위한 트레이닝 데이터와 학습 결과를 바탕으로 실제 탐지를 목표로 하는 테스트 데이터로 구분된다.

[0120] 도 6은 기계 학습 엔진(103)에서의 트레이닝 데이터의 일부를 보여주는 것이다.

[0121] 트레이닝 데이터는 10개의 가상 모바일 단말로부터 수집했으며 모니터링 된 시점에서 각 가상 모바일 단말의 상태는 미리 알고 있다고 가정 한 상태로 수집하였다.

[0122] 단말의 행동 정보는 dimension 18인 vector로 나타내게 되고 이를 기계 학습 엔진(103)이 parsing 할 수 있도록 ARFF라는 데이터 포멧을 사용한다.

[0123] ARFF (Attribute-Relation File Format)는 weka에서 파일로 입출력을 수행할 때에 사용되는 속성과 관계를 설명한 파일포맷이다.

[0124] ARFF 포멧은 대략 다음과 같습니다.

[0125] @RELATION은 데이터가 어떠한 관계를 나타내고 있는지를 보여주는 데이터의 title 이다.

[0126] @ATTRIBUTE는 각 entity값이 어떤 정보를 나타내는지를 보여준다.

[0127] @DATA 이후부터는 트레이닝 데이터가 존재한다.

[0128] 각 라인은 1분동안 어떤 가상 모바일 단말 하나에서 수집된 행동 정보를 나타낸다.

[0129] 예를 들어 @DATA의 첫줄은 1.0.0.1의 2012년 1월 26일 오후 5시 20분의 상황정보 둘째줄은 1.0.0.2의 2012년 1월 26일 오후 5시 20분의 상황정보를 나타낸다.

[0130] 본원 발명에서의 가상 모바일 단말 상황 정보는 1 분동안의 통신한 원격 호스트 수, 패킷 수, flow 수, bytes 량, port 53번으로 통신한 byte 량, port 80으로 통신한 byte량, port 443으로 통신한 량, well-known port로 통신한 량, 나머지 포트로 통신한 량등의 네트워크 상황 정보 및 Process 생성 횟수, running process 수, context switch 수, system cpu 사용, user cpu 사용, mapped memory량, active memory량, anonymous memory 량, free memory량등의 호스트 상황 정보를 포함한다.

[0131] 도 7 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말의 트래픽 생성량의 결과를 보여주는 도면이다.

[0132] 도 7 은 가상 모바일 단말로부터 추출한 행동 특징을 3시간동안 모니터링하여 RRD tool을 사용해 그래프로 나타낸 예시이다. 각 단말의 모니터링된 결과는 웹 포탈로 서비스 되어 관리자가 한눈에 단말의 상태를 파악 할 수 있도록 하였으며 추가적으로 필요한 정보를 쉽게 추가 하거나 변경 할 수 있다.

[0133] 도 8 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말의 context switch의 결과를 보여주는 도면이다.

[0134] 도 8 은 가상 모바일 단말로부터 추출한 context switch의 결과를 보여주는 도면이다.

[0135] 도 9 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말의 User CPU의 결과를 보여주는 도면이다.

[0136] 도 9 는 가상 모바일 단말로부터 추출한 User CPU의 결과를 보여주는 도면이다.

[0137] 도 10 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 가상 모바일 단말이 접속한 remote host 수 결과를 보여주는 도면이다.

[0138] 도 10 은 가상 모바일 단말로부터 추출한 remote host 수 결과를 보여주는 도면이다.

[0139] 도 11 은 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 장치의 행동 분석 결과를 보여주는 도면이다.

[0140] 도 11 은 일정 주기(매 분)마다 crontab을 사용하여 지난 1분동안 서버로 전송된 데이터를 대상으로 비정상 활

동을 탐지한 결과를 나타낸 예시이다.

[0141] 각 단말의 상태는 앞서 설명한 바와 같이 Inactive, Active, Abnormal로 구분된다.

[0142] 각 상태에 따라 단말 상태를 노랑, 녹색, 적색으로 표현하여 역시 웹 포탈을 통해 보여준다.

[0143] 위 그래프는 실제 malware인 Gold Miner를 실행해 보았을 때 나타나는 모습이다.

[0144] 20:30부터 21:00까지 Gold Miner 응용프로그램을 실행 하여 플래이 하였으며 그 이후에도 서비스가 종료되지 않고 백그라운드에서 작동하여 계속해서 비정상으로 측정되는 것을 볼 수 있다. (Gold Miner 실행 중 잘못 detection 된 부분은 training set에 추가하여 현재 정상적으로 탐지되고 있음)

[0145] 이처럼 수집된 데이터는 1년 단위의 그래프까지 그릴 수 있도록 RRD 데이터베이스를 설계하였다.

[0146] 추후 대량의 트레이닝 데이터를 확보하여 알고리즘을 학습시킬 경우 보다 정확한 탐지가 가능할 것으로 예상되며, 비정상 행동뿐만 아니라 응용프로그램별 profiling, 사용자별 profiling도 가능할 것으로 예상된다.

[0147] 도 12 는 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석 방법의 흐름도를 보여주는 도면이다.

[0148] 본원 발명의 클라우드 시스템에서의 가상 인스턴스 행동 분석은 non-production service node의 서버(100)에서 수행된다.

[0149] 통신 모듈을 통하여 클라우드 서비스를 제공하는 서버(110)에서 수집된 적어도 하나 이상의 상황 정보(context)를 수신한다.

[0150] 분석부(104)에서 상황 정보(context)의 기계 학습을 통하여 가상 인스턴스 (VI : Virtual Instance)의 상태를 분석한다.

[0151] 표시부(105)는 가상 인스턴스의 상태를 active, inactive, abnormal 상태로 구분하여 표시한다.

[0152] 분석부(104)는 소정의 기계 학습 알고리즘을 통하여 기계 학습을 수행하는 기계 학습 엔진(Machine Learning Engine)을 포함하며,기계 학습 알고리즘은 SVM(Support Vector Machine), Random Forest 또는 베이시안 네트워크(Bayesian Network)등을 실시예로 들 수 있다.

[0153] 본원 발명에서의 가상 인스턴스의 행동 분석을 위한 상황 정보는 가상 인스턴스의 호스트 상황 정보 및 가상 인스턴스를 포함하여 클라우드 서비스를 제공하는 서버의 네트워크 상황 정보를 포함하여 분석 결과의 신뢰성을 높혔다.

[0154] 본원 발명에서의 행동 분석이 수행되는 가상 인스턴스는 복수개로 구성될 수 있고, 호스트 상황 정보는 각각의 가상 인스턴스에 포함된 에이전트(agent)에 의해 수집되고 동시에 상황 정보 수집 장치인 서버(110)의 자원 관리 도메인 영역의 에이피아이(API : Application Programming Interface)를 통하여 수집된다.

[0155] 행동 분석을 위한 네트워크 상황 정보는 서버(110)의 유저 도메인 영역(Dom U)에 네트워크 상황 정보를 수집하는 분석용 가상 인스턴스를 생성하여,가상 인스턴스에서 발생하는 트래픽(traffic)의 분석용 가상 인스턴스에 미러링(Mirroring) 방법으로 네트워크 상황 정보를 수집한다.

[0156] 본원 발명의 가상 인스턴스 행동 분석에서 이용되는 호스트 상황 정보는 가상 인스턴스의 CPU 유저 사용량, 가상 인스턴스의 CPU 시스템 사용량, 가상 인스턴스의 사용 메모리량, 가상 인스턴스의 미사용 메모리량, 가상 인스턴스의 anonymous 메모리량, 가상 인스턴스의 동작 프로세스 수 및 가상 인스턴스의 프로세스 생성 횟수등을 실시예로 들 수 있다.

[0157] 본원 발명의 가상 인스턴스 행동 분석에서 이용되는 네트워크 상황 정보는 가상 인스턴스가 접속한 원격 호스트 수,가상 인스턴스가 발생시긴 플로우(flow) 수, 가상 인스턴스가 발생시킨 패킷 양, 가상 인스턴스가 발생시킨 트래픽의 양, 가상 인스턴스가 특정 포트로 발생시킨 트래픽의 양, 가상 인스턴스가 Well-known 포트로 발생시킨 트래픽의 양 및 가상 인스턴스가 상기 Well-known 포트가 아닌 포트로 발생시킨 트래픽의 양 등을 실시예로 들 수 있다.

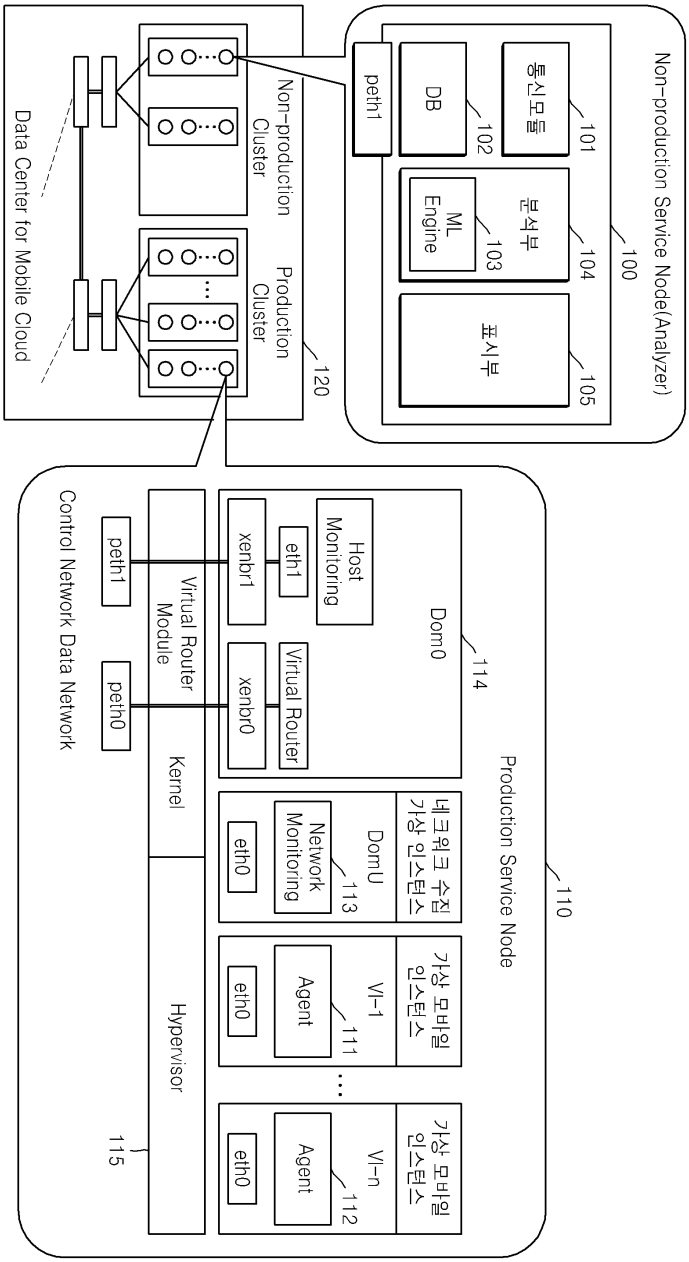
[0158] 본원 발명에서의 행동 분석을 위한 가상 인스턴스, 가상 머신은 모바일 단말을 가상화한 모바일 가상 인스턴스이며, 클라우드 서비스는 모바일 클라우드 서비스가 될 수 있다.

[0159] 이상에서와 같이 도면과 명세서에서 최적 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를

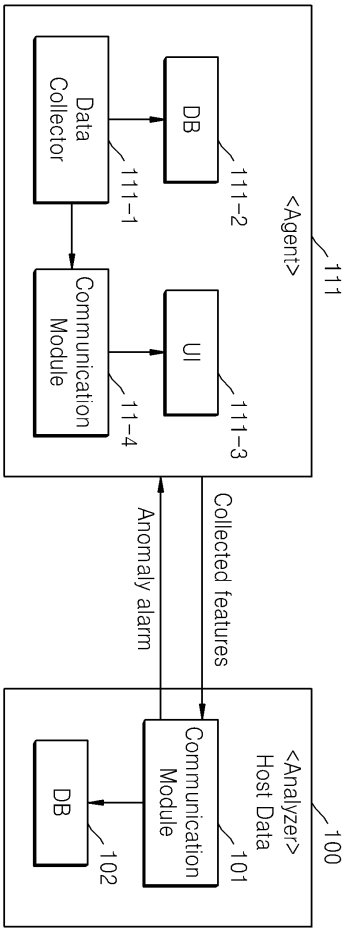
제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

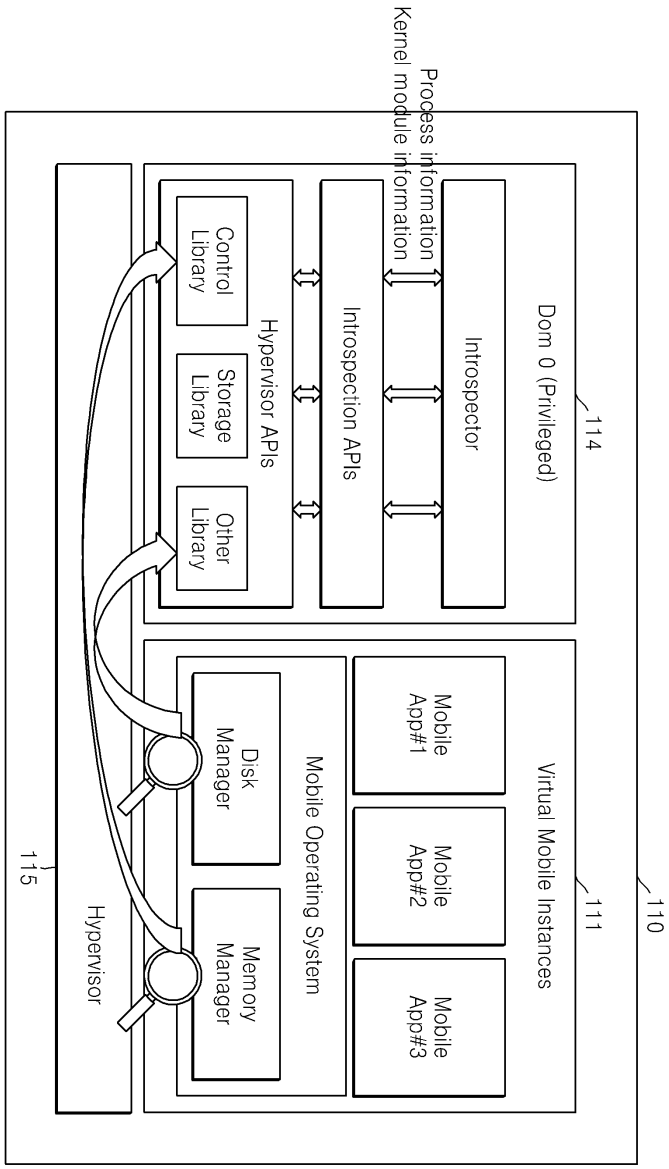
도면1



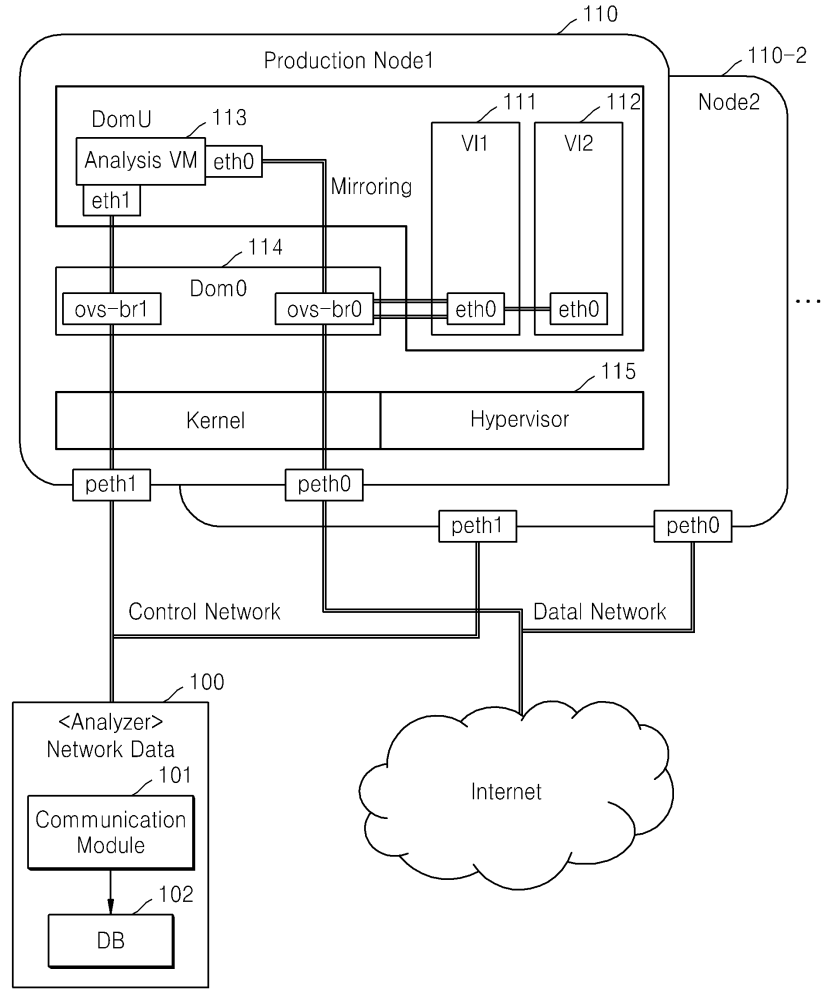
도면2


<Agent>
111
Data Collector
111-1
DB
111-2
Communication Module
11-4
UI
111-3
Anomaly alarm
Collected features
<Analyzer>
Host Data
100
Communication Module
101
DB
102

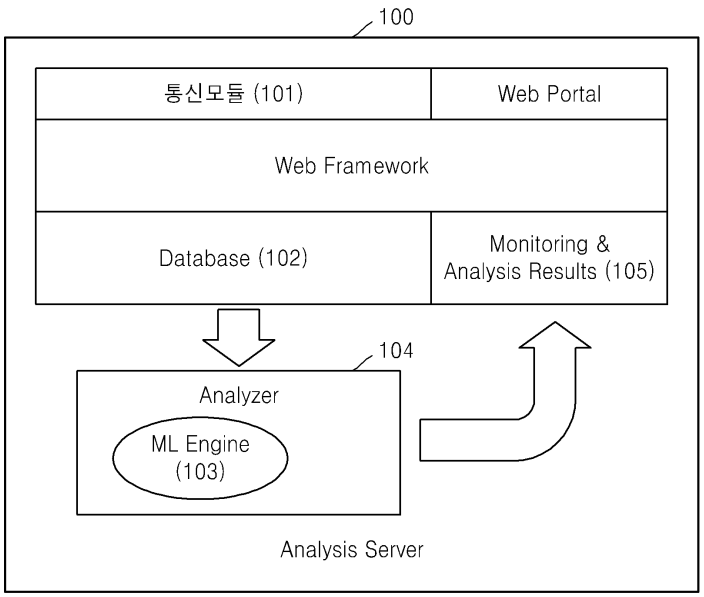
도면3


Process information
Kernel module information
Dom 0 (Privileged)
114
Introspector
Introspection APIs
Hypervisor APIs
Control Library
Storage Library
Other Library
Virtual Mobile Instances
111
Mobile App#1
Mobile App#2
Mobile App#3
Mobile Operating System
Disk Manager
Memory Manager
110
Hypervisor
115

도면4


110
Production Node1
110-2
Node2
DomU
113
Analysis VM
eth0
eth1
Mirroring
111
112
VI1
VI2
114
Dom0
ovs-br1
ovs-br0
eth0
eth0
115
Kernel
Hypervisor
peth1
peth0
peth1
peth0
Control Network
Datal Network
100
<Analyzer>
Network Data
101
Communication Module
102
DB
Internet

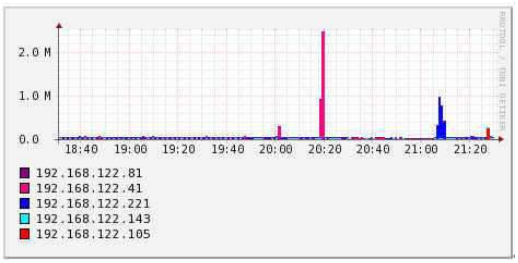
도면5


100
통신모듈 (101)
Web Portal
Web Framework
Database (102)
Monitoring & Analysis Results (105)
104
Analyzer
ML Engine (103)
Analysis Server

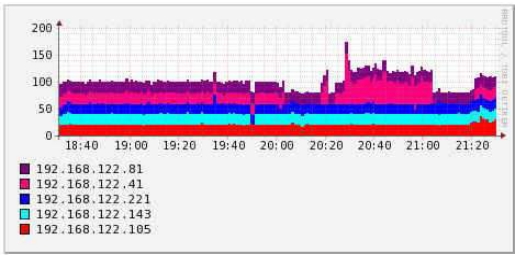
도면6

```
@RELATION  nids_hids

@ATTRIBUTE  hosts REAL
@ATTRIBUTE  pkts REAL
@ATTRIBUTE  flows REAL
@ATTRIBUTE  bytes REAL
@ATTRIBUTE  p53 REAL
@ATTRIBUTE  p80 REAL
@ATTRIBUTE  p443 REAL
@ATTRIBUTE  p1024 REAL
@ATTRIBUTE  pOthers REAL

@ATTRIBUTE  proc_c REAL
@ATTRIBUTE  proc_r REAL
@ATTRIBUTE  con_s REAL
@ATTRIBUTE  cpu_s REAL
@ATTRIBUTE  cpu_u REAL
@ATTRIBUTE  mapped REAL
@ATTRIBUTE  active REAL
@ATTRIBUTE  anonymous REAL
@ATTRIBUTE  free REAL

@ATTRIBUTE  status {inactive, active, abnormal}

2,46,4,15892,0,15892,0,0,0,33,21,389,6,52,44740,124572,90640,672576,active
2,19,3,4239,0,4239,0,0,0,31,21,649,9,88,44740,125052,91152,672196,active
5,65,8,19473,901,15002,3570,0,0,30,21,19,4,36,43592,123936,90040,674568,active
2,19,3,4339,0,4339,0,0,0,30,22,367,3,93,44976,117336,87232,679736,active
2,18,3,4155,0,4155,0,0,0,32,21,19,0,0,43920,200944,84780,565180,inactive
2,36,4,10703,0,10703,0,0,0,43,23,122,5,74,45240,127260,95148,669852,active
1,17,2,4088,0,4088,0,0,0,30,21,19,0,0,43956,200624,84408,565676,inactive
2,48,4,16863,0,16863,0,0,0,29,21,19,0,0,43956,200216,84056,565924,inactive
3,41,3,16563,364,16199,0,0,0,32,22,303,3,94,47248,116772,86800,60100,active
1,17,2,4089,0,4089,0,0,0,31,21,19,0,0,43956,200776,84568,565428,inactive
2,42,4,15207,0,15207,0,0,0,31,22,320,7,89,44936,117552,87496,679496,active
```

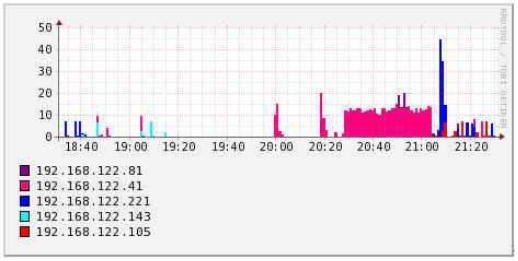
도면7



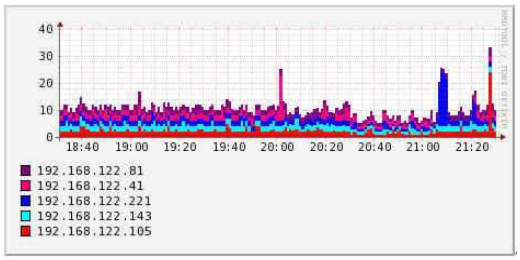
도면8



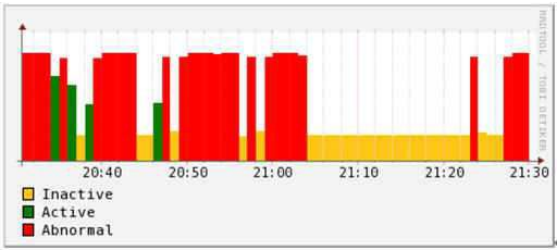
도면9



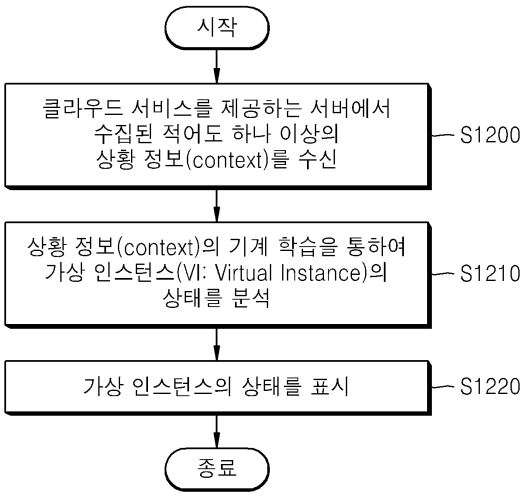
도면10



도면11



도면12



도면13

CPU(%)	Memory(KB)	Processes
CPU Usage(User)	Free memory	CPU Usage
CPU Usage(System)	Active Memory	Number of Thread
	Inactive memory	Memory Usage
	Anonymous pages	Context Switches
	Mapped pages	Non-voluntarily Context Switches
Network	OS	RX Bytes
3G TX Packets	Running processes	TX Bytes
3G TX Bytes	Context switches	
3G RX Packets	Process Created	
3G RX Bytes	Process Blocked	
WiFi TX Packets		
WiFi TX Bytes		