(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0077009
(43) 공개일자 2016년07월01일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/108 (2013.01)
H04L 63/14 (2013.01)
(21) 출원번호 10-2015-7016876
(22) 출원일자(국제) 2015년04월30일
심사청구일자 2015년06월24일
(85) 번역문제출일자 2015년06월24일
(86) 국제출원번호 PCT/CN2015/078019
(87) 국제공개번호 WO 2016/082462
국제공개일자 2016년06월02일
(30) 우선권주장
201410708281.6 2014년11월27일 중국(CN)

(71) 출원인
시아오미 아이엔씨.
중국 베이징 하이단 디스트릭트 칭허 미들 스트리트, 엔오. 68, 레인보우 시티 쇼핑 몰 투 오브 차이나 리소시즈, 13층
(72) 발명자
장 화
중국 베이징 100085 하이단 디스트릭트 칭허 미들 스트리트 넘버 68 레인보우 시티 쇼핑 몰 투 오브 차이나 리소시즈 13층 시아오미 아이엔씨. 사내
시아 이
중국 베이징 100085 하이단 디스트릭트 칭허 미들 스트리트 넘버 68 레인보우 시티 쇼핑 몰 투 오브 차이나 리소시즈 13층 시아오미 아이엔씨. 사내
(뒷면에 계속)
(74) 대리인
박영복, 황영욱

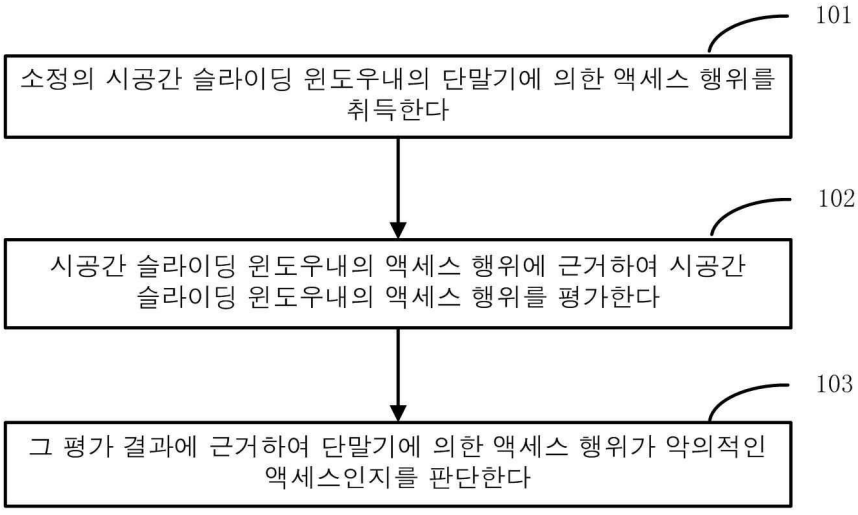
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **유저 행위 식별 방법 및 유저 행위 식별 장치, 프로그램 및 저장매체**

(57) 요 약

본 발명은 악의적인 행위를 보다 더 효과적으로 보다 더 정확하게 식별하기 위한 유저 행위 식별 방법 및 유저 행위 식별 장치에 관한것이다. 상기 방법은 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하는 스텝과,상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝과, 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝을 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 2463/121 (2013.01)
(72) 발명자
홍 띵쿤
중국 베이징 100085 하이단 디스트릭트 칭허 미들 스트리트 넘버 68 레인보우 시티 쇼핑 몰 투 오브 차이나 리소시즈 13층 시아오미 아이엔씨. 사내
왕 하이조우
중국 베이징 100085 하이단 디스트릭트 칭허 미들 스트리트 넘버 68 레인보우 시티 쇼핑 몰 투 오브 차이나 리소시즈 13층 시아오미 아이엔씨. 사내

명 세 서

청구범위

청구항 1

소정의 시공간 슬라이딩 윈도우(time sliding window)내의 단말기에 의한 액세스(access) 행위를 취득하는 스텝(step)과,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝과,

그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝

을 포함하는 것을 특징으로 하는 유저 행위 식별 방법.

청구항 2

제 1항에 있어서,

상기 시공간 슬라이딩 윈도우는 m개로 등분 된 타임 슬라이스(time slices)를 포함하고,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득하는 스텝과,

n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단하는 스텝

을 포함하고,

그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은

n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝을 포함하는 것을 특징으로 하는 유저 행위 식별 방법.

청구항 3

제1항에 있어서,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 스텝과,

취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 스텝과,

상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단하는 스텝

을 포함하고,

그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은

상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝을 포함하는 것을 특징으로 하는 유저 행위 식별 방법.

청구항 4

제1항에 있어서,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 스텝과,

취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 스텝과,

상기 시간 분산과 시간 간격의 평균치의 비율을 산출하는 스텝과,

상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단하는 스텝

을 포함하고,

그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은

상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝을 포함하는 것을 특징으로 하는 유저 행위 식별 방법.

청구항 5

제1항에 있어서,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득하는 스텝과,

상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단하는 스텝과,

그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝

을 포함하는 것을 특징으로 하는 유저 행위 식별 방법.

청구항 6

소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하기 위한 취득 모듈과,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하기 위한 평가 모듈과,

그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하기 위한 판단 모듈

을 포함하는 것을 특징으로 하는 유저 행위 식별 장치.

청구항 7

제6항에 있어서,

상기 시공간 슬라이딩 윈도우는 m개로 등분 된 타임 슬라이스를 포함하고,

상기 평가 모듈은

타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득하기 위한 타임 슬라이스 서브 모듈과,

n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단하기 위한 제1 비례 서브모듈

을 포함하고,

상기 판단 모듈은

n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 것을 특징으로 하는 유저 행위 식별 장치.

청구항 8

제6항에 있어서,

상기 평가 모듈은

상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하기 위한 간격 서브모듈과,

취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하기 위한 분산 서브모듈과,

상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단하기 위한 제1 평가 서브모듈

을 포함하고,

상기 판단 모듈은

상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 것을 특징으로 하는 유저 행위 식별 장치.

청구항 9

제6항에 있어서,

상기 평가 모듈은

상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하기 위한 간격 서브모듈과,

취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하기 위한 분산 서브모듈과,

상기 시간 분산과 시간 간격의 평균치의 비율을 산출하기 위한 비율 서브모듈과,

상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단하기 위한 제2 비례 서브모듈

을 포함하고,

상기 판단 모듈은

상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 것을 특징으로 하는 유저 행위 식별 장치.

청구항 10

제6항에 있어서,

상기 평가 모듈은

상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득하기 위한 총횟수 서브모듈과,

상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단하기 위한 총횟수 판단 서브모듈과,

그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하기 위한 제 2의 평가 서브모듈

을 포함하는 것을 특징으로 하는 유저 행위 식별 장치.

청구항 11

프로세서와,

프로세서에 의해 실행 가능한 인스트럭션을 저장하기 위한 메모리

를 포함하는 유저 행위 식별 장치에 있어서,

상기 프로세서는

소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하고,

상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하며,

그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하도록 구성되는 것을 특징으로 하는 유저 행위 식별 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 통신 및 컴퓨터 처리 기술 분야에 관한 것이며, 특히 유저 행위 식별 방법 및 유저 행위 식별 장치에 관한 것이다.

[0002] 본 출원은, 출원 번호가CN201410708281.6이며, 출원일이 2014월 11월 27일인 중국 특허 출원을 기초로 우선권을 주장하고, 당해 중국 특허 출원의 모든 내용을 본원에 원용한다.

배 경 기 술

[0003] 인터넷의 발전에 수반해 네트워크를 통한 자원 공유화가 실현되었다. 사람들은 네트워크를 통하여 풍부한 정보를 신속하고 편리하게 취득하는 것이 가능하게 되었다. 하지만, 많은 웹 사이트들이 사람들에게 정보를 제공하는 한편, 악의적인 공격등에 노출되고 있다.

[0004] 본 발명의 발명자는, 종래 기술에 있어서, 짧은 시간내에 웹 사이트에 데이터 패킷을 빈번히 송신하는 등 악의적인 공격 방식을 발견했다. 이러한 현상은 상품을 다투어 살 때 늘 발생하는 현상으로써, 짧은 시간 내에 빈번히 웹 사이트에 액세스 하여 할인 상품을 다투어 사는 현상이다. 이러한 고빈도의 액세스 행위는, 통상 상품을 다투어 사기 위하여 개발된 소프트웨어에 의해 실현되며, 수동 조작에 의해 높은 빈도의 액세스를 실현할 수 없다. 종래 기술에 있어서, 해당 악의적인 행위를 저지하는 수단이 없는 것은 아니지만, 그 저지 효과가 이상적이 못된다. 따라서, 어떻게 하면 악의적인 유저 행위를 보다 효과적으로 식별할 수 있는 지는 시급하게 해결해야 할 문제이다.

발명의 내용

해결하려는 과제

[0005] 본 발명은, 종래 기술에 존재하는 상기와 같은 문제를 해결하기 위하여 유저 행위 식별 방법 및 유저 행위 식별 장치를 제공한다.

과제의 해결 수단

[0006] 본 발명의 제1 양태에 따르면,

[0007] 소정의 시공간 슬라이딩 윈도우(time sliding window)내의 단말기에 의한 액세스(access) 행위를 취득하는 스텝과,

[0008] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝과,

[0009] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝을 포함하는 유저 행위 식별 방법을 제공한다.

발명의 효과

[0010] 본 발명의 실시예에 따른 기술방안에 의하면, 유저(user)의 액세스 행위를 시공간 슬라이딩 윈도우를 이용해 모니터링 하여 액세스 행위를 평가하는 것을 통하여 유저의 액세스 행위가 악의적인 것인지를 판단하는 유익한 효과를 얻을 수 있다.

[0011] 일 실시예에 있어서,

[0012] 상기 시공간 슬라이딩 윈도우는 m개로 등분 된 타임 슬라이스(time slice)를 포함하고,

[0013] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

[0014] 타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득하는 스텝과,

[0015] n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단하는 스텝

[0016] 을 포함하고,

[0017] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은

[0018] n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝을 포함한다.

[0019] 본 발명의 실시예에 따른 기술방안에 의하면, 각 타임 슬라이스내의 액세스 행위를 모니터링하여 액세스 횟수가 지속적으로 높은 수치를 검사하는 것을 통하여 액세스 행위가 악의적인 행위인지를 판단하므로, 그 평가 결과가 더욱 정확할 수 있다는 유익한 효과를 얻을 수 있다.

[0020] 일 실시예에 있어서,

[0021] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

[0022] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 스텝과,

[0023] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 스텝과,

[0024] 상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단하는 스텝

[0025] 을 포함하고,

[0026] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은

[0027] 상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝을 포함한다.

[0028] 본 발명의 실시예에 따른 기술방안에 의하면, 시간 간격의 분산을 산출하는 것을 통하여 액세스 행위가 고정된 빈도로 발생하는지 여부를 판단하고, 액세스 행위가 고정된 빈도로 발생하는 경우, 당해 액세스 행위가 유저에 의한 행위가 아니라 소프트웨어에 의한 행위라고 판단할 수 있으므로, 악의적인 행위를 더욱 정확하게 식별할 수 있다는 유익한 효과를 얻을 수 있다.

[0029] 일 실시예에 있어서,

[0030] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

[0031] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 스텝과,

[0032] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 스텝과,

[0033] 상기 시간 분산과 시간 간격의 평균치의 비율을 산출하는 스텝과,

[0034] 상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단하는 스텝

[0035] 을 포함하고,

[0036] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은

[0037] 상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝을 포함한다.

[0038] 본 발명의 실시예에 따른 기술방안에 의하면, 분산과 시간 간격의 평균치를 더 비교하는 것을 통하여 악의적인 행위를 더욱 정확하게 식별할 수 있다는 유익한 효과를 얻을 수 있다.

[0039] 일 실시예에 있어서,

[0040] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은

[0041] 상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득하는 스텝과,

[0042] 상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단하는 스텝과,

[0043] 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝을 포함한다.

[0044] 본 발명의 실시예에 따른 기술방안에 의하면, 상기 기술방안의 기초상에서 액세스 행위의 총횟수를 이용하여 액세스 행위를 더 한층 평가하는 것을 통하여 악의적인 행위를 더욱 정확하게 식별할 수 있다는 유익한 효과를 얻을 수 있다.

[0045] 본 발명의 제2 양태에 따르면,

[0046] 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하기 위한 취득 모듈과,

[0047] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하기 위한 평가 모듈과,

[0048] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하기 위한 판단 모듈을 포함하는 유저 행위 식별 장치를 제공한다.

[0049] 일 실시예에 있어서,

[0050] 상기 시공간 슬라이딩 윈도우는 m개로 등분 된 타임 슬라이스를 포함하고,

[0051] 상기 평가 모듈은

[0052] 타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득하기 위한 타임 슬라이스 서브모듈과,

[0053] n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단하기 위한 제1 비례 서브모듈

[0054] 을 포함하고,

[0055] 상기 판단 모듈은

[0056] n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0057] 일 실시예에 있어서,

[0058] 상기 평가 모듈은

[0059] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하기 위한 간격 서브모듈과,

[0060] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하기 위한 분산 서브모듈과,

[0061] 상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단하기 위한 제1 평가 서브모듈

[0062] 을 포함하고,

[0063] 상기 판단 모듈은

[0064] 상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0065] 일 실시예에 있어서,

[0066] 상기 평가 모듈은

[0067] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하기 위한 간격 서브모듈과,

[0068] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하기 위한 분산 서브모듈과,

[0069] 상기 시간 분산과 시간 간격의 평균치의 비율을 산출하기 위한 비율 서브모듈과,

[0070] 상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단하기 위한 제2 비례 서브모듈

[0071] 을 포함하고,

[0072] 상기 판단 모듈은

[0073] 상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0074] 일 실시예에 있어서,

[0075] 상기 평가 모듈은

[0076] 상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득하기 위한 총횟수 서브모듈과,

[0077] 상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단하기 위한 총횟수 판단 서브모듈과,

[0078] 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하기 위한 제 2의 평가 서브모듈을 포함한다.

[0079] 본 발명의 제3 양태에 따르면,

[0080] 프로세서와,

[0081] 프로세서에 의해 실행 가능한 인스트럭션을 저장하기 위한 메모리

[0082] 를 포함하는 유저 행위 식별 장치를 제공하고,

[0083] 상기 프로세서는

[0084] 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하고,

[0085] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하고,

[0086] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하도록 구성된다.

[0087] 이상의 일반적인 설명과 이하의 세부적인 설명은 예시적인 것으로서 본 발명에 대한 한정으로서 이해하여서는 아니 된다.

도면의 간단한 설명

[0088] 여기에 도시된 도면은, 명세서에 포함되어 명세서의 일부분을 구성하며 본 발명의 실시예에 대한 설명에 사용됨

과 동시에 본 발명의 원리를 해석하기 위하여 사용된다.

도 1은 예시적인 일 실시예에 따른 유저 행위 식별 방법의 흐름도이다.

도 2는 예시적인 일 실시예에 따른 유저 행위 식별 방법의 흐름도이다.

도 3은 예시적인 일 실시예에 따른 유저 행위 식별 방법의 흐름도이다.

도 4는 예시적인 일 실시예에 따른 유저 행위 식별 장치의 블럭도이다.

도 5는 예시적인 일 실시예에 따른 평가 모듈의 블럭도이다.

도 6 A는 예시적인 일 실시예에 따른 평가 모듈의 블럭도이다.

도 6 B는 예시적인 일 실시예에 따른 평가 모듈의 블럭도이다.

도 7은 예시적인 일 실시예에 따른 평가 모듈의 블럭도이다.

도 8은 예시적인 일 실시예에 따른 장치의 블럭도이다.

발명을 실시하기 위한 구체적인 내용

[0089] 이하, 도면을 참조하여 예시적인 실시예에 대해 상세하게 설명하기로 한다. 이하의 도면에 관한 설명에 있어서, 별도의 설명이 없는 이상, 서로 다른 도면상의 동일한 부호는 동일 또는 유사한 요소를 표시한다. 이하의 예시적 실시예에 대한 복수의 실시 형태는 본 발명과 관련되는 모든 실시 형태를 표시하는 것은 아니다. 이와 반대로, 이들은 첨부된 특허 청구의 범위에 기재되는 본 발명의 일부의 양태와 일치한 장치 및 방법의 예에 지나지 않는다.

[0090] 현재, 네트워크상에서의 이벤트가 빈번히 진행됨에 따라 인터넷 점포는 기간 한정의 할인 이벤트를 빈번히 개최하고 있다. 유저(user)는 저가격 상품을 사기 위하여 짧은 시간내에 해당 점포의 웹 사이트(Web site)에 빈번히 액세스(access) 한다. 일부의 유저는 상품을 다투어 사기 위하여 개발된 소프트웨어를 이용해 구입 행위를 실행한다. 상품을 다투어 사기 위하여 개발된 소프트웨어는, 일반 유저보다 높은 액세스 빈도로 점포의 웹 사이트를 액세스 할 수 있다. 그러나, 상품을 다투어 사기 위하여 개발된 소프트웨어에 의한 액세스 행위는 일종의 악의적인 행위로써 웹 사이트가 일시적으로 열람 불가 상태가 되게 할 수 있다. 하나의 가능한 해결안으로서, 소정 시간내의 액세스 횟수가 소정의 역치를 초과하는지 여부를 판단하여, 만약 초과 할 경우, 악의적인 액세스 행위가 존재한다고 판단한다. 하지만, 당해 식별 방법은 비교적 간단하여, 당해 액세스 횟수가 유저의 행위에 의한 것인지, 아니면 상품을 다투어 사기 위하여 개발된 소프트웨어에 의한 것인지를 정확하게 식별할 수 없으며 그 식별 결과가 정확하지 않다.

[0091] 본 실시예에서는, 이러한 문제를 해결하기 위하여, 단말기에 의한 액세스 행위를 시공간 슬라이딩 윈도우(time sliding window)에서 모니터링 하는 것을 통하여 단말기에 의한 액세스 행위가 악의적인 것인지를 정확하게 식별할 수 있다.

[0092] 본 실시예에 따른 시공간 슬라이딩 윈도우는 다이나믹 시공간 윈도우(dynamic time window)이고, 그 길이는 일정하며 예를 들면 3600초이다. 당해 시공간 슬라이딩 윈도우는 그 종료 위치가 항상 현재 시간이기에, 당해 시공간 슬라이딩 윈도우는 시간의 경과에 따라 이동한다.

[0093] 종래 기술중의 소정 시간 길이에 따라 액세스 횟수를 검출하는 기술방안으로서, 예를 들면, 소정 시간 길이가 1000초이며, 0~1000초 사이에 1회 검출하고, 1001~2000초 사이에 1회 검출하며, 그 이후는 마찬가지 방식으로 검출을 반복한다. 하지만, 이와 같은 경우, 500~1500초 사이에 발생하는 액세스 행위는 검출할 수 없다. 때문에, 본 실시예에서는, 시공간 슬라이딩 윈도우의 이동에 수반해 리얼타임으로 검출을 실시하도록 한다. 예를 들면, 시공간 슬라이딩 윈도우는 그 소정 시간 길이가 1000초이며, 0~1000초 사이에 1회 검출하고, 1~1001초 사이에 1회 검출하며, 2~1002초 사이에 1회 검출하고, 그 이후는 마찬가지 방식으로 검출을 반복한다. 본 실시예에서는, 종래 기술방안과 비교하여 그 검출 결과가 더욱 정확하고 악의적인 행위를 더욱 정확하게 식별할 수 있다.

[0094] 도 1은 예시적인 일 실시예에 따른 유저 행위 식별 방법의 흐름도이다. 당해 방법은 서버에 의해 실현되며, 도 1에 도시된 바와 같이 이하의 스텝을 포함한다.

[0095] 스텝 101에서는 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득한다.

[0096] 스텝 102에서는 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0097] 스텝 103에서는 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단한다.

[0098] 본 실시예에서는, 단말기에 의한 액세스 행위를 시공간 슬라이딩 윈도우내에서 리얼타임으로 모니터링 할 수 있고, 또한 일정 시간내의 액세스 행위를 모니터링 하여 액세스 행위가 악의적인지를 평가할 수 있으므로, 그 식별 결과가 더욱 정확하다. 본 실시예에서는, 단일 단말기의 행위에 대하여 모니터링 및 평가를 하고 있는데, 이 단말기는 유저명, IP(인터넷 프로토콜) 주소 또는 MAC(매체 액세스 제어) 주소등에 의해 확정할 수 있다.

[0099] 악의적인 액세스의 존재가 식별되면, 예를 들어 단말기에 검증 코드를 송신하도록 요구하고, 또는 당해 유저(또는 당해 단말기)에 의한 액세스를 일시적으로 차단하고, 또는 당해 유저를 블랙 리스트에 기입하여 당해 유저의 액세스를 영원히 거부하고, 또는 경고 메시지를 유저에게 송신하는 등 복수 종류의 수단을 채용할 수 있다.

[0100] 일 실시예에서, 스텝 102는 스텝 A로서 실현된다.

[0101] 스텝 A에서는, 상기 시공간 슬라이딩 윈도우중의 각 타임 슬라이스내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0102] 본 실시예에서는, 시공간 슬라이딩 윈도우를 동일 길이(등분)의 복수의 타임 슬라이스로 세분한다. 예를 들어, 시공간 슬라이딩 윈도우의 소정 시간 길이가 3600초이며, 10개의 타임 슬라이스를 포함한 경우, 각 타임 슬라이스의 시간 길이는 360초이다. 본 실시예에서는, 타임 슬라이스를 단위로 하여 유저의 액세스 행위를 모니터링 하는 것을 통하여 모니터링의 입도를 더욱 축소시킬 수 있어 악의적인 행위를 더욱 정확하게 식별할 수 있다. 또한, 본 실시예에서는, 각 타임 슬라이스내의 액세스 행위 및 시공간 슬라이딩 윈도우내의 전체 액세스 행위에 근거하여 평가를 실시하기 때문에 그 평가 결과가 더욱 정확하다.

[0103] 일 실시예에서, 스텝 A는 스텝 A1와 스텝 A2를 포함한다.

[0104] 스텝 A1에서, 각 타임 슬라이스에 대하여, 타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지 여부를 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득한다.

[0105] 스텝 A2에서, n와 타임 슬라이스 총수량 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단한다.

[0106] 스텝 103은 스텝 A3로서 실현될 수 있다.

[0107] 스텝 A3에서, n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0108] 즉, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 타임 슬라이스를 결정한다. 타임 슬라이스 총수량 중 슬라이스 횟수 역치를 초과하는 타임 슬라이스 수량의 비례가, 소정의 제1 비례 역치를 초과하는지 여부를 판단한다. 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0109] 본 실시예에서, 타임 슬라이스 총수량 중 슬라이스 횟수 역치를 초과하는 타임 슬라이스 수량의 비례가, 소정의 제1 비례 역치를 초과하는 경우, 액세스 횟수가 너무 높아 악의적인 액세스가 존재한다고 판단한다. 그렇지 아니한 경우, 악의적인 액세스가 존재하지 않는다고 판단한다.

[0110] 예를 들면, 시공간 슬라이딩 윈도우(T)가 3600초의 시간 길이를 가지고, 10개의 타임 슬라이스 t1~t10를 포함하는 경우, 각 타임 슬라이스의 길이는 360초이다. 그리고 10개의 타임 슬라이스에 대응하는 액세스 횟수는 각각 t1=50, t2=60, t3=52, t4=55, t5=48, t6=56, t7=58, t8=54, t9=56, t10=57이다. 슬라이스 횟수 역치가 50이라고 하면, 타임 슬라이스 t5를 제외한 다른 9개의 타임 슬라이스에 대한 액세스 횟수는 모두 슬라이스 횟수 역치를 초과한다. 슬라이스 횟수 역치를 초과하는 타임 슬라이스의 수량이 타임 슬라이스 총수량중에서 차지하는 비례는 9/10=90%로 산출된다. 제1 비례 역치가90%인 경우, 슬라이스 횟수 역치를 초과하는 타임 슬라이스의 수량이 타임 슬라이스 총수량중에서 차지하는 비례인 90%와 제1 비례 역치인90%를 비교하는 것을 통하여 액세스 행위를 평가하며, 당해 시공간 슬라이딩 윈도우(T)내에 악의적인 액세스 행위가 존재한다고 판단할 수 있다.

[0111] 일 실시예에서, 스텝 102는 기술방안 B에 의해서도 실현될 수 있다.

[0112] 기술방안 B 중,

[0113] 스텝 B1에서, 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득한다.

[0114] 스텝 B2에서, 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출한다.

[0115] 스텝 B3에서, 상기 시간 분산에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다. 여기서, 상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단한다.

[0116] 스텝 103에서, 상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0117] 본 실시예에서는, 시간 분산을 소정의 분산 역치와 비교하여, 소정의 분산 역치보다 큰 경우, 분산이 비교적 큰 것을, 즉 액세스 행위의 시간 간격의 변동이 비교적 큰 것을 나타내고 있으므로, 당해 액세스 행위가, 상품을 다투어 사기 위하여 개발된 소프트웨어에 의한 행위가 아니고, 유저에 의한 행위이라고 판단할 수 있고, 또한 악의적인 행위가 존재하지 않는다고 판단할 수 있다. 이와 반대로, 소정의 분산 역치 이하인 경우, 악의적인 행위가 존재한다고 판단한다.

[0118] 예를 들면, 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격 x1, x2, x3 … xn를 취득한다. 이 경우, 이하의 식에 의해 분산을 산출할 수 있다.

[0119] $$s^2 = \frac{1}{n}[(x1 - \bar{x})^2 + (x2 - \bar{x})^2 + \ldots (xn - \bar{x})^2]$$

$\bar{x}$

[0120] 여기서, $\bar{x}$ 는 x1~xn의 평균치이며, s는 산출하려고 하는 분산치이다.

[0121] 일 실시예에서, 기술방안 B는 스텝 A1~A3와 조합하여 실시 할 수 있다. 예를 들면, 각 타임 슬라이스에 대응하는 분산을 산출하여 분산이 분산 역치보다 큰 타임 슬라이스를 확정하고, 분산이 분산 역치보다 큰 타임 슬라이스의 수량과 타임 슬라이스 총수량의 비례를 결정한 후 당해 비례를 제1 비례 역치와 비교하여, 악의적인 액세스가 존재하는지를 판단한다.

[0122] 일 실시예에서, 기술방안 B를 더 개량할 수 있다. 스텝 B3는 스텝 B31 및 B32를 포함할 수 있다.

[0123] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득한다.

[0124] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출한다.

[0125] 스텝 B31에서, 상기 시간 분산과 시간 간격의 평균치의 비율을 산출한다.

[0126] 스텝 B32에서, 상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단한다. 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0127] 스텝 103은 스텝 B33로서 실현된다.

[0128] 스텝 B33에서, 상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0129] 본 실시예에서, 시간 분산과 시간 간격의 평균치의 비율이 소정의 제2 비례 역치를 초과하면, 당해 시간 분산을 가지는 시간 간격은 시간 간격의 평균치에 매우 접근하는 값이기에, 당해 액세스 행위가 상품을 다투어 사기 위하여 개발된 소프트웨어에 의한 행위이며, 악의적인 액세스가 존재한다고 판단할 수 있다. 그렇지 아니한 경우, 당해 액세스 행위는 유저에 의한 행위이며, 악의적인 액세스가 존재하지 않는다고 판단할 수 있다.

[0130] 예를 들면, 평균치 x가 1이며, 시간 분산이 0.5인 경우, 시간 분산과 평균치의 비례는50%이며, 소정의 제2 비례 역치100%보다 크다. 분산 0.5는 비교적 작기는 하지만 평균치 1에서 부터 떨어져 있는 정도가 비교적 크다.

[0131] 또 예를 들면, 평균치 x가 10이며, 시간 분산이 0.5인 경우, 시간 분산과 평균치의 비례는5%이며, 소정의 제2 비례 역치10%보다 작다. 평균치 10이 비교적 크기 때문에, 시간 분산 0.5를 가지는 시간 간격은 평균치에 매우 접근하는 수치이다.

[0132] 본 실시예에서, 분산과 평균치의 접근 정도(다른 면에서 보면, 떨어져 있는 정도라고도 할 수 있다)를 비교하는 것을 통하여 액세스 행위를 더욱 정확하게 평가할 수 있다.

[0133] 일 실시예에서, 스텝 102는 기술방안 C로서 실현될 수 있다.

[0134] 기술방안 C 중,

[0135] 스텝 C1에서, 상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득한다.

[0136] 스텝 C2에서, 상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단한다.

[0137] 스텝 C3에서, 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0138] 본 실시예에서는, 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수가 총횟수 역치를 초과하면, 액세스량이 너무 많아 악의적인 액세스가 존재한다고 판단한다. 그렇지 아니한 경우, 악의적인 액세스가 존재하지 않는다고 판단한다.

[0139] 일 실시예에서, 기술방안 C는 상기의 기술방안과 조합하여 실시할 수 있다. 스텝 A 또는 기술방안 B의 판단 결과의 기초 상에서, 기술방안 C의 판단을 실행하여, 각 기술방안의 판단결과 모두가 악의적인 액세스가 존재한다고 판단되었을 경우에만 악의적인 액세스가 존재한다는 결론을 내릴 수 있다.

[0140] 이하, 몇개의 실시예를 통해서 유저 행위 식별 방법을 소개하도록 한다.

[0141] 도 2는 예시적인 일 실시예에 따른 유저 행위 식별 방법의 흐름도이다. 당해 방법은 서버에 의해 실현되며, 도 2에 되시된 바와 같이 이하의 스텝을 포함한다.

[0142] 스텝 201에서, 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득한다.

[0143] 스텝 202에서, 시공간 슬라이딩 윈도우중의 타임 슬라이스마다, 타임 슬라이스에 대응하는 액세스 횟수를 소정의 슬라이스 횟수 역치와 비교한다.

[0144] 스텝 203에서, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 타임 슬라이스를 결정한다.

[0145] 스텝 204에서, 슬라이스 횟수 역치를 초과하는 타임 슬라이스의 수량이 타임 슬라이스 총수량에서 차지하는 비례를 산출한다.

[0146] 스텝 205에서, 산출된 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단한다. 소정의 제1 비례 역치를 초과하는 경우, 스텝 206으로 이동하고, 소정의 제1 비례 역치를 초과하지 않는 경우, 스텝 207으로 이동한다.

[0147] 스텝 206에서, 악의적인 액세스가 존재한다고 판단한다.

[0148] 스텝 207에서, 악의적인 액세스가 존재하지 않는다고 판단한다.

[0149] 본 실시예에서는, 타임 슬라이스를 이용해 액세스 행위를 보다 세부적으로 모니터링 할 수 있다. 액세스 횟수를 작은 입도로 모니터링 하는 것을 통하여 악의적인 액세스가 존재하는 지를 더욱 정확하게 식별할 수 있다.

[0150] 도 3은 예시적인 일 실시예에 따른 유저 행위 식별 방법의 흐름도이다. 당해 방법은 서버에 의해 실현되며, 도 3에 되시된 바와 같이 이하의 스텝을 포함한다.

[0151] 스텝 301에서, 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득한다.

[0152] 스텝 302에서, 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득한다.

[0153] 스텝 303에서, 취득한 시간 간격에 근거하여 시간 간격의 평균치를 산출한다.

[0154] 스텝 304에서, 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출한다.

[0155] 스텝 305에서, 상기 시간 분산과 시간 간격의 평균치의 비율을 산출한다.

[0156] 스텝 306에서, 상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단한다. 소정의 제2 비례 역치보다 작은 경우, 스텝 307으로 이동하고, 소정의 제2 비례 역치 이상인 경우, 스텝 308으로 이동한다.

[0157] 스텝 307에서, 악의적인 액세스가 존재한다고 판단한다.

[0158] 스텝 308에서, 악의적인 액세스가 존재하지 않는다고 판단한다.

[0159] 본 실시예에서는, 분산을 이용하여 취득한 액세스 행위가 균일한 시간 간격으로 발생하였는지 여부를 판단한다. 그러한 경우, 유저에 의한 액세스 행위가 아니라 소프트웨어에 의한 액세스 행위라고 판단하며, 악의적인 액세스가 존재한다고 판단한다. 그렇지 아니한 경우, 악의적인 액세스가 존재하지 않는다고 판단한다. 당해 방법에 의하면, 악의적인 액세스 행위를 더욱 정확하게 식별할 수 있다.

[0160] 이상의 설명에 의하여 서버에 의해 실현되는 유저 행위 식별 방법이 보다 더욱 명확하게 이해할수 있게 되었다. 이하, 장치의 내부 구조와 기능에 대해 소개하도록 한다.

[0161] 도 4는 예시적인 일 실시예에 따른 유저 행위 식별 장치의 모식도이다. 도 4를 참조하면, 해당 장치는 취득 모듈(401), 평가 모듈(402) 및 판단 모듈(403)을 포함한다.

[0162] 취득 모듈(401)은 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득한다.

[0163] 평가 모듈(402)은 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0164] 판단 모듈(403)은 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단한다.

[0165] 일 실시예에서, 상기 시공간 슬라이딩 윈도우는 m개로 등분 된 타임 슬라이스를 포함한다. 도 5에 되시된 바와 같이, 상기 평가 모듈(402)은 타임 슬라이스 서브모듈(4021)과 제1 비례 서브모듈(4028)을 포함한다.

[0166] 타임 슬라이스 서브모듈(4021)은 타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득한다.

[0167] 제1 비례 서브모듈(4028)은 n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단한다.

[0168] 상기 판단 모듈(403)은 n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0169] 일 실시예에서, 도 6 A에 되시된 바와 같이, 상기 평가 모듈(402)은 간격 서브모듈(4022), 분산 서브모듈(4023) 및 제1 평가 서브모듈(4024)을 포함한다.

[0170] 간격 서브모듈(4022)은, 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득한다.

[0171] 분산 서브모듈(4023)은 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출한다.

[0172] 제1 평가 서브모듈(4024)은 상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단한다.

[0173] 상기 판단 모듈(403)은 상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0174] 일 실시예에서, 타임 슬라이스 서브모듈(4021)은 간격 서브모듈(4022), 분산 서브모듈(4023) 및 제1 평가 서브모듈(4024)을 포함할 수도 있다.

[0175] 일 실시예에서, 도 6 B에 되시된 바와 같이, 상기 평가 모듈(402)은 간격 서브모듈(4022), 분산 서브모듈(4023), 비율 서브모듈(4029)및 제2 비례 서브모듈(40210)을 포함한다.

[0176] 간격 서브모듈(4022)은 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득한다.

[0177] 분산 서브모듈(4023)은 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출한다.

[0178] 비율 서브모듈(4029)는 상기 시간 분산과 시간 간격의 평균치의 비율을 산출한다.

[0179] 제2 비례 서브모듈(40210)는 상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단한다.

[0180] 상기 판단 모듈(403)은 상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단한다.

[0181] 일 실시예에서, 도 7에 되시된 바와 같이, 상기 평가 모듈(402)은 총횟수 서브모듈(4025), 총횟수 판단 서브모듈(4026) 및 제2 평가 서브모듈(4027)을 포함한다.

[0182] 총횟수 서브모듈(4025)은 상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득한다.

[0183] 총횟수 판단 서브모듈(4026)은 상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단한다.

[0184] 제2 평가 서브모듈(4027)은 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가한다.

[0185] 상기 실시예에 따른 장치의 각 모듈에 의한 조작의 구체적인 형태에 관하여, 유저 행위 식별 방법에 관한 실시예에 대해 이미 상세하게 설명하고 있기에, 여기에서는 그 상세한 설명을 생략 하도록 한다.

[0186] 도 8은 예시적인 일 실시예에 따른 유저 행위를 식별하기 위한 장치(800)의 블럭도이다. 예를 들면, 장치(800)는 컴퓨터로 제공될 수 있다. 도 8을 참조하면, 장치(800)는 1개 또는 복수의 프로세서를 포함하는 처리 어셈블리(822)와, 처리 어셈블리(822)에 의해 실행 가능한 예를 들면 응용 프로그램등과 같은 인스트럭션을 저장하기 위한 메모리(832)를 대표로 하는 메모리 자원을 포함한다. 메모리(832)에 저장되는 응용 프로그램은 각각 1셋트의 인스트럭션에 대응하는 1개 또는 복수의 모듈을 포함할 수 있다. 또한, 처리 어셈블리(822)는 인스트럭션을 실행할 수 있도록 구성되어, 상기의 유저 행위 식별 방법을 수행할 수 있다.

[0187] 장치(800)는 장치(800)의 전원 관리를 수행하도록 구성되는 전원 어셈블리(826), 장치(800)을 네트워크에 접속시키기 위한 1개의 유선 또는 무선 네트워크 인터페이스(850), 1개의 입출력(I/O) 인터페이스(858)를 포함할 수 있다. 장치(800)는, 예를 들어 Windows ServerTM, Mac OS XTM, UnixTM, LinuxTM, FreeBSDTM 또는 이에 유사한 오퍼레이팅 시스템과 같은 메모리(832)에 저장된 오퍼레이팅 시스템을 구비할 수 있다.

[0188] 프로세서와 프로세서에 의해 실행 가능한 인스트럭션을 저장하기 위한 메모리를 포함하는 유저 행위 식별 장치에 있어서,

[0189] 상기 프로세서는,

[0190] 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하고,

[0191] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하고,

[0192] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하도록 구성된다.

[0193] 상기 프로세서는,

[0194] 상기 시공간 슬라이딩 윈도우가 m개로 등분 된 타임 슬라이스를 포함하고,

[0195] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 것이,

[0196] 타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스 취득하는 것과,

[0197] n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단하는 것

[0198] 을 포함하고,

[0199] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 것이,

[0200] n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 것

[0201] 을 포함하도록 구성될 수 있다.

[0202] 또한, 상기 프로세서는,

[0203] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 것이,

[0204] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의

시간 간격을 취득하는 것과,

[0205] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 것과,

[0206] 상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단하는 것

[0207] 을 포함하고,

[0208] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 것이,

[0209] 상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 것

[0210] 을 포함하도록 구성될 수 있다.

[0211] 상기 프로세서는,

[0212] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 것이,

[0213] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 것과,

[0214] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 것과,

[0215] 상기 시간 분산과 시간 간격의 평균치의 비율을 산출하는 것과,

[0216] 상기 비율이 소정의 제2 비례 역치보다 작은가 아닌가를 판단하는 것

[0217] 을 포함하고,

[0218] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 것이,

[0219] 상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 것

[0220] 을 포함하도록 구성될 수 있다.

[0221] 또한, 상기 프로세서는,

[0222] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 것이,

[0223] 상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득하는 것과,

[0224] 상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단하는 것과,

[0225] 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 것

[0226] 을 포함하도록 구성될 수 있다.

[0227] 컴퓨터에 의해 판독 가능한 비휘발성 기록 매체에 있어서, 상기 기록 매체중의 인스트럭션이 이동 단말기의 프로세서에 의해 실행되는 경우, 이동 단말기가 유저 행위 식별 방법을 실행할 수 있다.

[0228] 상기 유저 행위 식별 방법은,

[0229] 소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득하는 스텝과,

[0230] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝과,

[0231] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝

[0232] 을 포함한다.

[0233] 상기 기록 매체중의 인스트럭션은,

[0234] 상기 시공간 슬라이딩 윈도우가 m개로 등분 된 타임 슬라이스를 포함하고,

[0235] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은,

[0236] 타임 슬라이스내의 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는지를 타임 슬라이스마다 판단하여, 액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 n개의 타임 슬라이스를 취득하는 스텝과,

[0237] n와 m의 비례가 소정의 제1 비례 역치를 초과하는지 여부를 판단하는 스텝

[0238] 을 포함하고,

[0239] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은,

[0240] n와 m의 비례가 소정의 제1 비례 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝

[0241] 을 포함하도록 구성될수 있다.

[0242] 또한, 상기 기록 매체중의 인스트럭션은,

[0243] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은,

[0244] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 스텝과,

[0245] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 스텝과,

[0246] 상기 시간 분산이 소정의 분산 역치를 초과하는지 여부를 판단하는 스텝

[0247] 을 포함하고,

[0248] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은,

[0249] 상기 시간 분산이 소정의 분산 역치를 초과하는 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝

[0250] 을 포함하도록 구성될 수 있다.

[0251] 상기 기록 매체중의 인스트럭션은,

[0252] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은,

[0253] 상기 시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득하는 스텝과,

[0254] 취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출하는 스텝과,

[0255] 상기 시간 분산과 시간 간격의 평균치의 비율을 산출하는 스텝과,

[0256] 상기 비율이 소정의 제2 비례 역치보다 작은지 여부를 판단하는 스텝

[0257] 을 포함하고,

[0258] 그 평가 결과에 근거하여 상기 단말기에 의한 액세스 행위가 악의적인 액세스인지를 판단하는 스텝은,

[0259] 상기 비율이 소정의 제2 비례 역치보다 작은 경우, 상기 단말기에 의한 액세스 행위가 악의적인 액세스라고 판단하는 스텝

[0260] 을 포함하도록 구성될 수 있다.

[0261] 또한, 상기 기록 매체중의 인스트럭션은,

[0262] 상기 시공간 슬라이딩 윈도우내의 액세스 행위에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝은,

[0263] 상기 시공간 슬라이딩 윈도우내의 액세스 행위의 총횟수를 취득하는 스텝과,

[0264] 상기 총횟수가 소정의 총횟수 역치를 초과하는지 여부를 판단하는 스텝과,

[0265] 그 판단 결과에 근거하여 상기 시공간 슬라이딩 윈도우내의 액세스 행위를 평가하는 스텝

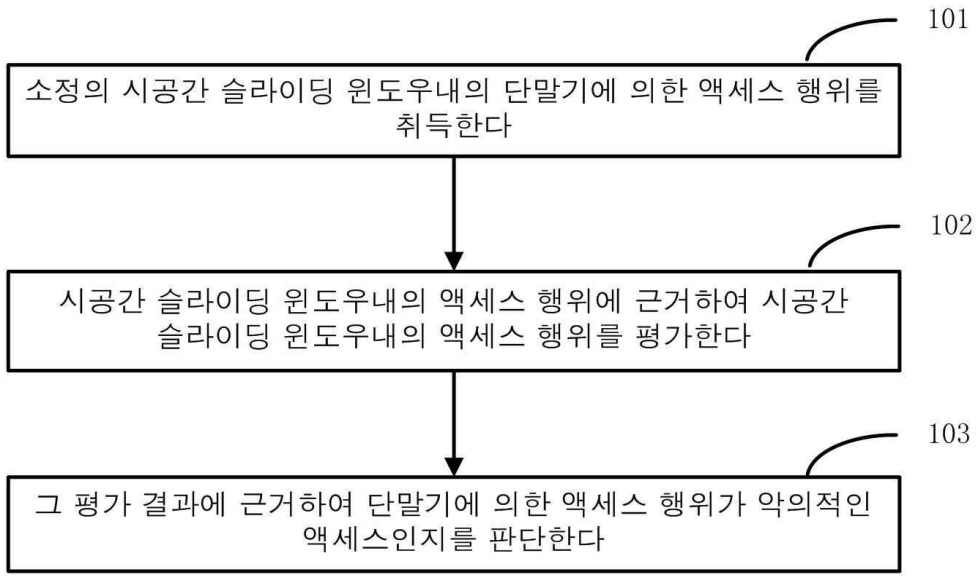
[0266] 을 포함하도록 구성될 수 있다.

[0267] 당업자는 명세서를 참조하고 또한 여기서 공개한 발명을 실행한 후, 본 발명의 다른 실시방안을 용이하게 생각해낼 수 있다. 본출원은, 본 발명의 임의의 변형, 용도 또는 적응적 변화를 포함하고, 이러한 변형, 용도 또는 적응적 변화는, 본 발명의 일반적인 원리에 따르며, 본 명세서에서 공개하지 않은 본 기술분야의 공지상식 또는 관용기술수단을 포함한다. 명세서와 실시예는, 단지 예시적인 것으로서, 본 발명의 보호범위와 취지는 특허청구범위에 의해 한정된다.

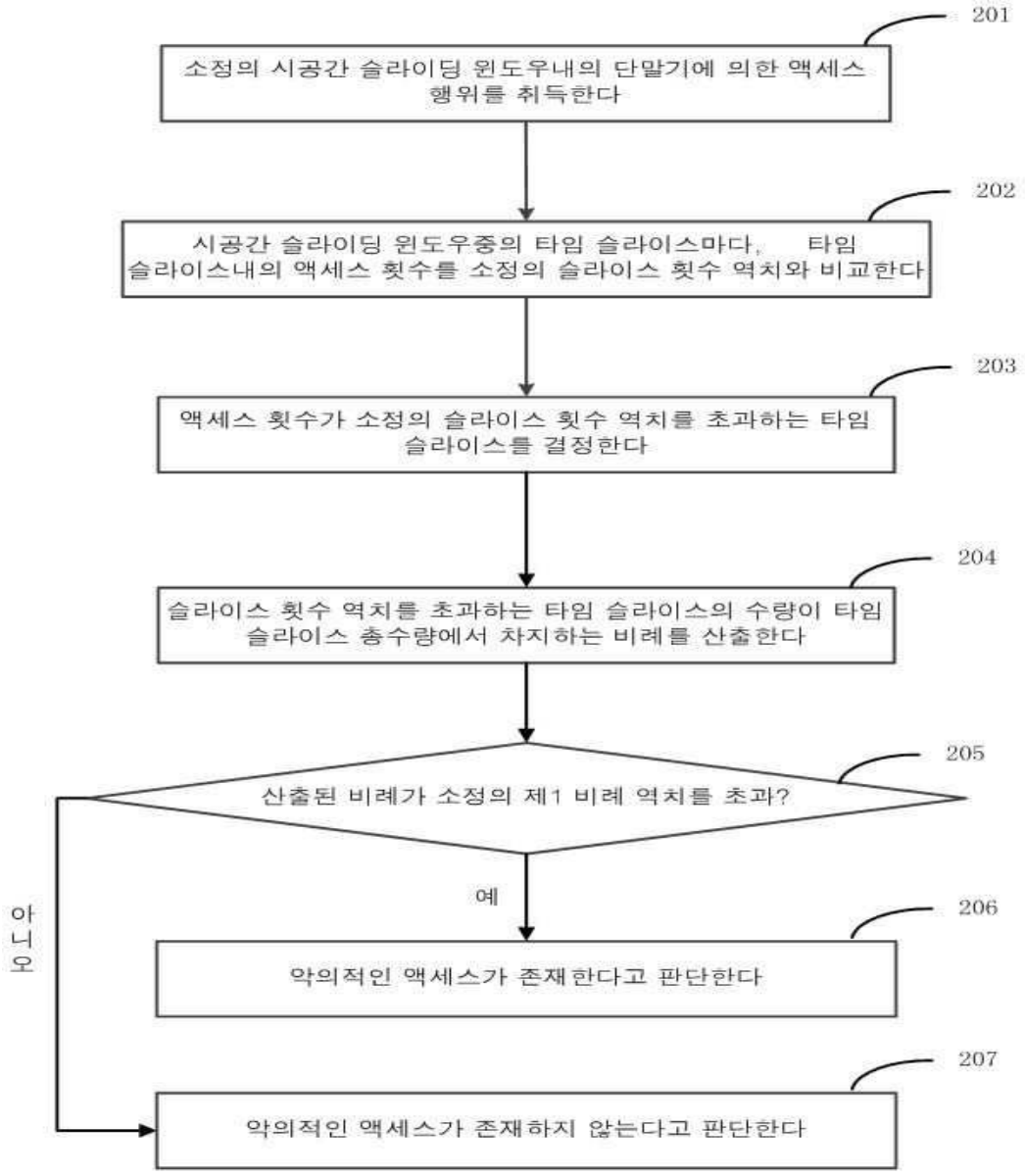
[0268] 본 발명은, 상기에 기재되고 도면에 나타낸 구체적인 구조에 한정되지 않으며, 그 범위내에서 다양한 수정과 변형을 실시할 수 있다는것을 이해해야 한다. 본 발명의 범위는 특허청구범위에 의해 제한된다.

도면

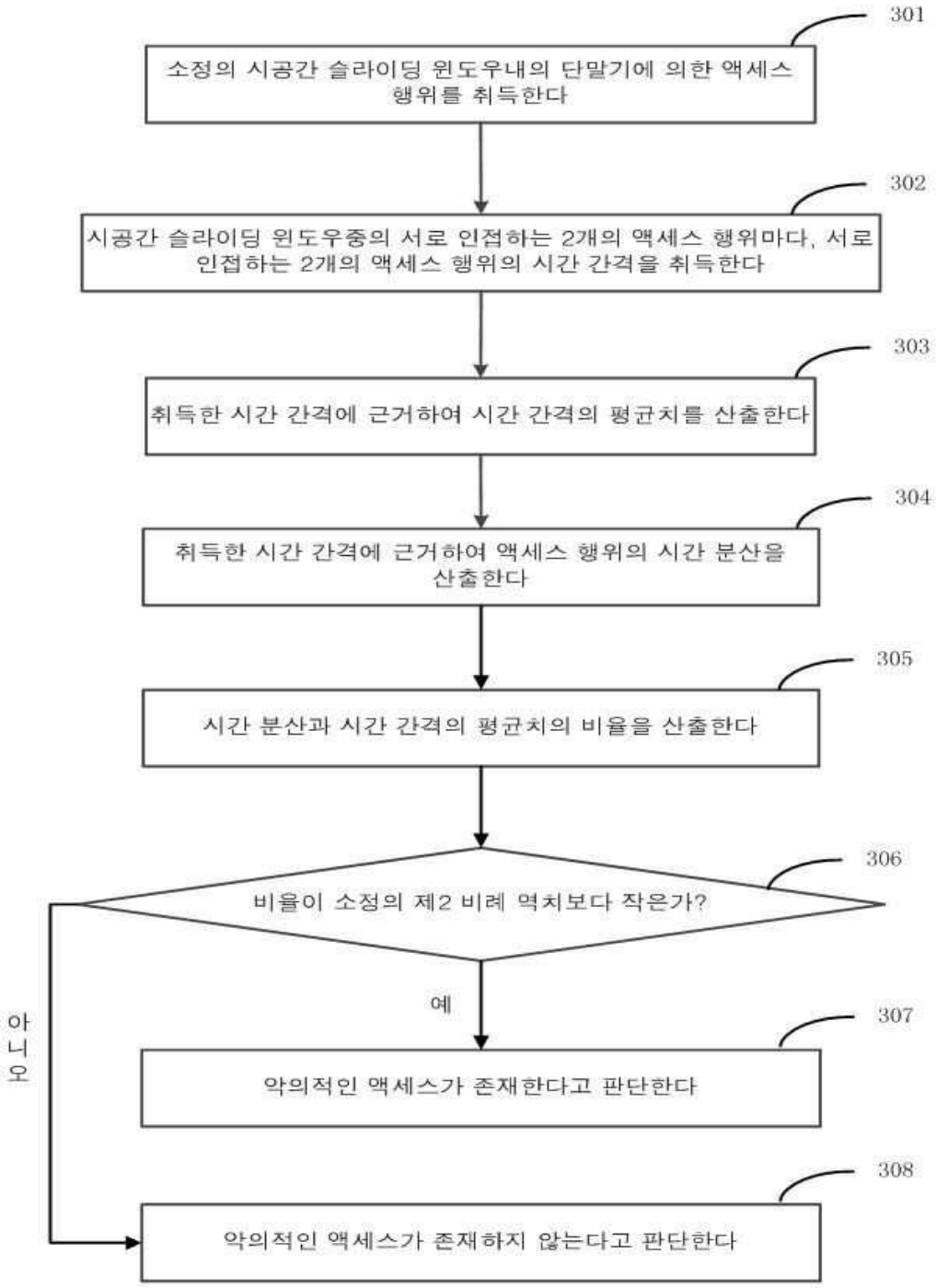
도면1



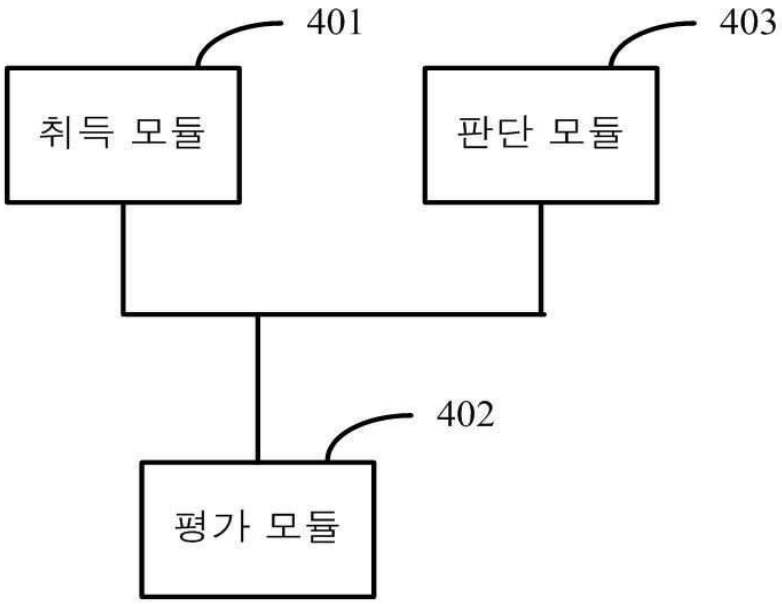
도면2


201
소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득한다
202
시공간 슬라이딩 윈도우중의 타임 슬라이스마다, 타임 슬라이스내의 액세스 횟수를 소정의 슬라이스 횟수 역치와 비교한다
203
액세스 횟수가 소정의 슬라이스 횟수 역치를 초과하는 타임 슬라이스를 결정한다
204
슬라이스 횟수 역치를 초과하는 타임 슬라이스의 수량이 타임 슬라이스 총수량에서 차지하는 비례를 산출한다
205
산출된 비례가 소정의 제1 비례 역치를 초과?
예
아니오
206
악의적인 액세스가 존재한다고 판단한다
207
악의적인 액세스가 존재하지 않는다고 판단한다

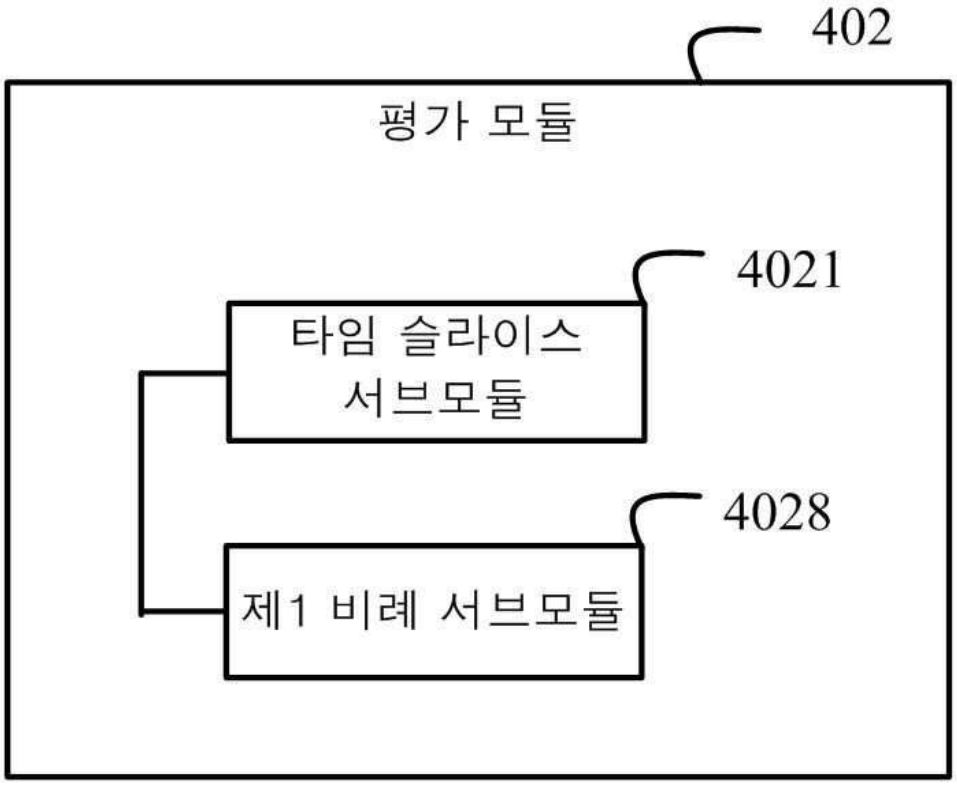
도면3


301
소정의 시공간 슬라이딩 윈도우내의 단말기에 의한 액세스 행위를 취득한다
302
시공간 슬라이딩 윈도우중의 서로 인접하는 2개의 액세스 행위마다, 서로 인접하는 2개의 액세스 행위의 시간 간격을 취득한다
303
취득한 시간 간격에 근거하여 시간 간격의 평균치를 산출한다
304
취득한 시간 간격에 근거하여 액세스 행위의 시간 분산을 산출한다
305
시간 분산과 시간 간격의 평균치의 비율을 산출한다
306
비율이 소정의 제2 비례 역치보다 작은가?
예
아니오
307
악의적인 액세스가 존재한다고 판단한다
308
악의적인 액세스가 존재하지 않는다고 판단한다

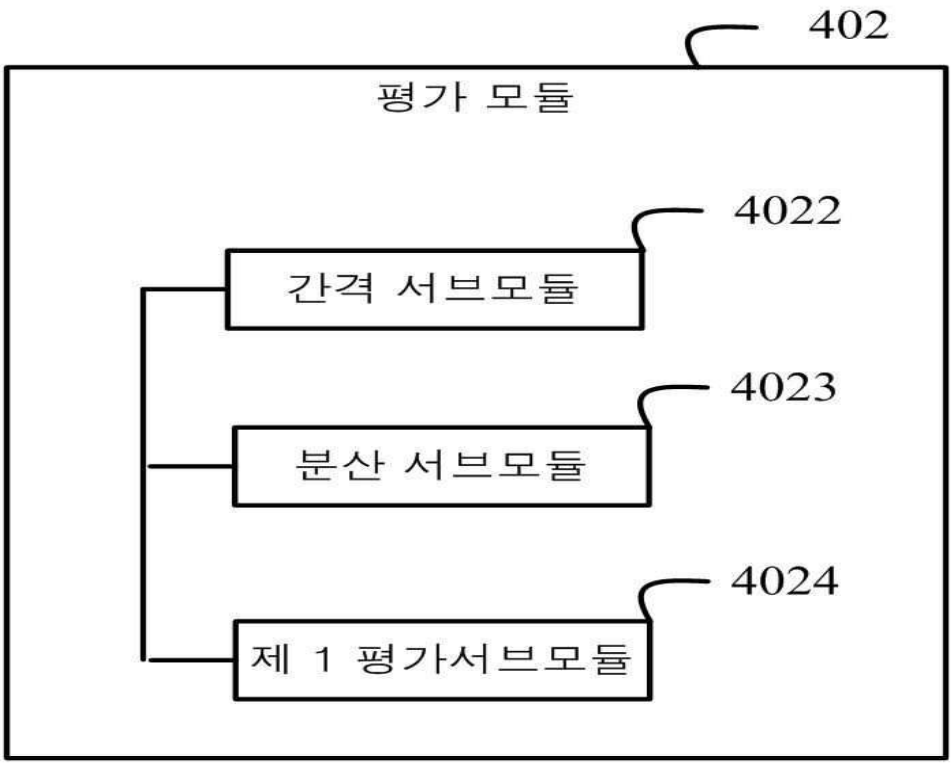
도면4


401
403
취득 모듈
판단 모듈
402
평가 모듈

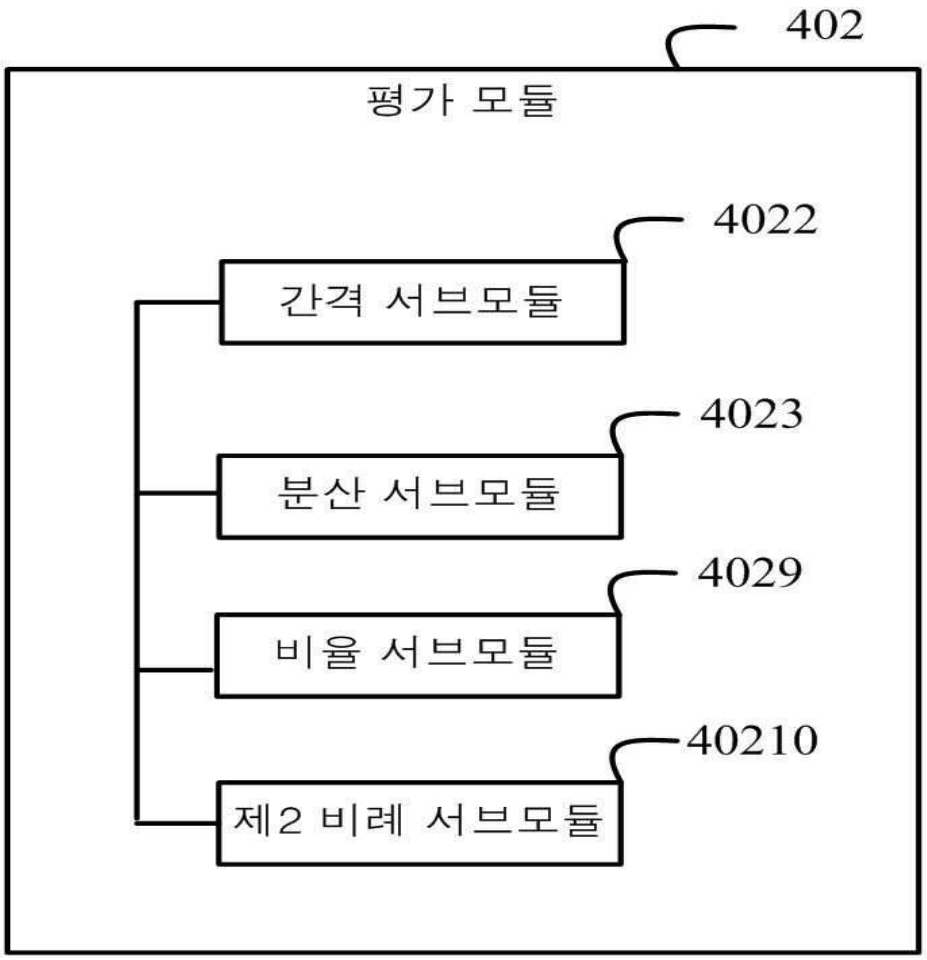
도면5


402
평가 모듈
4021
타임 슬라이스
서브모듈
4028
제1 비례 서브모듈

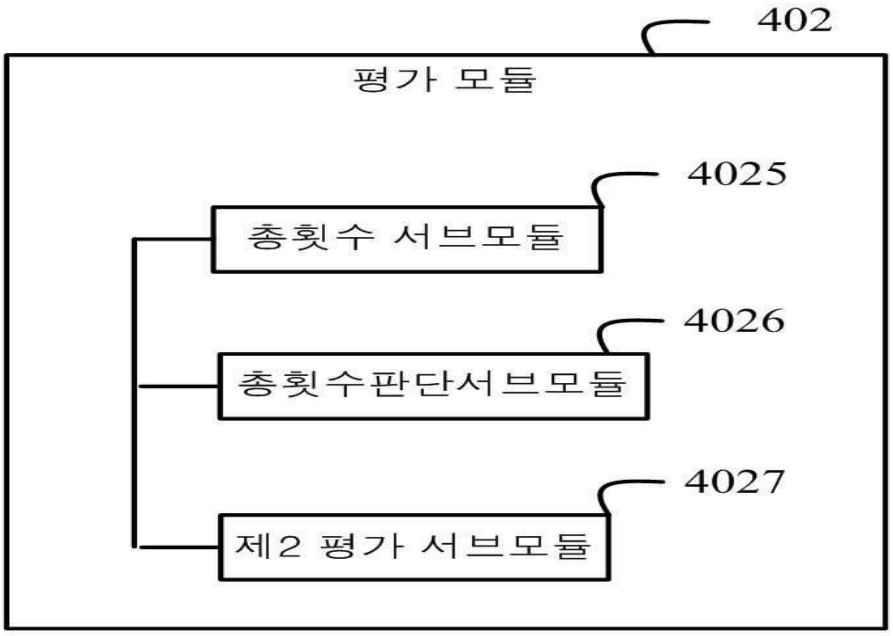
도면6a



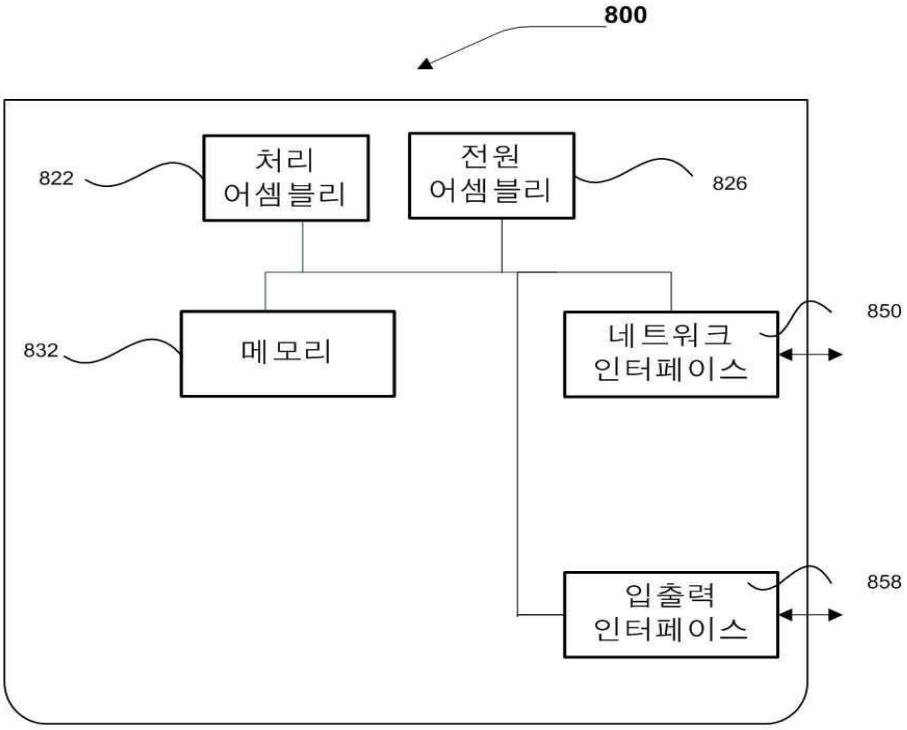
도면6b


402
평가 모듈
4022
간격 서브모듈
4023
분산 서브모듈
4029
비율 서브모듈
40210
제2 비례 서브모듈

도면7


402
평가 모듈
4025
총횟수 서브모듈
4026
총횟수판단서브모듈
4027
제2 평가 서브모듈

도면8


800
822
처리
어셈블리
전원
어셈블리
826
832
메모리
네트워크
인터페이스
850
입출력
인터페이스
858