



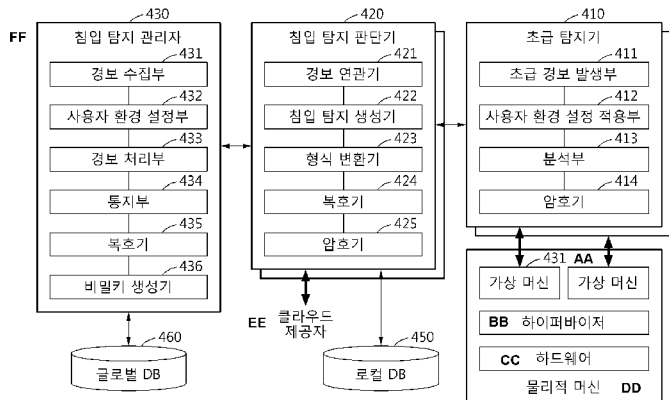
- (51) 국제특허분류:
G06F 21/20 (2006.01) G06F 11/30 (2006.01)
G06F 15/16 (2006.01)
- (21) 국제출원번호: PCT/KR2012/007754
- (22) 국제출원일: 2012년 9월 26일 (26.09.2012)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2011-0097068 2011년 9월 26일 (26.09.2011) KR
10-2011-0129243 2011년 12월 5일 (05.12.2011) KR
- (71) 출원인: 인텔렉추얼디스커버리 주식회사 (INTELLECTUAL DISCOVERY CO., LTD.) [KR/KR]; 135-090 서울시 강남구 삼성로 511, 10층, Seoul (KR).
- (72) 발명자: 허의남 (HUH, Eui Nam); 138-040 서울시 송파구 풍납동 388-7 우성아파트 2동 708호, Seoul (KR).
나상호 (NA, Sang Ho); 446-906 경기도 용인시 기흥구 서천동 1번지 전자정보대학 322호, Gyeonggi-do (KR).
박준영 (PARK, Jun Young); 446-906 경기도 용인시 기흥구 서천동 1번지 전자정보대학 322호, Gyeonggi-do (KR).
- (74) 대리인: 특허법인 무한 (MUHANN PATENT & LAW FIRM); 135-814 서울시 강남구 논현동 51-8 명림빌딩 2, 5, 6층, Seoul (KR).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) Title: METHOD AND APPARATUS FOR DETECTING AN INTRUSION ON A CLOUD COMPUTING SERVICE

(54) 발명의 명칭: 클라우드 컴퓨팅 서비스로의 침입을 탐지하는 방법 및 장치

[Fig. 4]



- 410 ... Elementary detector
411 ... Elementary alarm generating unit
412 ... User environment setup unit
413 ... Alarm processing unit
414 ... Analyzing unit
415 ... Encoder
420 ... Intrusion detecting and determining device
421 ... Alarm correlator
422 ... Intrusion detecting and generating device
423 ... Format converter
424 ... Decoder
425 ... Encoder
430 ... Intrusion detecting and managing device
431 ... Alarm collecting unit
432 ... User environment setup unit
433 ... Alarm processing unit
434 ... Notifying unit
435 ... Decoder
436 ... Secret key generator
450 ... Local DB
460 ... Global DB
AA ... Virtual machine
BB ... Hypervisor
CC ... Hardware
DD ... Physical machine
EE ... Cloud provider

(57) Abstract: Provided are a method and an apparatus for detecting an intrusion on a cloud computing service. An elementary detector monitors a virtual machine provided by the clouding computing service, and generates an elementary alarm based on the result of monitoring. An intrusion detecting and determining device compares the elementary alarm and a local database to determine whether an intrusion on a clouding computing service has occurred. The intrusion detecting and determining device generates a hyper alarm upon determining that an intrusion has occurred. An intrusion detecting and managing device compares the hyper alarm and a global database to determine whether an intrusion has occurred.

(57) 요약서: 클라우드 컴퓨팅 서비스에서의 침입을 탐지하기. 위한 방법 및 장치가 제공된다. 초급 탐지기는 클라우드 컴퓨팅 서비스에 의해 제공되는 가상 머신을 모니터링하고, 모니터링의 결과에 기반하여 초급 경보를 생성한다. 침입 탐지 판단기는 초급 경보 및 로컬 데이터베이스를 비교함으로써 클라우드 컴퓨팅 서비스로의 침입의 발생 여부를 판단한다. 침입 탐지 판단기는 침입이 발생한 것으로 판단한 경우 하이퍼 경보를 생성한다. 침입 탐지 관리자는 하이퍼 경보 및 전역 데이터베이스를 비교함으로써 침입의 발생 여부를 판단한다.



공개:

- 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

명세서

발명의 명칭: 클라우드 컴퓨팅 서비스로의 침입을 탐지하는 방법 및 장치

기술분야

- [1] 클라우드 컴퓨팅 서비스를 제공하기 위한 방법 및 장치에 관한 것으로, 보다 상세히는 클라우딩 컴퓨팅 서비스에서의 컴퓨터 시스템 또는 네트워크 상에서 발생하는 인가되지 않은 침입 행동을 실시간으로 탐지하는 방법 및 장치가 개시된다.

배경기술

- [2] 클라우드 컴퓨팅은 가상화(visualization) 기술 및 분산 처리(distributed processing) 기술을 활용함으로써 대규모의 IT 자원을 제공하는 기술이다. 클라우드 컴퓨팅 서비스에 의해 사용자는 인터넷을 통해 컴퓨팅 자원에 대한 서비스를 제공받을 수 있다. 여기서, 컴퓨팅 자원은 메모리(memory) 자원, 중앙 처리 장치(Central Processing Unit; CPU) 자원, 네트워크 자원 및 스토리지(storage) 자원 등을 포함할 수 있다. 사용자는 자신이 사용한 컴퓨팅 자원에 상응하는 요금을 클라우드 컴퓨팅 서비스의 운영 주체에게 지불할 수 있다.
- [3] 말하자면, 클라우드 컴퓨팅은 서로 상이한 물리적인 위치에 존재하는 컴퓨팅 자원들을 가상화 기술을 통해 하나의 컴퓨팅 자원으로 통합하고, 통합된 컴퓨팅 자원을 사용자들에게 제공하는 기술이다. 즉, 클라우딩 컴퓨팅은 '인터넷에 기반한 사용자 중심의 주문형 아웃소싱 서비스 기술'로 간주될 수 있다.
- [4] 사용자는, 인터넷이 제공된다면, 클라우드 컴퓨팅 서비스를 통해 자신만의 컴퓨팅 환경을 시간 및 장소에 무관하게 사용할 수 있다. 클라우딩 컴퓨팅 서비스는 사용자에게 상기의 사용자가 사용한 자원만큼의 요금을 부과한다. 또한, 사용자는 클라우드 컴퓨팅 서비스의 컴퓨팅 환경을 통해, 하드웨어 서비스, 소프트웨어 서비스 및 사후 서비스 등과 같은 모든 서비스를 제공받을 수 있다. 따라서, 시스템의 유지 및 보수 비용이 절감될 수 있고, 하드웨어 및 소프트웨어의 구매 비용이 절감될 수 있고, 컴퓨팅 처리를 위해 사용되는 에너지가 절감될 수 있다.
- [5] 클라우드 컴퓨팅 서비스가 주목을 받음에 따라, IT 대기업들의 주도 하에 클라우드 컴퓨팅 서비스가 널리 보급되고 있다. 클라우드 컴퓨팅 서비스에 있어서, 퍼블릭 클라우드(public cloud), 프라이빗 클라우드(private cloud) 등과 같은 4가지의 클라우드 컴퓨팅 서비스 타입이 존재한다.
- [6] 퍼블릭 클라우드 서비스는, 불특정된 다수의 사용자들에게 인터넷을 통해 클라우드 서비스를 제공한다. 퍼블릭 클라우드 서비스는 무상의 서비스 제공을 의미하는 것은 아니며, 서비스에 관련된 데이터 및 소스의 공개(open)을

의미하는 것 또한 아니다. 퍼블릭 클라우드 서비스에서도, 사용자 접근 제어(access control) 및 과금 등과 같은 서비스가 제공될 수 있다. 퍼블릭 클라우드 서비스 하에서는, 서비스의 제공자가 사용자의 정보를 관리하고, 모든 클라우드 컴퓨팅 서비스의 리소스들이 공유된다. 따라서, 퍼블릭 클라우드 서비스는 사용자의 개인 정보의 보호에 있어서, 취약점을 갖는다.

- [7] 프라이빗 클라우드 서비스는 퍼블릭 클라우드 서비스에서와 같은 컴퓨팅 환경을 제공한다. 프라이빗 클라우드 서비스는 특정한 기업 또는 기관에서 클라우드 컴퓨팅 서비스, 데이터 및 프로세스를 직접 관리하는 클라우드 서비스를 의미한다. 말하자면, 프라이빗 클라우드 서비스는 보안을 위해서 외부로부터의 접근을 회피하고, 인증된 사용자들만의 접근을 허용하는 폐쇄적인 클라우드 서비스 타입이다.
- [8] 커뮤니케이션 클라우드 서비스는 특정한 사용자들의 집단을 위한 클라우드 컴퓨팅 서비스이다. 커뮤니케이션 클라우드 서비스는 특정한 집단의 구성원들에게만 접근 권한을 부여한다. 집단의 구성원들은 커뮤니케이션 클라우드 서비스를 통해 서로 간에 데이터 및 어플리케이션 등을 공유한다.
- [9] 하이브리드 클라우드 서비스는 퍼블릭 클라우드 서비스 및 프라이빗 클라우드 서비스가 결합된 서비스이다. 하이브리드 클라우드 서비스는 기본적으로 퍼블릭 클라우드 서비스를 제공하며 사용자가 공유를 원치 않는 데이터 및 서비스에 대해서는 프라이빗 클라우드 서비스의 정책을 따른다.
- [10] 클라우드 컴퓨팅 서비스의 구조는 인프라형 서비스 구조, 플랫폼형 서비스 구조 및 소프트웨어 서비스 구조로 분류될 수 있다. 인프라형 서비스 구조는 사용자의 요구에 맞춰 사용자만의 컴퓨팅 환경을 제공한다. 플랫폼형 서비스 구조는 사용자의 컴퓨팅 목적에 맞게 사용자가 플랫폼을 선택하고, 선택된 플랫폼을 사용할 수 있는 환경을 제공한다. 소프트웨어 서비스 구조는 사용자가 사용 목적에 맞는 소프트웨어를 선택하여 사용할 수 있는 환경을 제공한다.
- [11] 침입 탐지는 컴퓨터 시스템이나 네트워크에서 발생하는 침입 공격 신호를 분석하는 프로세스이다. 침입 공격 신호는 트래픽 과부하 및 권한 탈취 등을 포함한다.
- [12] 악성 코드와 같은 여러 가지 이유에 기인하여 침입 사고가 발생한다. 예컨대, 공격자가 인터넷을 통해 인가되지 않은 접속을 할 수 있다. 또한, 인가된 사용자가 권한을 오용할 수 있고, 권한의 탈취를 시도할 수 있다. 일부의 침입 사고는 악의적인 것일 수 있으나, 대부분의 침입 사고는 악의적인 것이 아니다. 예컨대, 한 사용자가 컴퓨터의 주소를 잘못 입력할 수 있다. 잘못 입력된 주소로 인해, 우연히 권한을 갖지 않은 다른 시스템으로부터의 연결이 시도될 수 있다.
- [13] 침입 탐지 시스템(Intrusion Detection System; IDS)는 상술된 것과 같은 침입에 대한 탐지 프로세스를 자동으로 수행한다. 컴퓨팅 자원을 위협하는 신호를 분석함으로써 침입 행동을 실시간으로 탐지하는 시스템이다. 침입 탐지 시스템은 상기의 신호를 분석하기 위해 컴퓨터 시스템 또는 네트워크에서

발생하는 이벤트를 모니터링할 수 있다. 침입 탐지 시스템은 보안 정책 및 알려진 침입 사례 등에 기반하여 상기의 신호를 분석할 수 있다.

- [14] 침입 탐지 시스템은 크게 두 가지의 타입들로 구분될 수 있다. 두 가지의 타입들은 각각 네트워크 기반의 침입 탐지 시스템(Network-based Intrusion Detection System; NIDS) 및 호스트 기반의 침입 탐지 시스템(Host-based Intrusion Detection System; HIDS)이다.
- [15] NDIS는 네트워크 상에서 하나의 독립된 시스템으로 운용된다. NDIS는 모니터링에 있어서 네트워크 자원이 손실되지 않고, 데이터 변조가 되지 않는다는 장점을 갖는다. 또한, NDIS는 네트워크 전체에 대한 트래픽 감시 및 검사를 할 수 있다. NDIS는 오탐률이 높다는 단점 및 트래픽이 높은 네트워크에서는 탐지되지 못하는 패킷이 많아진다는 단점을 갖는다.
- [16] HIDS는 컴퓨터 시스템의 운영 체제에 추가적으로 설치거나, 일반적인 클라이언트에 설치되어 운용된다. HIDS는 시스템 호출, 애플리케이션 로그, 파일시스템 수정, 호스트와 연관된 다른 호스트의 활동 및 상기의 다른 호스트의 상태 등과 B은 데이터를 수집 및 분석한다. 상기의 수집 및 분석에 의해 침입 탐지가 수행된다. HIDS는 침입 탐지에 있어서 높은 정확도를 제공한다. HIDS는 전체적인 네트워크에 대한 침입 탐지를 할 수 없다. 또한, HIDS는 호스트의 내부에 위치하기 때문에 호스트와 함께 침입 공격의 대상이 될 수 있다.
- [17] 침입 탐지 기법은 오용 탐지(misuse detection) 기법 및 비정상 탐지(anomaly detection) 기법으로 분류될 수 있다.
- [18] 오용 탐지 기법에서, 패킷 또는 로그 정보와 같은 현재 발생 신호는 문자열 비교 연산을 통해 신호 목록과 비교된다. 오용 탐지 기법은 상기의 비교를 통해 침입을 탐지하기 때문에, 알려진 위협을 탐지함에 있어서는 매우 효과적이다. 그러나, 오용 탐지 기법은 이전에 알려지지 않은 위협, 회피 기술을 사용한 위장 위협 및 변형된 위협을 탐지함에 있어서는 비효과적이다.
- [19] 다양한 네트워크 및 각종 프로그램의 프로토콜에 있어서, 오용 탐지 기법과 같은 신호 기반 탐지 기법이 사용될 수 있는 범위는 상대적으로 좁다. 또한, 복잡한 통신 하에서는, 신호 기반 탐지 기법은 공격 탐지에 부적합하다. 또한, 상술된 것처럼, 오용 탐지 기법은 알려진 공격 패턴을 적용하는 패턴 비교를 통해 침입 탐지를 수행한다. 따라서, 오용 탐지 기법은 알려진 공격 패턴에 포함되지 않는 새로운 공격 패턴에는 취약하며, 새로운 공격 패턴에 대한 지속적인 업데이트를 한다.
- [20] 비정상 탐지 기법은 평소의 트래픽 및 신호를 정의하고, 평소의 트래픽 및 신호에 대한 편차를 지정한다. 비정상 탐지 기법은 트래픽 및 신호가 편차의 범위를 벗어날 경우 공격을 탐지하는 프로세스이다. 비정상 탐지 기법을 사용하는 침입 탐지 시스템은 사용자, 호스트, 네트워크 연결 또는 애플리케이션 등과 같은 탐지 대상의 정상적인 행동을 정의하고, 상기의 탐지 대상의 행동에 대한 허용 범위를 설정한다. 상기의 허용 범위는 탐지 대상의 행동의 정상적인

범위일 수 있다. 비정상 탐지 기법은 일정한 시간을 기준으로 탐지 대상의 행동이 설정된 허용 범위를 초과할 경우 공격이 발생한 것을 인식한다. 인식된 공격은 관리자에게 알려진다.

- [21] 비정상 탐지 기법은 통계적인 방법을 사용하여 탐지 대상의 현재의 활동 및 평소의 활동을 비교한다. 비정상 탐지 기법은 상기의 비교의 결과 비정상이 탐지되었을 때, 관리자에게 비정상이 탐지되었음을 알린다. 예컨대, 탐지된 비정상은 탐지 대상이 대역폭을 초과하여 사용한 것일 수 있다. 비정상 탐지 기법은 사용자가 전송한 전자 메일의 개수, 실패한 로그인 횟수, 일정 시간 동안의 호스트의 프로세서 사용량 등과 같은 행동 속성에 기반하여 허용 범위를 설정할 수 있다. 여기서, 일정 시간은 일 단위의 또는 주 단위의 시간일 수도 있다. 비정상 탐지 기법은 아직 알려지지 않은 위협을 탐지함에 있어서 매우 효과적이다.
- [22] 트레이닝 기간은 임계치 설정을 위해 사용되는 일정 시간이다. 비정상 탐지 기법에 있어서, 임계치의 설정은 고정적이거나 유동적일 수 있다. 고정적인 임계치 설정은 침입 탐지 시스템이 새롭게 임계치를 설정하지 않는 한 변경되지 않는 것이다. 유동적인 임계치 설정은 침입 탐지 시스템 내에서 추가적인 이벤트가 발생할 때마다 끊임없이 조정되는 것이다. 비정상 탐지 기법에 있어서, 임계치를 초과하지 않는 침입 공격은 빈번하게 발생한다. 또한, 세부적인 임계치 설정은 컴퓨팅 활동에 있어서 큰 부담을 가하고, 컴퓨팅 성능을 저하시킨다.
- [23] 예컨대, 큰 파일의 전송을 요하는 특별한 유지 활동이 오직 한 달에 한번 발생하는 경우, 상기의 유지 활동은 트레이닝 기간에는 나타나지 않는다. 그러나, 상기의 유지 활동이 지속적으로 발생하면, 비정상 탐지 기법은 상기의 유지 활동을 침입으로 간주되고 경보를 발생시킨다.
- [24] 유동적인 환경에서는, 종종 임계치를 벗어나지만 정상적인 활동이 존재할 수 있다. 따라서, 비정상 탐지 기법은 가긍정(false positive) 판단을 할 수도 있다. 비정상 탐지 기법의 사용에 있어서 주목될만한 또 다른 문제는, 다량의 복잡한 트래픽이 발생할 때에는 비정상 탐지 기법에 의해 침입 탐지에 대한 올바른 분석 및 판단이 이루어지기가 매우 어렵다는 점이다.
- [25] 상술된 NIDS 및 HIDS는 기존의 인터넷 환경에서 널리 사용되는 침입 탐지 시스템이다. 그러나, NIDS 및 HIDS는 클라우드 환경에 있어서는 부적합한 침입 탐지 시스템이다.
- [26] NIDS는 네트워크 내에 위치하여, 자신이 위치한 네트워크 전체에 대한 트래픽 분석 및 모니터링을 제공한다. 그러나, 클라우드 컴퓨팅 서비스는 가상화 기술을 이용함으로써 클라우드 컴퓨팅 시스템의 내부에서도 가상의 네트워크를 형성한다. NIDS는 내부의 가상 머신(virtual machine)들 간에서의 침입 및 클라우드 컴퓨팅 서비스의 제공자들 간의 침입 등을 고려하지 않는다. 따라서, NIDS는 클라우드 환경에서는 적합하지 않다.
- [27] HIDS는 호스트들 각각에 위치하여, 호스트의 로그 정보에 대한 검사,

호스트에서 동작하는 애플리케이션에 대한 검사 및 다른 호스트와의 통신에 대한 모니터링 등을 수행한다. HIDS의 검사 및 모니터링은 각 호스트에 독립적으로 수행된다. 따라서, HIDS는 대규모의 침입 공격 또는 합동 공격에는 취약하다는 단점을 갖는다.

- [28] 따라서, 클라우드 환경에 적 W나 새로운 침입 탐지 시스템이 요구된다.

발명의 상세한 설명

기술적 과제

- [29] 일 실시예는 NIDS 및 HIDS을 이용함으로써 클라우드 환경에 적합한 침입 탐지 방법 및 장치를 제공한다.
- [30] 일 실시예는 침입 탐지 시스템의 성능 저하 및 침입 탐지 시스템에 대한 공격 발생에 대비한 노드들 간의 인증 방법 및 장치를 제공한다.
- [31] 일 실시예는 침입 탐지 시스템의 성능 저하 및 침입 탐지 시스템에 대한 공격 발생에 대비한 암호화 방법 및 장치를 제공한다.

과제 해결 수단

- [32] 일 측에 있어서, 클라우딩 컴퓨팅 서비스에 의해 제공되는 가상 머신을 모니터링하고, 상기 모니터링의 결과에 기반하여 초급 경보를 생성하는 초급 탐지기 및 상기 초급 경보에 기반하여 상기 클라우딩 컴퓨팅 서비스로의 침입의 발생 여부를 판단하는 침입 탐지 판단기를 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템이 제공될 수 있다.
- [33] 상기 초급 탐지기는 상기 가상 머신의 트래픽 값이 임계 값을 초과하였을 때 상기 초급 경보를 생성할 수 있다.
- [34] 상기 임계 값은 상기 클라우딩 컴퓨팅 서비스의 서비스 제공자가 상기 가상 머신의 사용자에게 제공될 수 있는 범위로서 설정한 한정 범위 내로 제한될 수 있다.
- [35] 상기 초급 경보는 상기 가상 머신의 상태 값 및 임계 초과 값을 포함할 수 있다.
- [36] 상기 임계 초과 값은 상기 가상 머신이 트래픽 값이 임계 값을 초과한 정도를 나타낼 수 있다.
- [37] 상기 침입 탐지 판단기는 상기 초급 정보 및 블랙리스트를 서로 비교함으로써 상기 침입의 발생 여부를 판단할 수 있다.
- [38] 상기 블랙리스트는 상기 침입 탐지 판단기의 지역 데이터베이스 내에 저장될 수 있다.
- [39] 상기 블랙 리스트는 알려진 공격 패턴 및 관리자에 의해 작성된 공격 패턴을 포함할 수 있다.
- [40] 상기 침입 탐지 판단기는 가상 머신 별로 구성된 상기 초급 탐지기를 생성할 수 있다.
- [41] 상기 초급 탐지기는 비정상 탐지 기법을 사용할 수 있다.
- [42] 상기 가상 머신 및 상기 초급 탐지기는 각각 복수 개일 수 있다.

- [43] 상기 침입 탐지 관리자는 상기 복수 개의 초급 탐지기들로부터 상기 초급 경보를 수신할 수 있다.
- [44] 상기 클라우드 컴퓨팅 서비스의 침입 탐지 시스템은, 하이퍼 경보에 기반하여 상기 침입의 발생 여부를 판단하는 침입 탐지 관리자를 더 포함할 수 있다.
- [45] 상기 침입 탐지 판단기는 침입 정보 및 가상 머신의 상태 값을 상기 초급 경보와 연관시킴으로써 상기 하이퍼 경보를 생성할 수 있다.
- [46] 상기 침입 정보는 가상 머신에 대한 공격의 발생 장소 및 상기 공격의 패턴을 포함할 수 있다.
- [47] 상기 침입 탐지 관리자는 상기 하이퍼 경보 및 블랙리스트가 서로 유사 또는 일치하는 경우 상기 침입이 발생한 것으로 판단할 수 있다.
- [48] 다른 일 측에 따르면, 클라우딩 컴퓨팅 서비스에 의해 제공되는 가상 머신을 모니터링한 결과에 기반하여 초급 경보를 생성하는 단계 및 상기 초급 경보에 기반하여 상기 클라우드 컴퓨팅 서비스로의 침입의 발생 여부를 판단하는 단계를 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법이 제공될 수 있다.
- [49] 상기 클라우드 컴퓨팅 서비스의 침입 탐지 방법은, 하이퍼 경보에 기반하여 상기 침입의 발생 여부를 판단하는 단계를 더 포함할 수 있다.

발명의 효과

- [50] 내부의 가상 머신들 간의 침입 및 클라우드 서비스 제공자들 간의 침입 등을 탐지할 수 있고, 대규모의 침입 공격 또는 합동 공격을 탐지할 수 있는 방법 및 장치가 제공된다.
- [51] 침입 탐지 시스템의 성능 저하 및 침입 탐지 시스템에 대한 공격 발생에 대비한 노드들 간의 인증 방법 및 장치가 제공된다.
- [52] 침입 탐지 시스템의 성능 저하 및 침입 탐지 시스템에 대한 공격 발생에 대비한 암호화 방법 및 장치가 제공된다.

도면의 간단한 설명

- [53] 도 1은 공개 키 기반 암호화의 과정을 설명한다.
- [54] 도 2는 ID 기반 암호화 방법을 설명한다.
- [55] 도 3은 식별자 기반 인증 방법을 설명한다.
- [56] 도 4는 일 실시예에 따른 클라우드 컴퓨팅 서비스에서의 침입 탐지 시스템의 구성도이다.
- [57] 도 5는 일 실시예에 따른 침입 탐지 방법의 흐름도이다.

발명의 실시를 위한 형태

- [58] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [59] 도 1은 공개 키 기반 암호화의 과정을 설명한다.
- [60] 대칭 키 기반 암호화는 암호화 및 복호화에 동일한 키를 사용하는 암호화의 방식일 수 있다.

- [61] 대칭 키 기반 암호화에서 사용되는 키는 비밀(secret) 키일 수 있다. 암호화 및 복호화를 수행하는 당사자들은 동일한 비밀 키를 소유할 수 있다. 메시지의 암호화 및 복호화는 당사자들 간에 공유되는 비밀 키에 의해 수행될 수 있다. 즉, 비밀 키에 의해 암호화된 메시지는 동일한 비밀 키가 사용되지 않으면 복호화될 수 없을 수 있다.
- [62] 대칭 키 기반 암호화에 관련된 기술은, 마스터(master) 키에 기반한 기법, 페어-와이즈(pair-wise) 키에 기반한 기법 및 랜덤 키의 사전 분배에 기반한 기법 등이 있다.
- [63] 공개 키 기반 암호화는, 메시지를 암호화하는 공개 키 및 암호화된 메시지를 복호화하는 개인(private) 키가 별개로 존재하는 암호화 방식이다.
- [64] 사용자의 공개키는 일반적으로 모두에게 알려질 수 있다. 예컨대, 사용자는 공개 키 저장소로부터 자신 및 상대방의 공개 키를 제공할 수 있다.
- [65] 사용자의 개인 키는 상기의 사용자만이 알 수 있다. 메시지의 송신자는 메시지의 수신자의 공개 키로 메시지의 평문(plain text)을 암호화할 수 있고, 메시지의 암호문(encrypted text)을 수신자에게 전송할 수 있다. 메시지를 수신한 수신자는 자신의 개인 키를 사용하여 암호문을 복호화함으로써 원문을 획득할 수 있다. 상기의 암호화 및 복호화를 위해 공개 키 알고리즘이 사용될 수 있다.
- [66] 공개 키 기반 암호화는 대칭 키 기반 암호화에 비해 더 많은 연산 능력 및 메모리를 요구할 수 있다. 또한, 공개 키 기반 암호화에 있어서, 사용자들 각각의 공개키들은 사전에 인증되어야 할 수 있다.
- [67] 하기에서 도 2 및 도 3을 참조하여 식별 기반 암호화(Identity-Based Encryption; IBE)가 설명된다. IBE는 키의 사전 분배를 요구하지 않을 수 있으며, 상대적으로 적은 연산량이 요구될 수 있다. 또한, IBE는 동일한 보안 레벨에서 다른 암호화 알고리즘에 비해 수행 시간 및 메모리 사용량에 있어서 더 뛰어난 특성을 보일 수 있다.
- [68] 도 2는 ID 기반 암호화 방법을 설명한다.
- [69] 송신자는 수신자의 공개된 식별자(identifier; ID)를 이용함으로써 메시지를 암호화할 수 있다. 즉, 수신자의 ID가 수신자의 공개키로서 사용될 수 있다.
- [70] 암호화 키 ke 는 수신자의 ID i 에 기반하여 생성될 수 있다. 수신자의 공개 키로서 수신자의 ID가 사용될 수 있다. 암호화 키 ke 는 수신자의 ID i 일 수 있다.
- [71] 송신자 측에서, 메시지 m 은 암호화 키 ke 를 사용하는 암호화에 의해 암호문 c 로 변환될 수 있다. 암호문 c 는 암호화 키 ke 및 수신자의 ID i 에 기반하여 생성될 수 있다. 암호문 c 는 송신자로부터 수신자로 전달될 수 있다.
- [72] 수신자는 키 생성자로부터 복호화 키 kd 를 제공받을 수 있다. 복호화 키 kd 를 제공받기 위해서는 수신자의 인증이 필요하다. 수신자의 인증을 위해, 수신자는 키 생성자에게 수신자의 ID i 를 전송할 수 있다. 키 생성자는 수신자의 ID i 를 사용하여 수신자를 인증할 수 있다. 수신자가 인증되면 키 생성자는 복호화 키 kd 를 수신자에게 전송할 수 있다.

- [73] 수신자 측에서, 암호문 c 는 복호화 키 kd 를 사용하는 복호화에 의해 메시지 m 으로 변환될 수 있다. 메시지 m 은 복호화 키 kd 에 기반하여 생성될 수 있다.
- [74] 암호화 키 ke 및 복호화 키 kd 의 선택은 랜덤 시드 k 에 기반할 수 있다. 복호화 키 kd 는 수신자의 ID i 및 랜덤 시드 k 에 기반하여 생성될 수 있다.
- [75] 키 생성자는 IBE에서 가장 중요한 역할을 수행하는 것으로 간주될 수 있으며, 신뢰될 필요가 있다. 따라서, 키 생성자가 신뢰될 수 있는 3차 파티(3rd party)에 의해 관리되는 것이 바람직하다. 만약, 키 생성자가 위협받는 경우 IBE가 신뢰될 수 없다.
- [76] 도 3은 식별자 기반 인증 방법을 설명한다.
- [77] 식별자 기반 인증 방법은 도 2를 참조하여 전송된 식별자 기반 암호화 방법의 역순으로 수행될 수 있다.
- [78] 송신자 측에서, 메시지 m 은 서명 키 kg 를 사용하는 서명 생성(signature generation)에 의해 msi 로 암호화될 수 있다. 여기서, msi 는 메시지 및 서명(signature)일 수 있다. kg 는 비밀 키일 수 있다. 상기의 암호화는 인증을 위한 것일 수 있다.
- [79] 송신자는 서명 키 kg 를 획득하기 위해 키 생성자로 송신자의 ID i 를 전송할 수 있다. 서명 키 kg 는 수신자의 ID i 및 랜덤 시드 k 에 기반하여 생성될 수 있다. 키 생성자는 생성된 서명 키 kg 를 송신자로 전송할 수 있다.
- [80] 송신자는 생성된 msi 를 채널을 통해 전송할 수 있다. 수신자는 채널을 통해 msi 를 전송받을 수 있다. 전송된 msi 는 암호문 c 일 수 있다. 수신자는 복호화 키 kd 를 사용하여 서명을 검증함으로써 msi 가 송신자로부터 전송되었음을 검증할 수 있다. 수신자는 복호화 키 kd 를 사용하여 암호문 c 를 복호화함으로써 메시지 m 을 획득할 수 있다.
- [81] 복호화 키 kd 는 송신자의 ID i 에 기반하여 생성될 수 있다. 송신자의 ID i 는 공개된 것일 수 있다. 즉, 송신자의 공개 키로서 송신자의 ID가 사용될 수 있다. 복호화 키 kd 는 송신자의 ID i 일 수 있다.
- [82] 상기의 검증에 기반하여 수신자는 msi 가 유효한 것인지(valid) 또는 유효하지 않은 것인지(invalid)를 판단할 수 있다. 복호화에 의해 유효한 메시지 m 이 생성되는 경우, 수신자는 msi 가 유효한 것으로 판단할 수 있다. msi 가 유효하다는 것은 수신자가 인식하는 송신자로부터 msi 가 실제로 전송된 것을 의미할 수 있다.
- [83] 도 4은 일 실시예에 따른 클라우드 컴퓨팅 서비스에서의 침입 탐지 시스템의 구성도이다.
- [84] 하이퍼바이저는 하드웨어를 가상화함으로써 가상 머신(440)을 생성할 수 있다. 하이퍼바이저에 의해 하나의 물리적 머신 내에 복수 개의 가상 머신들이 생성될 수 있다. 클라우드 컴퓨팅 서비스에 의해 가상 머신(440)이 제공될 수 있다.
- [85] 클라우드 컴퓨팅 서비스에서의 침입 탐지 시스템(400)은 초급 탐지기(elementary detector)(410), 침입 탐지 판단기(420)(IDS dispatcher) 및 침입

- 탐지 관리자(430)(IDS manager)를 포함할 수 있다. 침입 탐지 시스템(400)은 클라우드 컴퓨팅 서비스로의 침입의 발생을 탐지할 수 있다.
- [86] 침입 탐지 시스템(400)은 암호화 및 복호화 기능을 제공할 수 있다.
- [87] 상술한 구성 외에 다른 구성이 클라우드 컴퓨팅 서비스에서의 침입 탐지 시스템(400)에 포함될 수 있음은 자명하다. 이하 클라우드 컴퓨팅 서비스에서의 침입 탐지 시스템(400)을 구성하는 구성요소에 대해서 상세하게 설명한다.
- [88] 초급 탐지기(410)는 사용자의 가상 머신(440)을 모니터링할 수 있다. 초급 탐지기(410)는 가상 머신(440)을 모니터링하기 위해 가상 머신(440) 내에 배치될 수 있으며, 가상 머신(440) 상에서 동작할 수 있다. 예컨대, 초급 탐지기(410)는 가상 머신(440)이 동작하는 물리적 머신(450)일 수 있다. 또는, 초급 탐지기(410)는 가상 머신(440) 내의 프로세스(process)로서 동작할 수 있다. 또는, 초급 탐지기(410)는 가상 머신(440)을 모니터링하는 프로세스(process)를 실행(execute)하는 물리적 머신(450)일 수 있다.
- [89] 초급 탐지기(410)는 비정상 탐지 기법을 사용할 수 있다.
- [90] 초급 탐지기(410)는 초급 경고 발생부(alert updater)(411), 사용자 환경 설정 적용부(412) 및 분석부(413)를 포함할 수 있다. 초급 탐지기(410)는 초급 탐지 암호기(elementary detecting encoder)(414)를 더 포함할 수 있다.
- [91] 초급 탐지기는 컴퓨팅 상태 값에 대한 수집 및 분석을 수행할 수 있다. 예컨대, 컴퓨팅 상태 값은 메모리의 사용량, CPU의 사용률, 네트워크 트래픽의 총량 및 침입 탐지 ID 등을 포함할 수 있다. 컴퓨팅 상태 값은 초급 탐지기(410)가 모니터링하는 가상 머신(440)의 상태 값일 수 있다. 상기의 컴퓨팅 상태 값은 침입 탐지 시스템(400)의 성능을 위해 수집 및 분석 가능한 컴퓨팅 상태 값들 중 소정의 일부일 수 있다.
- [92] 사용자의 가상 머신(440)은 가상 머신(440)의 상태 값을 초급 탐지기(410)로 전송할 수 있다. 가상 머신(440)의 상태 값은 네트워크 트래픽, 시스템 메모리, 시스템 파일 및 로그 등의 상태에 대한 값을 포함할 수 있다. 초급 탐지기(410)는 전송된 상태에 대한 값을 수집 및 분석할 수 있다. 상기의 전송은 실시간 전송 또는 주기적 전송일 수 있다.
- [93] 사용자는 자신의 가상 머신(440)과 관련된 초급 탐지기(410)의 임계 값을 설정할 수 있으며, 초급 탐지기(410)의 침입 탐지 기능을 추가 또는 제거할 수 있다. 여기서, 임계 값의 설정은 초급 탐지기(410)에 대한 사용자 환경 설정일 수 있다. 침입 탐지 판단기(420)는 초급 탐지기(410)에 대한 사용자 환경을 설정할 수 있고, 초급 탐지기(410)의 기능을 구성할 수 있다.
- [94] 사용자가 설정할 수 있는 임계 값의 범위는 클라우딩 컴퓨팅 서비스의 서비스 제공자가 사용자에게 제공될 수 있는 범위로서 설정한 한정 범위 내로 제한될 수 있다. 침입 탐지 관리자(430)는 사용자 환경 설정의 범위를 제한할 수 있다.
- [95] 초급 경고(raw alert)는 초급 탐지기(410)에 의해 발생하는 경고이다. 초급 경고는 가상 머신(440)을 모니터링한 결과에 기반하여 생성될 수 있다. 초급

탐지기(410)는 사용자의 가상 머신(440)의 트래픽 값이 임계 값을 초과하였을 때 초급 정보를 생성할 수 있다. 초급 정보는 임계 초과 값을 포함할 수 있다. 임계 초과 값은 가상 머신(440)의 트래픽 값이 임계 값을 초과한 정도를 나타낼 수 있다. 초급 정보는 전송된 가상 머신(440)의 상태 값을 포함할 수 있다.

- [96] 초급 정보는 침입 탐지 메시지 교체 형식(Intrusion Detection Message Exchange Form; IDMEF)과 같은 일반적인 형식으로 로컬 데이터베이스(450) 내에 저장될 수 있다. 초급 정보는 침입 여부의 결정을 위해 제공될 수 있다. 침입 여부는 초급 정보만에 의해서는 결정되지 않을 수 있다. 정확하고 자세한 분석을 위해 초급 정보는 초급 탐지기(410)로부터 침입 탐지 판단기(420)로 전송될 수 있다.
- [97] 분석부(413)는 가상 머신(440)의 트래픽 값이 임계 값을 초과했는지 여부를 판단할 수 있다.
- [98] 사용자 환경 설정 적용부(412)는 침입 탐지 관리자(430)의 사용자 환경 변수를 가상 머신(440)에 적용할 수 있다. 사용자 환경 변수는 임계 값을 포함할 수 있다.
- [99] 초급 정보 발생부(411)는 초급 정보를 발생시킬 수 있다. 초급 정보 발생부(411)는 분석부(413)가 트래픽 값이 임계 값을 초과한 것으로 판단한 경우 초급 정보를 발생시킬 수 있다. 초급 정보는 가상 머신(440)의 상태 값 및 임계 초과 값을 포함할 수 있다.
- [100] 초급 탐지기(410)가 생성될 때, 암호기(414)는 초급 탐지기(410)의 인증을 위해 침입 탐지 판단기(420)에 의해 생성된 초급 탐지기(410)의 고유 ID를 수신할 수 있다. 또한, 암호화를 위해, 암호기(414)는 침입 탐지 판단기(420)의 ID를 수신할 수 있다. 침입 탐지 판단기(420)의 ID는 침입 탐지 판단기(420)의 공개 키로서 사용될 수 있다.
- [101] 암호기(414)는 네트워크의 트래픽 값이 임계 값을 초과할 경우, 암호기(414)는 초급 정보를 침입 탐지 판단기(420)의 ID를 이용하여 암호화할 수 있다. 침입 탐지 ID, 임계 초과 값 및 가상 머신(440)의 상태 값을 포함할 수 있다.
- [102] 가상 머신(440)의 성능을 보장하기 위해, 암호기(414)는 최대한 경량화된 ID 기반 암호화 기법을 사용하여 초급 정보를 암호화할 수 있다. 침입 탐지 판단기(420)의 ID는 공개 키이므로, 초급 정보는 침입 탐지 판단기(420)의 ID를 이용함으로써 암호화될 수 있다.
- [103] 침입 탐지 판단기(420)는 침입의 발생 여부를 판단할 수 있다. 침입 탐지 판단기(420)는 침입이 발생하면 하이퍼 경고(hyper alert)를 침입 탐지 관리자(430)에게 전송할 수 있다. 하이퍼 경고는 침입에 관련하여 의심되는 데이터를 포함할 수 있다. 하이퍼 경고는 누적된 초급 정보를 포함할 수 있다.
- [104] 침입 탐지 판단기(420)는 가상 머신(440) 별로 구성된 초급 탐지기(410)를 생성 및 관리할 수 있다. 침입 탐지 판단기(420)는 클라우드 영역에 존재할 수 있다. 클라우드 정책에 따라, 복수 개의 침입 탐지 판단기들이 구성될 수 있다.
- [105] 침입 탐지 판단기(420)는 초급 정보 및 로컬 데이터베이스(450) 내의 블랙 리스트를 서로 비교함으로써 침입 여부를 판단할 수 있다. 침입 탐지

판단기(420)는 초급 정보의 가상 머신(440)의 상태 값 및 로컬 데이터베이스(450) 내의 블랙 리스트가 서로 유사 또는 일치하는 경우 침입이 발생한 것으로 판단할 수 있다. 블랙 리스트는 알려진 공격 패턴 및 침입자 관리자에 의해 작성된 공격 패턴을 포함할 수 있다. 침입 탐지 판단기(420)는 침입이 발생한 것으로 판단하면, 하이퍼 정보를 침입 탐지 관리자(IDS manager)(430)에게 전송할 수 있다.

- [106] 침입 탐지 판단기(420)는 정보 연관기(alert correlator)(421), 침입 탐지 생성기(IDS generator) 및 형식 변환기(translation engine)(423)를 포함할 수 있다. 침입 탐지 판단기(420)는 복호기(424) 및 암호기(425)를 더 포함할 수 있다.
- [107] 침입 탐지 판단기(420)는 클라우드 서버를 관리하기 위해 독립적인 서버 또는 관리 시스템으로서 운용될 수 있다. 침입 탐지 판단기(420)는 암호화를 위해 침입 탐지 관리자 ID를 저장할 수 있다. 침입 탐지 판단기(420)의 생성 및 추가시에, 침입 탐지 판단기(420) 내에 암호화를 위한 침입 탐지 관리자 ID가 저장될 수 있다.
- [108] 침입 탐지 생성기(422)는 초급 탐지기(410)를 생성할 수 있다. 침입 탐지 생성기(422)는 가상 머신(440)을 모니터링하는 초급 탐지기(410)를 생성할 수 있으며, 가상 머신(440) 내에 초급 탐지기(410)를 생성할 수 있다. 침입 탐지 생성기(422)는 생성된 초급 탐지기(410)를 관리할 수 있다.
- [109] 침입 탐지 생성기(422)는 사용자에게 의해 설정된 임계 값에 기반하여 초급 탐지기(410)를 생성 및 관리할 수 있다. 여기서, 임계 값의 설정은 초급 탐지기(410)에 대한 사용자 환경 설정일 수 있다.
- [110] 형식 변환기(423)는 초급 탐지기(411)로부터 전송된 초급 정보 및 상태 값을 IDMEF으로 변환할 수 있다. 형식 변환기(423)는 IDMEF 형식으로 변환된 초급 정보 및 상태 값을 로컬 데이터베이스(450) 내에 저장할 수 있다.
- [111] 초급 정보는 단방향으로 전송될 수 있다. 예컨대, 초급 정보는 초급 탐지기(410)로부터 형식 변환기(423)로 전송될 수 있다.
- [112] 정보 연관기(421)는 침입 정보 및 가상 머신(440)의 상태 값을 초급 정보와 연관시킴으로써 하이퍼 정보를 생성할 수 있다. 침입 정보는 가상 머신(440)에 대한 공격의 발생 장소 및 공격의 패턴을 포함할 수 있다. 정보 연관기(421)는 생성된 하이퍼 정보를 침입 탐지 관리자(430)로 전송할 수 있다.
- [113] 정보 연관기(421)는 초급 정보 및 로컬 데이터베이스(450)의 블랙리스트를 서로 비교할 수 있고, 초급 정보 및 블랙리스트가 유사 또는 일치하면 침입이 발생한 것으로 판단할 수 있다. 여기서, 초급 정보 중 상태 값 및 상태 임계 값이 비교를 위해 사용될 수 있다.
- [114] 정보 연관기(421)는 초급 정보 및 블랙리스트를 연관함으로써 의심스러운 신호 또는 공격을 판단할 수 있다. 정보 연관기(421)는 의심스러운 신호 또는 공격을 보안 관리자 또는 사용자에게 알리기 위해 하이퍼 정보를 침입 탐지 관리자(430)로 전송할 수 있다. 말하자면, 정보 연관기(421)는 복수 개의 가상

머신들 또는 클라우드들로부터 수신되는 초급 정보들 각각 및 블랙리스트를 비교함으로써 의심스러운 신호가 공격인지 여부를 확실하게 확인하기 위해 하이퍼 정보를 침입 탐지 관리자(430)로 전송할 수 있다. 예컨대, 침입 탐지 시스템(400)은 가상 머신(440)의 상태 값만을 알 수 있기 때문에, 의심스러운 신호가 공격인지 여부를 침입 탐지 관리자(430)를 통해 확인할 수 있다. 침입 탐지 관리자(430)는 복수의 초급 정보들 각각을 블랙리스트와 비교함으로써 침입 공격의 발생의 여부를 판단할 수 있다.

- [115] 침입 탐지 판단기(420)는 가짜(fake) 초급 탐지기의 식별 및 초급 탐지기(410)의 인증을 위해 침입 탐지 관리자 ID를 저장할 수 있다. 초급 탐지기(410)가 생성될 때 초급 탐지기(410)에게 부여되는 초급 탐지기 ID는 침입 탐지 관리자 ID일 수 있다. 또는, 초급 탐지기 ID는 침입 탐지 관리자 ID에 기반하여 생성될 수 있다.
- [116] 침입 탐지 관리자 ID가 수정될 경우, 침입 탐지 판단기(420)는 상기의 수정에 기반하여 갱신된 초급 탐지기 ID를 초급 탐지기(410)로 재전송할 수 있다. 초급 탐지기(410)는 갱신된 초급 탐지기 ID를 저장할 수 있다.
- [117] 침입 탐지 판단기(420)는 암호화된 초급 정보의 복호화를 수행할 수 있다. 침입 탐지 판단기(420)는 초급 정보가 포함하는 초급 탐지기 ID를 침입 탐지 관리자 ID와 비교함으로써 초급 탐지기(410)를 인증할 수 있다.
- [118] 복호기(424)는 초급 탐지기(410)의 암호기(414)에 의해 생성된 암호화된 초급 정보의 복호화를 수행할 수 있다. 복호기(424)는 상기의 복호화를 위해, 침입 탐지 관리자(430)의 비밀 키 생성기(436)에게 비밀 키를 요청할 수 있다. 비밀 키의 요청을 위해 복호기(424)는 침입 탐지 판단기 ID를 비밀 키 생성기(436)로 전송할 수 있다. 비밀 키 생성기(436)는 침입 탐지 판단기 ID에 기반하여 비밀 키를 생성할 수 있다. 비밀 키 생성기(436)는 생성된 비밀 키를 복호기(424)로 전송할 수 있다.
- [119] 복호기(424)는 전송된 비밀 키를 사용하여 암호화된 초급 정보의 복호화를 수행할 수 있다. 복호기(424)는 복호화된 초급 정보가 포함하는 초급 탐지기 ID를 침입 탐지 관리자 ID와 비교함으로써 초급 탐지기(410) 및 전송된 초급 정보를 인증할 수 있다.
- [120] 복호기(424)는 인증된 초급 정보를 형식 변환기(423)로 전송할 수 있다. 형식 변환기(423)는 전송된 초급 정보를 로컬 데이터베이스(450) 내에 저장할 수 있다. 정보 연관기(421)는 로컬 데이터베이스(450) 내에 저장된 초급 정보를 침입 패턴과 비교할 수 있다.
- [121] 암호기(425)는 침입 탐지 판단기(420)가 생성하는 하이퍼 정보 및 침입 탐지 판단기 ID를 암호화함으로써 암호화된 하이퍼 정보를 생성할 수 있다. 암호기(426)는 암호화된 하이퍼 정보를 침입 탐지 관리자(430)로 전송할 수 있다. 하이퍼 정보는 누적된 초급 정보와 연관된 공격 패턴에 대한 정보 및 의심되는 공격 패턴에 대한 정보를 포함할 수 있다.
- [122] 초급 탐지기(410) 및 가상 머신(440)은 각각 복수 개일 수 있다. 침입 탐지

관리자(430)는 복수 개의 클라우드 제공자들의 모든 초급 탐지기들의 초급 정보들을 수신할 수 있다. 침입 탐지 관리자(430)는 수신한 초급 정보들을 글로벌 데이터베이스(460) 내에 저장할 수 있다. 침입 탐지 관리자(430)는 침입탐지 판단기(420)의 하이퍼 정보 및 글로벌 데이터베이스(460)의 블랙리스트가 유사 또는 일치하면 침입이 발생한 것으로 판단할 수 있다. 침입 탐지 관리자(430)는 침입이 발생한 것으로 판단한 경우 침입 탐지를 통지할 수 있다.

- [123] 침입 탐지 관리자(430)는 복수 개의 클라우드 제공자들 각각에 위치한 침입 탐지 판단기(420)의 하이퍼 정보, 초급 정보 및 글로벌 데이터베이스(460)의 블랙리스트를 서로 비교할 수 있고, 상기의 비교에 기반하여 침입의 발생 여부를 판단할 수 있고, 침입이 발생한 것으로 판단한 경우 침입 탐지를 통지할 수 있다.
- [124] 사용자는 클라우드 서비스의 이용의 목적에 따라, 가상머신(40) 내에 생성되는 초급 탐지기(410)의 임계 값 및 기능 등을 설정할 수 있다. 상기의 임계 값 및 기능은 관리가 허용하는 범위 내에서만 설정될 수 있다. 침입 탐지 관리자는 초급 탐지기(410)의 임계 값 및 기능 등을 설정할 수 있다.
- [125] 침입 탐지 관리자(430)는 복수 개의 클라우드 제공자들의 침입 탐지 정보 및 침입 탐지 정보를 글로벌 데이터베이스(460) 내에 저장할 수 있다.
- [126] 침입 탐지 관리자(430)는 정보 수집부(alert collector)(431), 사용자 환경 설정부(432), 정보 처리부(alert processor)(433) 및 통지부(notificator)(434)를 포함할 수 있다. 침입 탐지 관리자(430)는 복호기(435) 및 비밀 키 생성기(private-key generator)(436)를 더 포함할 수 있다. 침입 탐지 관리자(430)는 침입 탐지 관리자 ID를 저장할 수 있다.
- [127] 사용자 환경 설정부(432)는 클라우드 서비스의 이용의 목적에 따라 사용자 환경 변수를 설정할 수 있다. 사용자 환경 변수는 초급 탐지기(410)의 임계 값을 포함할 수 있다.
- [128] 정보 수집부(431)는 클라우드 서버의 영역 내에서 발생하는 모든 정보들을 수신할 수 있고, 수신된 모든 정보들을 글로벌 데이터베이스(460) 내에 저장할 수 있다.
- [129] 정보 처리부(433)는 글로벌 데이터베이스(460) 내에 저장된 정보를 분석함으로써 블랙리스트를 생성할 수 있고, 침입의 발생 여부를 판단할 수 있다.
- [130] 통지부(434)는 정보 처리부(433)가 침입이 발생한 것으로 판단한 경우 침입 탐지를 사용자 및 관리자에게 통지할 수 있다.
- [131] 사용자 환경 설정부(432)는 사용자의 클라우드 서비스의 이용의 목적에 따라 가상머신(440) 내에 생성되는 초급 탐지기(410)의 임계 값 및 기능 등을 설정할 수 있다.
- [132] 정보 처리부(433)는 전송된 하이퍼 정보 및 글로벌 데이터베이스(460)의 블랙리스트를 서로 비교할 수 있고, 하이퍼 정보 및 블랙리스트가 서로 유사 또는 일치하는 경우 침입이 발생한 것으로 판단할 수 있다.

- [133] 침입 탐지 판단기(420)가 침입이 발생한 것으로 판단하지 않아서 하이퍼 정보가 없는 경우, 정보 처리부(433) 복수 개의 클라우드들에서 발생한 초급 정보들 및 각각과 글로벌 데이터베이스(460) 내의 블랙리스트를 비교할 수 있고, 초급 정보 및 블랙리스트가 서로 유사 또는 일치하는 경우 침입이 발생한 것으로 판단할 수 있다.
- [134] 정보 처리부(433)는 하이퍼 정보가 전송된 경우 우선적으로 글로벌 데이터베이스(460) 내에 저장된 초급 정보, 하이퍼 정보 및 블랙리스트에 기반하여 침입이 발생하였는지 여부를 판단할 수 있다.
- [135] 정보 수집부(431)는 클라우드 서버 영역에서 발생하는 모든 정보들을 수신할 수 있으며, 정보 처리부(433)가 수신된 정보들을 처리할 수 있도록 수신된 정보들을 글로벌 데이터베이스(460) 내에 저장할 수 있다.
- [136] 통지부(434)는, 정보 처리부(433)가 새로운 침입이 발생한 것으로 판단한 경우, 상기의 침입의 침입 패턴을 기존의 블랙리스트에 추가할 수 있고, 침입 패턴이 추가된 블랙리스트를 글로벌 데이터베이스(460) 내에 저장할 수 있다. 통지부(434)는 침입 패턴이 추가된 블랙리스트를 모든 침입 탐지 판단기들 각각으로 전송할 수 있다. 통지부(434)는 침입에 관련된 목록을 작성할 수 있다. 통지부(434)는 사용자에게 의해 목록이 요청된 경우, 사용자에게 목록을 제공할 수 있다.
- [137] 통지부(434)는 정보 처리부(433)가 침입이 발생한 것으로 판단한 경우 침입 탐지를 사용자 및 관리자에게 통지할 수 있다.
- [138] 침입 탐지 관리자(430)는 침입 탐지 판단기 ID 및 모든 초급 탐지기들의 초급 탐지기 ID를 저장할 수 있다.
- [139] 모든 초급 탐지기들에서 생성된 초급 정보들은 침입 탐지 관리자(430)로 전송될 수 있다. 초급 정보의 인증을 위해, 침입 탐지 관리자(430)는 초급 탐지기 ID를 저장 및 관리할 수 있다.
- [140] 침입 탐지 관리자(430)는 침입 탐지 판단기(420)가 추가될 때, 침입 탐지 판단기 ID를 침입 탐지 판단기(420)에게 부여할 수 있다. 침입 탐지 관리자(430)는 하이퍼 정보의 복호화 및 인증을 수행할 수 있다.
- [141] 침입 탐지 관리자(430)는 모든 초급 탐지기들의 초급 탐지기 ID들을 알고 있다. 따라서, 복호기(435)는 초급 탐지기(410)의 초급 탐지기 ID 및 암호 키를 사용하여 암호화된 초급 정보의 복호화를 수행할 수 있다. 복호기(435)는 침입 탐지 관리자 ID 및 비밀 키 생성기(436)를 사용함으로써 침입 탐지 판단기(420)의 암호기(425)에서 생성된 암호화된 하이퍼 정보의 복호화를 수행할 수 있다. 복호화의 수행 후에, 복호기(435)는 초급 정보의 인증 및 하이퍼 정보의 인증을 수행할 수 있다.
- [142] 비밀 키 생성기(437)는 ID에 대응하는 비밀 키를 생성할 수 있다. 비밀 키 생성기(437)는 노드로부터 ID를 포함하는 요청을 수신하면, ID에 대응하는 비밀 키를 생성할 수 있고, 생성된 비밀 키를 노드로 전송할 수 있다.

- [143] 비밀 키 생성기(437)는 IBE의 키 생성자와 동일한 기능을 수행할 수 있다. 비밀 키 생성기(437)는 노드의 ID에 대응하는 비밀 키를 생성할 수 있고, 생성된 비밀 키를 비밀 키를 요청한 노드에게 제공할 수 있다.
- [144] 침입 탐지 관리자(420) 및 로컬 데이터베이스(450)는 각각 복수 개일 수 있다. 복수 개의 클라우드 제공자들은 각각 침입 탐지 관리자(420) 및 로컬 데이터베이스(450)를 운영할 수 있다.
- [145] 도 5는 일 실시예에 따른 침입 탐지 방법의 흐름도이다.
- [146] 단계(510)에서, 침입 탐지 관리자(430)의 사용자 환경 설정부(432)는 클라우드 서비스의 이용의 목적에 따라 사용자 환경 변수를 설정할 수 있다. 사용자 환경 변수는 초급 탐지기(410)의 임계 값을 포함할 수 있다.
- [147] 사용자는 클라우드 서비스에 가입할 때, 클라우드 서비스의 이용을 위해, 사용자 환경 설정부(432)에서 초급 탐지기(410)의 임계 값을 포함하는 사용자 환경 변수를 설정할 수 있다.
- [148] 단계(512)에서, 사용자에게 클라우드 서비스를 제공하는 가상 머신(440)이 생성될 수 있다.
- [149] 단계(520)에서, 침입 탐지 판단기(420)의 침입 탐지 생성기(422)는 초급 탐지기(410)를 생성할 수 있다. 침입 탐지 생성기(422)는 가상 머신(440)이 생성될 때 정해진 컴퓨팅 자원을 사용할 수 있다.
- [150] 단계(522)에서, 침입 탐지 생성기(422)는 생성된 초급 탐지기(10)에게 초급 탐지기 ID를 부여할 수 있다.
- [151] 단계(524)에서, 초급 탐지기(10)는 부여된 초급 탐지기 ID를 저장할 수 있다. 초급 탐지기 ID는 암호화된 통신을 위해 사용될 수 있다.
- [152] 단계(526)에서, 초급 탐지기(410)의 사용자 환경 설정 적용부(412)는 초급 탐지기(410)의 성능을 구성할 수 있다. 사용자 환경 설정 적용부(412)는 임계 값 및 침입 탐지 기능의 추가 및 삭제 등에 기반하여 초급 탐지기(410)의 성능을 구성할 수 있다.
- [153] 단계(530)에서, 가상 머신(440)은 가상 머신(440)의 상태 값을 초급 탐지기(410)로 전송할 수 있다. 상기의 전송은 실시간 전송 또는 주기적 전송일 수 있다.
- [154] 단계(532)에서, 초급 탐지기(410)의 분석부(413)는 전송된 상태 값을 확인함으로써 가상 머신(440)의 트래픽 값이 임계 값을 초과했는지 여부를 판단할 수 있다.
- [155] 분석부(413)가 트래픽 값이 임계 값을 초과한 것으로 판단한 경우, 하기의 단계들이 계속 수행될 수 있다.
- [156] 분석부(413)가 트래픽 값이 임계 값을 초과한 것으로 판단한 경우, 단계(540)에서, 초급 탐지기(410)의 초급 정보 발생부(411)는 초급 정보를 생성할 수 있다.
- [157] 단계(540)에서 생성된 초급 정보는 임계 초과 값 및 가상 머신(440)의 상태 값을

포함하기 때문에, 암호화가 요구된다. 단계(542)에서, 초급 탐지 암호기(414)는 초급 정보를 침입 탐지 판단기(420)의 ID를 사용하여 암호화함으로써 암호화된 초급 정보를 생성할 수 있다.

[158] 단계(544)에서, 초급 정보 발생부(411) 또는 초급 탐지 암호기(414)는 초급 정보를 침입 탐지 판단기(420)로 전송할 수 있다. 상기의 초급 정보는 암호화된 초급 정보일 수 있다.

[159] 침입 탐지 판단기(420)는 초급 정보를 수신할 수 있다. 수신된 초급 정보가 암호화된 수신 정보인 경우, 하기의 단계들(546, 548, 550 및 552)이 수행될 수 있다.

[160] 암호화된 초급 정보는 침입 탐지 판단기 ID로 암호화될 수 있다. 단계(546)에서, 침입 탐지 판단기(420)는 초급 정보의 복호화를 위해 침입 탐지 관리자(430)의 비밀 키 생성기(436)에게 비밀 키를 요청할 수 있다. 침입 탐지 판단기(420)는 비밀 키 생성기(436)에게 초급 탐지기(410)의 인증을 요청할 수 있다. 침입 탐지 판단기(420)는 침입 탐지 판단기 ID를 사용하여 비밀 키 생성기(436)에게 비밀 키를 요청할 수 있다.

[161] 단계(548)에서, 비밀 키 생성기(436)는 침입 탐지 판단기 ID에 기반하여 생성된 비밀 키를 침입 탐지 판단기(420)로 전송할 수 있다.

[162] 단계(550)에서, 침입 탐지 판단기(420)의 복호기(424)는 수신된 비밀 키를 사용하여 암호화된 초급 정보의 복호화를 수행할 수 있다.

[163] 단계(552)에서, 침입 탐지 판단기(420)는 초급 정보가 포함하는 초급 탐지기 ID를 침입 탐지 관리자 ID와 비교함으로써 초급 탐지기(410)를 인증할 수 있다.

[164] 초급 정보가 포함하는 초급 탐지기 ID가 가짜 초급 탐지기 ID인 경우, 침입 탐지 판단기(420)는 하이퍼바이저 또는 가상 머신(440)에게 가짜 초급 정보가 발견된 것을 통보할 수 있다. 하이퍼바이저 또는 가상 머신(440)에게 가짜 초급 정보 대해 관련된 조치를 취할 수 있다.

[165] 단계(554)에서, 침입 탐지 판단기(420)는 초급 정보를 침입 탐지 관리자(410)로 전송할 수 있다. 침입 탐지 관리자(410)로 전송된 초급 정보는 암호화된 초급 정보일 수 있다. 침입 탐지 판단기(420)의 암호기(425)는 초급 정보의 암호화를 수행할 수 있다. 상기의 전송은 주기적 전송일 수 있다.

[166] 단계(560)에서, 침입 탐지 판단기(420)는 초급 정보의 데이터를 분석함으로써 침입의 발생 여부를 판단할 수 있다. 상기의 초급 정보는 누적된 초급 정보일 수 있다. 침입 탐지 판단기(420)는 초급 정보 및 로컬 데이터베이스(450)의 블랙리스트를 서로 비교할 수 있고, 초급 정보 및 블랙리스트가 유사 또는 일치하면 침입이 발생한 것으로 판단할 수 있다. 여기서, 초급 정보 중 상태 값 및 상태 임계 값이 비교를 위해 사용될 수 있다.

[167] 침입이 발생한 것으로 판단한 경우, 단계(562)에서, 침입 탐지 판단기(420)는 하이퍼 정보를 생성할 수 있다.

[168] 단계(564)에서, 암호기(425)는 침입 탐지 관리자 ID를 이용함으로써 하이퍼

경보의 암호화를 수행할 수 있다.

- [169] 단계(566)에서, 침입 탐지 판단기(420)는 하이퍼 경보를 침입 탐지 관리자(430)로 전송할 수 있다. 상기의 하이퍼 경보는 암호화된 하이퍼 경보일 수 있다.
- [170] 단계(570)에서, 침입 탐지 관리자(430)는 암호화된 초급 경보를 복호화하기 위한 제1 비밀 키 및 암호화된 하이퍼 경보를 복호화하기 위한 제2 비밀 키를 생성할 수 있다. 침입 탐지 관리자(430)는 비밀 키 생성기(436)에게 제1 비밀 키 및 제2 비밀 키의 생성을 요청할 수 있다. 상기의 요청을 위해, 침입 탐지 관리자(430)는 침입 탐지 판단기 ID 및 침입 탐지 관리자 ID를 비밀 키 생성기(436)로 전송할 수 있다. 비밀 키 생성기(436)는 침입 탐지 판단기 ID에 기반하여 제1 비밀 키를 생성할 수 있고, 침입 탐지 관리자 ID에 기반하여 제2 비밀 키를 생성할 수 있다. 비밀 키 생성기(436)는 생성된 제1 비밀 키 및 제2 비밀 키를 침입 탐지 관리자(430)로 전송할 수 있다.
- [171] 단계(572)에서, 침입 탐지 관리자(430)의 복호기(435)는 제1 비밀 키를 사용함으로써 암호화된 초급 경보의 복호화를 수행할 수 있다. 복호기(435)는 제2 비밀 키를 사용함으로써 암호화된 하이퍼 경보의 복호화를 수행할 수 있다.
- [172] 단계(574)에서, 침입 탐지 관리자(430)는 초급 정보의 인증 및 하이퍼 정보의 인증을 수행할 수 있다. 침입 탐지 관리자(430)는 초급 정보가 포함하는 침입 탐지 관리자 ID를 침입 탐지 관리자(430)가 저장하는 침입 탐지 관리자 ID와 비교함으로써 초급 탐지기(410)를 인증할 수 있다. 침입 탐지 관리자(430)는 하이퍼 정보가 포함하는 침입 탐지 관리자 ID를 침입 탐지 관리자(430)가 저장하는 침입 탐지 관리자 ID와 비교함으로써 침입 탐지 판단기(420)를 인증할 수 있다.
- [173] 단계(580)에서, 침입 탐지 관리자(430)는 침입의 발생 여부를 판단할 수 있다. 침입 탐지 관리자(430)는 복수 개의 클라우드 제공자들 각각에 위치한 침입 탐지 판단기(420)의 하이퍼 경보, 초급 경보 및 글로벌 데이터베이스(460)의 블랙리스트를 서로 비교할 수 있고, 상기의 비교에 기반하여 침입의 발생 여부를 판단할 수 있다.
- [174] 또한, 침입 탐지 판단기(420)에서 침입이 발생한 것으로 판단하지 않아 하이퍼 경보가 존재하지 않는 경우, 경보 처리부(433)는 초급 경보 및 글로벌 데이터베이스(460)의 블랙리스트를 서로 비교할 수 있고, 상기의 비교에 기반하여 침입의 발생 여부를 판단할 수 있다.
- [175] 경보 처리부(433)는 침입이 발생한 것으로 판단한 경우, 침입의 발생을 통지부(34)에게 알릴 수 있다. 경보 처리부(433)는 전송된 하이퍼 경보 및 글로벌 데이터베이스(460)의 블랙리스트를 서로 비교할 수 있고, 하이퍼 경보 및 블랙리스트가 서로 유사 또는 일치하는 경우 침입이 발생한 것으로 판단할 수 있다.
- [176] 침입 탐지 판단기(420)가 침입이 발생한 것으로 판단하지 않아서 하이퍼

경보가 없는 경우, 경보 처리부(433) 복수 개의 클라우드들에서 발생한 초급 경보들 및 각각과 글로벌 데이터베이스(460) 내의 블랙리스트를 비교할 수 있고, 초급 경보 및 블랙리스트가 서로 유사 또는 일치하는 경우 침입이 발생한 것으로 판단할 수 있다.

- [177] 경보 수집부(431)는 클라우드 서버의 영역 내에서 발생하는 모든 경보들을 수신할 수 있고, 수신된 모든 경보들을 글로벌 데이터베이스(460) 내에 저장할 수 있다. 정보 수집부(431)는 침입 탐지 판단기(420) 또는 침입 탐지 관리자(430)로부터 전송된 초급 경보 및 하이퍼 경보를 수신할 수 있다. 정보 수집부(431)는 수집된 초급 경보 및 하이퍼 경보를 경보 처리부(433)가 사용할 수 있게 하기 위해 글로벌 데이터베이스(460) 내에 저장할 수 있다.
- [178] 단계(582)에서, 통지부(434)는 경보 처리부(433)가 침입이 발생한 것으로 판단한 경우 침입 탐지를 사용자 및 관리자에 통지할 수 있다.
- [179] 통지부(434)는, 경보 처리부(433)가 새로운 침입이 발생한 것으로 판단한 경우, 상기의 침입의 침입 패턴을 기존의 블랙리스트에 추가할 수 있고, 침입 패턴이 추가된 블랙리스트를 글로벌 데이터베이스(460) 내에 저장할 수 있다. 통지부(434)는 침입 패턴이 추가된 블랙리스트를 모든 침입 탐지 판단기들 각각으로 전송할 수 있다.
- [180] 앞서 설명한 기술적 내용들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예들을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 하드웨어 장치는 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [181] 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 특히, 본 실시예에서는 터치 감지 디스플레이의 화면에 디지털 콘텐츠를 표시하는 콘텐츠 표시 코드와, 터치 감지 디스플레이에 대한 사용자의 터치 입력을 통해 디지털 콘텐츠에서 사용자가 선택한 객체를 인식하는 객체 인식 코드와, 사용자의 요청에 따라 객체에 애니메이션을 적용한 애니메이션 데이터를 생성하여 저장하는 애니메이션 저장

코드와, 디지털 콘텐츠의 내용이 구분된 항목 별로 각 항목에서 생성된 에너지 데이터의 개수를 카운트 하는 에너지 카운트 코드와, 사용자의 요청에 따라 항목 별 에너지 데이터의 개수를 제공하는 에너지 제공 코드를 포함하는 프로그램이 기록되는 컴퓨터 판독 가능 매체를 포함할 수 있다. 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용 어플리케이션(예를 들어, 스마트폰 어플리케이션, 피쳐폰 VM(virtual machine) 등의 형태) 등으로 구성될 수 있다. 이는, 사용자 단말 및/또는 전자책 서비스 시스템의 메모리에 저장되어 사용자 단말 및/또는 전자책 서비스 시스템에서 구동되는 적어도 하나의 프로세서에 의해 실행되도록 구성될 수 있다.

[182] 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 또한, 상술한 파일 시스템은 컴퓨터 판독이 가능한 기록 매체에 기록될 수 있다.

[183] 이상과 같이 실시예를 통해 설명된 기술적 내용은 다양한 수정 및 변형이 가능하다. 그러므로, 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

청구범위

- [청구항 1] 클라우드 컴퓨팅 서비스에 의해 제공되는 가상 머신을 모니터링하고, 상기 모니터링의 결과에 기반하여 초급 경보를 생성하는 초급 탐지기; 및
상기 초급 경보에 기반하여 상기 클라우드 컴퓨팅 서비스로의 침입의 발생 여부를 판단하는 침입 탐지 판단기를 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 2] 제1항에 있어서,
상기 초급 탐지기는 상기 가상 머신의 트래픽 값이 임계 값을 초과하였을 때 상기 초급 경보를 생성하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 3] 제2항에 있어서,
상기 임계 값은 상기 클라우드 컴퓨팅 서비스의 서비스 제공자가 상기 가상 머신의 사용자에게 제공될 수 있는 범위로서 설정한 한정 범위 내로 제한되는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 4] 제1항에 있어서,
상기 초급 경보는 상기 가상 머신의 상태 값 및 임계 초과 값을 포함하고,
상기 임계 초과 값은 상기 가상 머신이 트래픽 값이 임계 값을 초과한 정도를 나타내는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 5] 제1항에 있어서,
상기 침입 탐지 판단기는 상기 초급 정보 및 블랙리스트를 서로 비교함으로써 상기 침입의 발생 여부를 판단하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 6] 제5항에 있어서,
상기 블랙리스트는 상기 침입 탐지 판단기의 지역 데이터베이스 내에 저장된, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 7] 제5항에 있어서,
상기 블랙 리스트는 알려진 공격 패턴 및 관리자에 의해 작성된 공격 패턴을 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 8] 제1항에 있어서,
상기 침입 탐지 판단기는 가상 머신 별로 구성된 상기 초급 탐지기를 생성하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 9] 제1항에 있어서,

- 상기 초급 탐지기는 비정상 탐지 기법을 사용하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 10] 제1항에 있어서,
상기 가상 머신 및 상기 초급 탐지기는 각각 복수 개이고,
상기 침입 탐지 관리자는 상기 복수 개의 초급 탐지기들로부터
상기 초급 정보를 수신하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 11] 제1항에 있어서,
하이퍼 정보에 기반하여 상기 침입의 발생 여부를 판단하는 침입 탐지 관리자
를 더 포함하고,
상기 침입 탐지 판단기는 침입 정보 및 가상 머신의 상태 값을 상기 초급 정보와 연관시킴으로써 상기 하이퍼 정보를 생성하는,
클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 12] 제11항에 있어서,
상기 침입 정보는 가상 머신에 대한 공격의 발생 장소 및 상기 공격의 패턴을 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 13] 제11항에 있어서,
상기 침입 탐지 관리자는 상기 하이퍼 정보 및 블랙리스트가 서로 유사 또는 일치하는 경우 상기 침입이 발생한 것으로 판단하는,
클라우드 컴퓨팅 서비스의 침입 탐지 시스템.
- [청구항 14] 클라우딩 컴퓨팅 서비스에 의해 제공되는 가상 머신을 모니터링한 결과에 기반하여 초급 정보를 생성하는 단계; 및
상기 초급 정보에 기반하여 상기 클라우딩 컴퓨팅 서비스로의 침입의 발생 여부를 판단하는 단계
를 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법.
- [청구항 15] 제14항에 있어서,
상기 초급 정보는 상기 가상 머신의 트래픽 값이 임계 값을 초과하였을 때 생성되는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법.
- [청구항 16] 제14항에 있어서,
상기 초급 정보는 상기 가상 머신의 상태 값 및 임계 초과 값을 포함하고,
상기 임계 초과 값은 상기 가상 머신이 트래픽 값이 임계 값을 초과한 정도를 나타내는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법.
- [청구항 17] 제14항에 있어서,

상기 침입의 발생 여부는 상기 초급 정보 및 블랙리스트를 서로 비교함으로써 판단되는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법.

[청구항 18]

제17항에 있어서,

상기 블랙 리스트는 알려진 공격 패턴 및 관리자에 의해 작성된 공격 패턴을 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법.

[청구항 19]

제17항에 있어서,

하이퍼 정보에 기반하여 상기 침입의 발생 여부를 판단하는 단계를 더 포함하고,

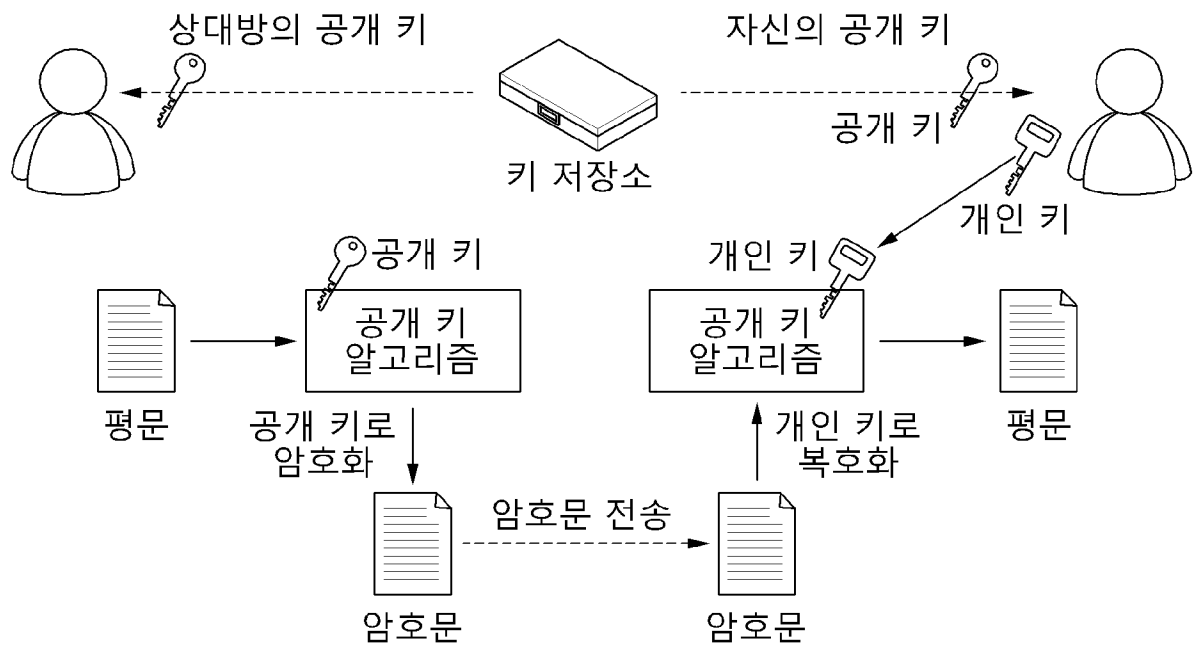
상기 하이퍼 정보는 침입 정보 및 가상 머신의 상태 값을 상기 초급 정보와 연관시킴으로써 생성되는, 클라우드 컴퓨팅 서비스의 침입 탐지 방법.

[청구항 20]

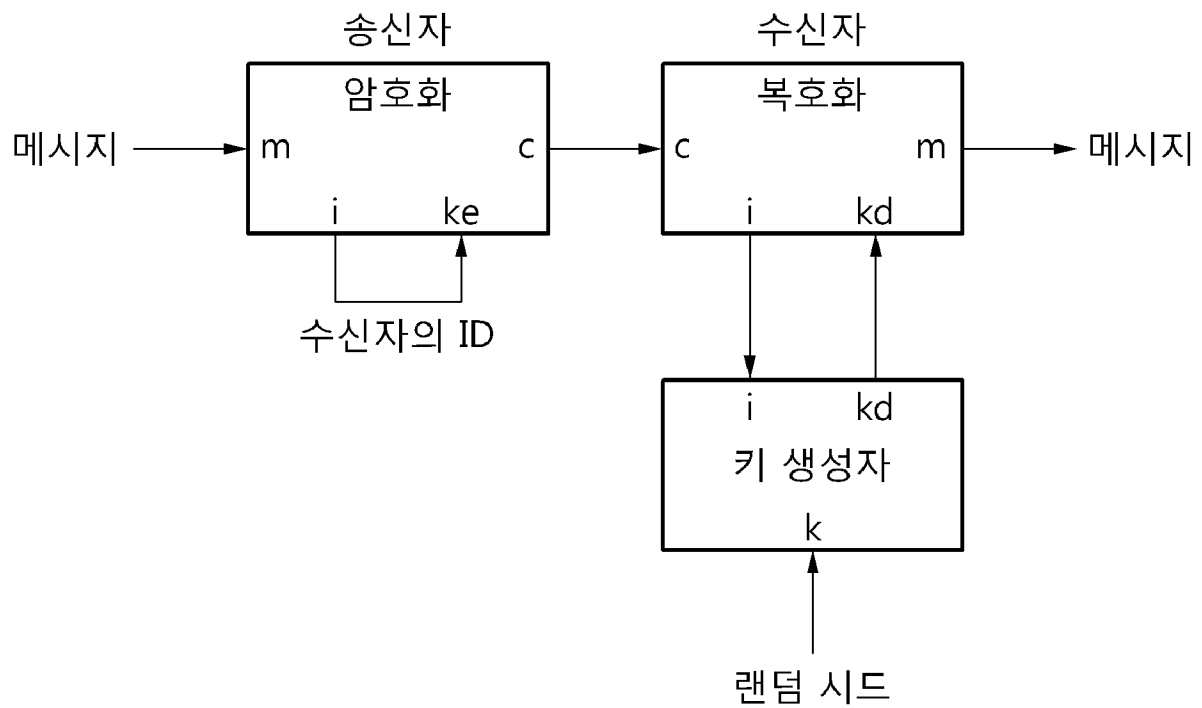
제19항에 있어서,

상기 침입 정보는 가상 머신에 대한 공격의 발생 장소 및 상기 공격의 패턴을 포함하는, 클라우드 컴퓨팅 서비스의 침입 탐지 시스템.

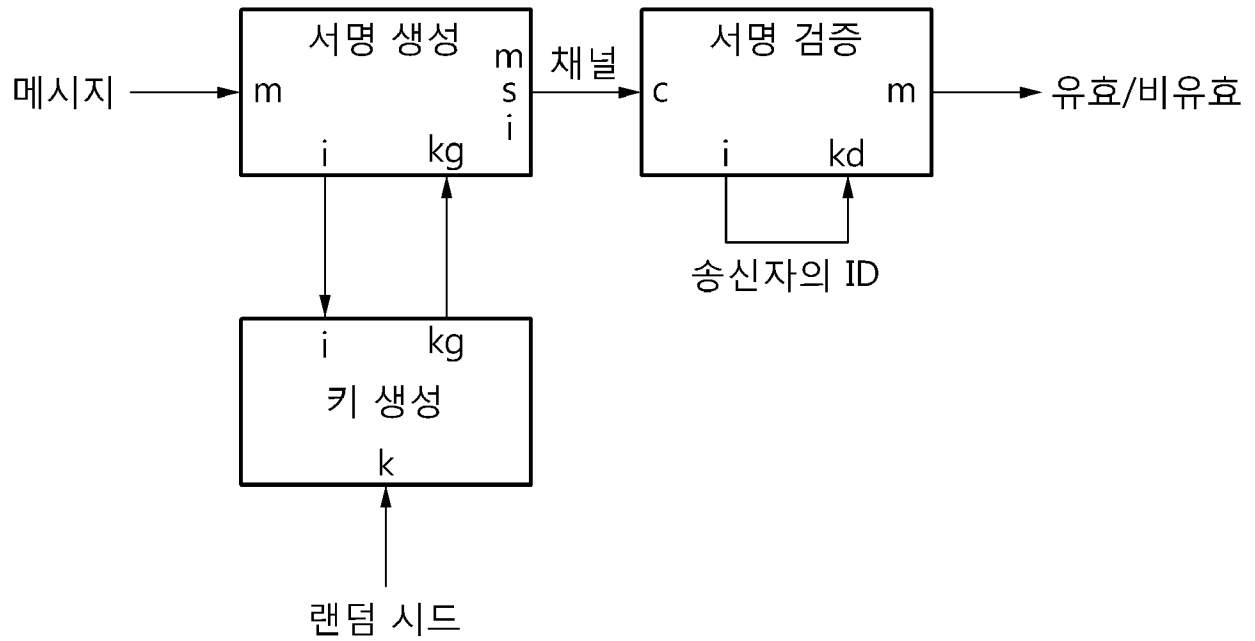
[Fig. 1]



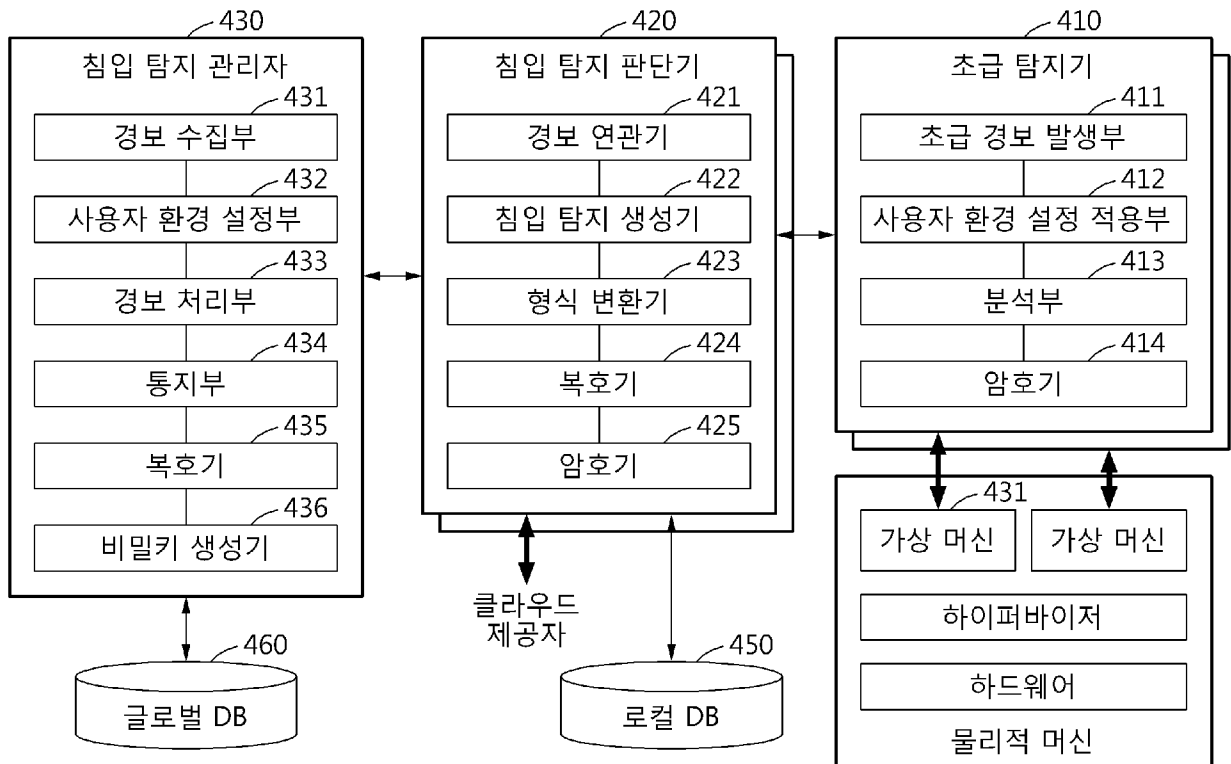
[Fig. 2]



[Fig. 3]



[Fig. 4]



[Fig. 5]

