특허증

CERTIFICATE OF PATENT

특 허 Patent Number	제 10-2906043 호
출원번호 Application Number	제 10-2025-0040842 호
출원일 Filing Date	2025년 03월 31일
등록일 Registration Date	2025년 12월 24일

발명의 명칭 Title of the Invention

위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션 제공 방법

특허권자 Patentee

주식회사 퓨즈에이엑스(110111-*****)**
서울특별시 강남구 역삼로17길 37, 3층 (역삼동)

발명자 Inventor

허재남(721108-*****)**
서울특별시 서초구 방배천로18길 11 롯데캐슬아르떼 110동1203호

위의 발명은 「특허법」에 따라 특허원부에 등록되었음을 증명합니다.

This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Ministry of Intellectual Property.

지식재산처
Ministry of
Intellectual Property

2025년 12월 24일

QR코드로 현재기준
등록사항을 확인하세요

지식재산처장
MINISTER,
MINISTRY OF INTELLECTUAL PROPERTY

지식재산처장의인

김 용 선

(19) 대한민국 지식재산처(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2026년01월02일
(11) 등록번호 10-2906043
(24) 등록일자 2025년12월24일

(51) 국제특허분류(Int. Cl.)
G08B 21/02 (2006.01) *G06T 5/30* (2006.01)
G06T 5/70 (2024.01) *G06V 10/75* (2022.01)
G06V 10/82 (2022.01) *G06V 20/52* (2022.01)
G06V 40/20 (2022.01) *G08B 21/18* (2006.01)
G08B 25/14 (2006.01) *G10L 25/48* (2013.01)
H04W 4/02 (2018.01)
(52) CPC특허분류
G08B 21/02 (2013.01)
G06T 5/30 (2013.01)
(21) 출원번호 10-2025-0040842
(22) 출원일자 2025년03월31일
심사청구일자 2025년03월31일
(56) 선행기술조사문헌
KR1020210129842 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 퓨즈에이엑스
서울특별시 강남구 역삼로17길 37, 3층 (역삼동)
(72) 발명자
허재남
서울특별시 서초구 방배천로18길 11 롯데캐슬아르떼 110동1203호
(74) 대리인
전정욱

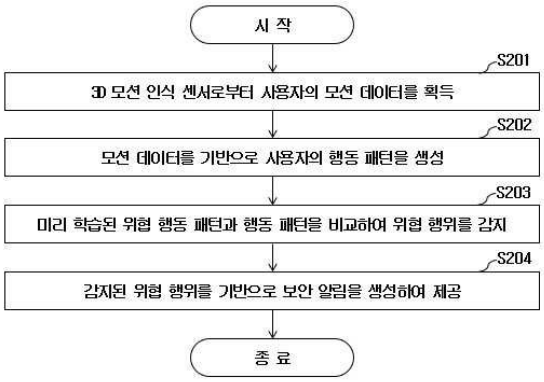
전체 청구항 수 : 총 2 항 심사관 : 김대환

(54) 발명의 명칭 **위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션 제공 방법**

(57) 요 약

일실시예에 따른 장치는 3D 모션 인식 센서로부터 사용자 모션 데이터를 획득하고, 이를 기반으로 사용자 행동 패턴을 생성한 후, 미리 학습된 위협 행동 패턴과 비교하여 위협 행위를 감지하고, 감지된 위협 행위를 기반으로 보안 알림을 생성하여 제공할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
G06T 5/70 (2024.01)
G06V 10/75 (2023.08)
G06V 10/82 (2022.01)
G06V 20/52 (2023.08)
G06V 40/20 (2022.01)
G08B 21/182 (2013.01)
G08B 25/14 (2013.01)
G10L 25/48 (2013.01)
H04W 4/02 (2020.05)

명 세 서

청구범위

청구항 1

장치에 의해 수행되는 방법에 있어서,

3D 모션 인식 센서로부터 사용자의 모션 데이터를 획득하는 단계;

상기 모션 데이터를 기반으로 사용자의 행동 패턴을 생성하는 단계;

미리 학습된 위협 행동 패턴과 상기 행동 패턴을 비교하여 위협 행위를 감지하는 단계; 및

상기 감지된 위협 행위를 기반으로 보안 알림을 생성하여 제공하는 단계를 포함하고,

상기 보안 알림을 생성하여 제공하는 단계는,

상기 위협 행위가 감지된 환경에서 상기 행동 패턴으로부터 사용자의 움직임 속도, 방향성, 반복성, 가속도 및 자세 변화를 분석하여 위험 지수를 산출하는 단계,

상기 위험 지수가 미리 설정된 기준 이상인 경우, 해당 사용자를 주요 사용자로 분류하고, 상기 위험 지수가 미리 설정된 기준 미만인 경우, 해당 사용자를 주변 사용자로 분류하는 단계,

사용자를 위협 행위를 가한 가해자 및 위협을 당한 피해자로 분류하도록 미리 학습된 인공지능 모델에 상기 주요 사용자의 행동 패턴을 입력하여 상기 주요 사용자를 상기 가해자 및 피해자로 분류하는 단계,

상기 주변 사용자의 시선 데이터, 음성 데이터 및 행동 패턴을 분석하여 상기 주요 사용자에 대한 관심도를 산출하는 단계,

상기 가해자에 대한 관심도가 상기 피해자에 대한 관심도 미만인 경우, 상기 위험 지수에 따라 미리 설정된 기본 알림 범위를 확인하는 단계,

상기 가해자에 대한 관심도가 상기 피해자에 대한 관심도 이상이면서, 상기 피해자에 대한 관심도가 감소하는 경우, 상기 기본 알림 범위에 상기 피해자에 대한 관심도에 따른 감소 가중치를 적용하여 알림 범위를 결정하는 단계,

상기 가해자에 대한 관심도가 상기 피해자에 대한 관심도 이상이면서, 상기 피해자에 대한 관심도가 증가하는 경우, 상기 기본 알림 범위에 상기 피해자에 대한 관심도에 따른 증가 가중치를 적용하여 알림 범위를 결정하는 단계,

상기 사용자의 단말로부터 연락처 정보 및 현재 위치 정보를 획득하는 단계,

상기 연락처 정보 및 상기 현재 위치 정보로부터 상기 결정된 알림 범위에 따라 비상 연락처를 추출하는 단계,

상기 가해자에 대한 관심도와 상기 피해자에 대한 관심도의 차이가 미리 설정된 기준 이상인 경우, 상기 가해자와 관련된 순으로 알림 순서를 결정하는 단계,

상기 가해자에 대한 관심도와 상기 피해자에 대한 관심도의 차이가 미리 설정된 기준 미만인 경우, 상기 피해자와 관련된 순으로 알림 순서를 결정하는 단계, 및

상기 알림 범위 및 알림 순서에 따라 보안 알림을 생성하여 제공하는 단계를 포함하는,

위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션 제공 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 위협 행위가 감지된 환경의 모니터링 영상을 제공하는 단계를 더 포함하고,

상기 모니터링 영상을 제공하는 단계는,

상기 위협 행위가 감지된 공간의 영상을 획득하고, 상기 위협 행위가 감지된 시점을 기준으로 상기 사용자의 위험 지수에 따라 결정된 공간 범위만큼 모니터링 영상을 추출하는 단계,

상기 위협 행위가 감지된 이후, 상기 주변 사용자의 상기 주요 사용자에 대한 관심도의 변화를 확인하는 단계,

상기 확인 결과로부터 상기 주요 사용자에 대한 관심도가 감소한 경우, 상기 사용자의 모션 데이터를 3D 좌표 데이터로 변환하는 단계,

상기 3D 좌표 데이터를 이용하여 신체 특징이 포함되지 않은 스켈레톤(Skeleton) 기반 형상으로 변환하는 단계,

상기 변환된 스켈레톤 데이터를 애니메이션화하여 상기 주변 사용자 및 주요 사용자를 변환하는 단계,

상기 확인 결과로부터 상기 주요 사용자에 대한 관심도가 유지되는 경우, 상기 주변 사용자를 상기 관심도에 반비례하도록 결정된 변환 정도에 따라 변환하고, 상기 주요 사용자는 변환하지 않는 단계,

상기 확인 결과로부터 상기 주요 사용자에 대한 관심도가 증가한 경우, 상기 주변 사용자 및 주요 사용자를 모두 변환하지 않는 단계,

상기 위협 행위가 감지된 공간의 위협 행위 감지 횟수, 위험 행위 감지 빈도, 위협 행위 지속 시간, 보안 기관까지의 거리, 주변 보안 기관의 개수 및 유동인구 수를 확인하여 공간의 보안 수준을 결정하는 단계,

상기 위협 행위가 감지된 시점에서 멀어질수록 블러 강도를 줄이되, 상기 공간의 보안 수준을 고려하여, 상기 블러 강도에 상기 보안 수준에 기반하여 결정된 가중치를 적용하여 블러 강도를 조정하는 단계, 및

상기 블러 강도를 상기 모니터링 영상의 배경 부분에 적용하는 단계를 포함하는,

위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션 제공 방법.

발명의 설명

기 술 분 야

[0001] 아래 실시예들은 위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션을 제공하는 기술에 관한 것이다.

배 경 기 술

[0002] 최근 학교, 공공장소, 교통시설, 병원, 기업 등의 다양한 공간에서 예기치 못한 위협 행위나 폭력 사건이 빈번하게 발생함에 따라, 실시간 감지 및 대응이 가능한 보안 기술에 대한 필요성이 커지고 있다. 전통적인 보안 시스템은 대부분 CCTV 영상 기반으로 수동 모니터링되거나 단순한 움직임 감지 센서에 의존하는 방식이 일반적이었다.

[0003] 그러나 이러한 방식은 실제 위협 행위가 발생했을 때 즉각적으로 대응하기 어려우며, 폭력의 정황이나 가해자·피해자 식별과 같은 상황 인식 기능이 부족하다는 문제점이 있다. 특히, 기존 시스템은 주변 사용자의 반응이나 시선, 피해자의 심리적 반응 등을 고려하지 못하여, 폭력 사건의 심각성이나 긴급도에 대한 종합적인 판단이 어렵다는 한계가 존재한다.

[0004] 한편, 인공지능(AI) 및 3D 모션 인식 기술의 발전으로, 사람의 행동을 보다 정밀하게 추적하고 분석할 수 있는 기술이 가능해지고 있다. 이러한 기술을 활용하면 단순한 움직임이 아닌, 주먹질, 발길질, 밀치기 등과 같은 특정한 폭력 동작을 인식할 수 있으며, Skeleton 기반의 자세 추적을 통해 행위의 방향성, 속도, 반복성 등을 실시간으로 분석할 수 있다.

[0005] 나아가, AI는 주변 사람들의 시선 방향, 반응, 이동 패턴 등까지 통합 분석함으로써, 사건의 맥락을 이해하고 대응 우선순위를 판단할 수 있는 기반을 제공한다. 이에 따라, 위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션 제공 서비스에 대한 개발이 요구되는 실정이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허 제10-2024-0053902호(2024.04.25 공개)

(특허문헌 0002) 대한민국 등록특허 제10-2126498호(2020.06.25 공고)

(특허문헌 0003) 대한민국 등록특허 제10-2580434호(2023.09.20 공고)

(특허문헌 0004) 대한민국 공개특허 제10-2024-0167545호(2024.11.27 공개)

발명의 내용

해결하려는 과제

[0007] 실시예들은 사람 간의 위협 행위를 인공지능 기반 3D 모션 분석을 통해 실시간으로 감지하고, 위협의 정도 및 상황에 따라 자동으로 보안 알림을 제공하고자 한다.

[0008] 실시예들은 위협 행위 감지 이후, 사용자 간의 행동 패턴과 관심도 변화를 분석하여 가해자 및 피해자를 정밀하게 식별하고, 이에 따라 비상 알림의 대상, 범위 및 순서를 동적으로 조정하는 보안 대응 서비스를 제공하고자 한다.

[0009] 실시예들은 위협이 발생한 공간의 보안 수준을 고려하여 모니터링 영상을 Skeleton 기반 애니메이션으로 처리하고, 개인정보 보호와 보안 분석이 공존하는 지능형 영상 제공 방식을 통해 사용자 프라이버시를 보호하면서도 위협 상황에 효과적으로 대응하고자 한다.

[0010] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 일실시예에 따르면, 장치에 의해 수행되는 방법은 상기 3D 모션 인식 센서로부터 사용자의 모션 데이터를 획득하는 단계, 상기 모션 데이터를 기반으로 사용자의 행동 패턴을 생성하는 단계, 미리 학습된 위협 행동 패턴과 상기 행동 패턴을 비교하여 위협 행위를 감지하는 단계 및 상기 감지된 위협 행위를 기반으로 보안 알림을 생성하여 제공하는 단계를 포함할 수 있다.

[0012] 상기 보안 알림을 생성하여 제공하는 단계는, 상기 위협 행위가 감지된 환경에서 상기 행동 패턴으로부터 사용자의 움직임 속도, 방향성, 반복성, 가속도 및 자세 변화를 분석하여 위험 지수를 산출하는 단계, 상기 위험 지수가 미리 설정된 기준 이상인 경우, 해당 사용자를 주요 사용자로 분류하고, 상기 위험 지수가 미리 설정된 기준 미만인 경우, 해당 사용자를 주변 사용자로 분류하는 단계, 사용자를 위협 행위를 가한 가해자 및 위협을 당한 피해자로 분류하도록 미리 학습된 인공지능 모델에 상기 주요 사용자의 행동 패턴을 입력하여 상기 주요 사용자를 상기 가해자 및 피해자로 분류하는 단계, 상기 주변 사용자의 시선 데이터, 음성 데이터 및 행동 패턴을 분석하여 상기 주요 사용자에 대한 관심도를 산출하는 단계, 상기 가해자에 대한 관심도가 상기 피해자에 대한 관심도 미만인 경우, 상기 위험 지수에 따라 미리 설정된 기본 알림 범위를 확인하는 단계, 상기 가해자에 대한 관심도가 상기 피해자에 대한 관심도 이상이면서, 상기 피해자에 대한 관심도가 감소하는 경우, 상기 기본 알림 범위에 상기 피해자에 대한 관심도에 따른 감소 가중치를 적용하여 알림 범위를 결정하는 단계, 상기 가해자에 대한 관심도가 상기 피해자에 대한 관심도 이상이면서, 상기 피해자에 대한 관심도가 증가하는 경우, 상기 기본 알림 범위에 상기 피해자에 대한 관심도에 따른 증가 가중치를 적용하여 알림 범위를 결정하는 단계, 상기 사용자의 단말로부터 연락처 정보 및 현재 위치 정보를 획득하는 단계, 상기 연락처 정보 및 상기 현재 위치 정보로부터 상기 결정된 알림 범위에 따라 비상 연락처를 추출하는 단계, 상기 가해자에 대한 관심도와 상기 피해자에 대한 관심도의 차이가 미리 설정된 기준 이상인 경우, 상기 가해자와 관련된 순으로 알림 순서를 결정하는 단계, 상기 가해자에 대한 관심도와 상기 피해자에 대한 관심도의 차이가 미리 설정된 기준 미만인 경우, 상기 피해자와 관련된 순으로 알림 순서를 결정하는 단계 및 상기 알림 범위 및 알림 순서에 따라 보안 알림을 생성하여 제공하는 단계를 포함할 수 있다.

[0013] 상기 장치에 의해 수행되는 방법은 상기 위협 행위가 감지된 환경의 모니터링 영상을 제공하는 단계를 더 포함하고, 상기 위협 행위가 감지된 환경의 모니터링 영상을 제공하는 단계는, 상기 위협 행위가 감지된 공간의 영

상을 획득하고, 상기 위협 행위가 감지된 시점을 기준으로 상기 사용자의 위험 지수에 따라 결정된 공간 범위만큼 상기 모니터링 영상을 추출하는 단계, 상기 위협 행위가 감지된 이후, 상기 주변 사용자의 상기 주요 사용자에 대한 관심도의 변화를 확인하는 단계, 상기 확인 결과로부터 상기 주요 사용자에 대한 관심도가 감소한 경우, 상기 사용자의 모션 데이터를 3D 좌표 데이터로 변환하는 단계, 상기 3D 좌표 데이터를 이용하여 신체 특징이 포함되지 않은 스켈레톤(Skeleton) 기반 형상으로 변환하는 단계, 상기 변환된 스켈레톤 데이터를 애니메이션화하여 상기 주변 사용자 및 상기 주요 사용자를 변환하는 단계, 상기 확인 결과로부터 상기 주요 사용자에 대한 관심도가 유지되는 경우, 상기 주변 사용자를 상기 관심도에 반비례하도록 결정된 변환 정도에 따라 변환하고, 상기 주요 사용자는 변환하지 않는 단계, 상기 확인 결과로부터 상기 주요 사용자에 대한 관심도가 증가한 경우, 상기 주변 사용자 및 상기 주요 사용자를 모두 변환하지 않는 단계, 상기 위협 행위가 감지된 공간의 위협 행위 감지 횟수, 위험 행위 감지 빈도, 위협 행위 지속 시간, 보안 기관까지의 거리, 주변 보안 기관의 개수 및 유동인구 수를 확인하여 공간의 보안 수준을 결정하는 단계, 상기 위협 행위가 감지된 시점에서 멀어질수록 블러 강도를 줄이되, 상기 공간의 보안 수준을 고려하여, 상기 블러 강도에 상기 보안 수준에 기반하여 결정된 가중치를 적용하여 블러 강도를 조정하는 단계 및 상기 블러 강도를 상기 모니터링 영상의 배경 부분에 적용하는 단계를 포함할 수 있다.

[0014] 상기 모니터링 영상을 제공하는 단계는, 상기 음성 센서로부터 상기 공간 내 사용자의 음성 데이터를 획득하고, 상기 음성 데이터를 분석하여 키워드를 추출하는 단계, 상기 키워드가 미리 설정된 기준 이상으로 언급된 것에 해당하는 키워드를 주의 키워드로 분류하는 단계, 상기 주의 키워드가 등장하는 경우, 상기 주의 키워드가 등장하는 시점부터 상기 주의 키워드의 언급 횟수 및 상기 공간 내 사용자의 현재 위치에 해당하는 구역의 사용자 밀도에 기반하여 결정된 음성 추출 길이만큼 상기 음성 데이터를 추출하는 단계, 상기 모니터링 영상에 상기 추출된 음성 데이터를 함께 재생되도록 제어하는 단계 및 상기 음성 데이터에서 소리의 세기가 미리 설정된 기준 세기 미만인 경우, 상기 음성 데이터를 텍스트 데이터로 변환하여 생성된 자막을 상기 모니터링 영상에 표시하는 단계를 포함할 수 있다.

[0015] 상기 장치에 의해 수행되는 방법은 안전 이동 경로를 생성하여 제공하는 단계;를 더 포함하고, 상기 안전 이동 경로를 생성하여 제공하는 단계는, 상기 위협 행위가 감지된 공간에서 미리 설정된 기준 거리 내의 주변 구역에 존재하는 사용자 중 상기 주변 사용자 및 상기 주요 사용자를 제외한 근접 사용자를 추출하는 단계, 상기 근접 사용자의 단말로부터 목적지에 대한 정보를 수신하는 단계, 상기 근접 사용자와 상기 주요 사용자 사이의 거리를 확인하는 단계, 상기 공간 내 위험 지수, 상기 주요 사용자에 대한 관심도, 사용자의 밀도, 상기 확인된 거리를 기반으로 공간의 회피 지수를 결정하는 단계, 상기 근접 사용자의 현재 위치, 상기 목적지에 대한 정보, 상기 공간의 회피 지수를 안전한 이동 경로를 생성하기 위해 학습된 인공지능 모델에 입력하여 상기 근접 사용자의 안전 이동 경로를 출력하는 단계 및 상기 공간에 해당하는 지도 상에 상기 안전 이동 경로를 표시하여 상기 근접 사용자의 단말로 제공하는 단계를 포함할 수 있다.

[0016] 일실시예에 따른 장치는 하드웨어와 결합되어 상술한 방법들 중 어느 하나의 항의 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램에 의해 제어될 수 있다.

발명의 효과

[0017] 실시예들은 사용자의 3D 모션 데이터를 기반으로 위협 행위 여부를 정밀하게 판단하고, 실시간으로 위협 상황을 감지하여 즉각적인 보안 알림을 생성할 수 있다.

[0018] 실시예들은 가해자 및 피해자 식별뿐만 아니라, 주변 사용자의 시선 및 반응 데이터를 종합 분석함으로써 상황의 심각성을 평가하고, 알림 범위 및 전송 우선순위를 자동 조정할 수 있다.

[0019] 실시예들은 위협 상황이 발생한 공간의 보안 수준을 종합적으로 분석하고, 개인정보를 보호하기 위한 Skeleton 기반의 익명화 영상 제공과 위협도 가중 블러 처리 기술을 통해 사용자의 프라이버시와 보안 효율성을 동시에 확보할 수 있다.

[0020] 한편, 실시예들에 따른 효과들은 이상에서 언급한 것으로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 해당 기술 분야의 통상의 지식을 가진 자에게 명확히 이해될 수 있을 것이다.

도면의 간단한 설명

[0021] 도 1은 일실시예에 따른 시스템의 구성을 설명하기 위한 도면이다.

도 2는 일실시예에 따른 위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션을 제공하는 과정을 설명하기 위한 순서도이다.

도 3은 일실시예에 따른 보안 알림을 생성하여 제공하는 과정을 설명하기 위한 순서도이다.

도 4는 일실시예에 따른 위협 행위가 감지된 환경의 모니터링 영상을 제공하는 과정을 설명하기 위한 순서도이다.

도 5는 일실시예에 따른 음성 데이터를 기반으로 모니터링 영상을 제공하는 과정을 설명하기 위한 순서도이다.

도 6은 일실시예에 따른 안전 이동 경로를 생성하여 제공하는 과정을 설명하기 위한 순서도이다.

도 7은 일실시예에 따른 장치의 구성의 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 그러나, 실시예들에는 다양한 변경이 가해질 수 있어서 특허출원의 권리 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 실시예들에 대한 모든 변경, 균등물 내지 대체물이 권리 범위에 포함되는 것으로 이해되어야 한다.

[0023] 실시예들에 대한 특정한 구조적 또는 기능적 설명들은 단지 예시를 위한 목적으로 개시된 것으로서, 다양한 형태로 변경되어 실시될 수 있다. 따라서, 실시예들은 특정한 개시형태로 한정되는 것이 아니며, 본 명세서의 범위는 기술적 사상에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[0024] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 이런 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 해석되어야 한다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0025] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[0026] 실시예에서 사용한 용어는 단지 설명을 목적으로 사용된 것으로, 한정하려는 의도로 해석되어서는 안된다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0027] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0028] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0029] 실시예들은 퍼스널 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨터, 스마트 폰, 텔레비전, 스마트 가전 기기, 지능형 자동차, 키오스크, 웨어러블 장치 등 다양한 형태의 제품으로 구현될 수 있다.

[0030] 본 발명에서, 인공지능(Artificial Intelligence, AI)은 인간의 학습능력, 추론능력, 지각능력 등을 모방하고, 이를 컴퓨터로 구현하는 기술을 의미하고, 기계 학습, 심볼릭 로직(Symbolic Logic) 등의 개념을 포함할 수 있다. 기계 학습(Machine Learning, ML)은 입력 데이터들의 특징을 스스로 분류 또는 학습하는 알고리즘 기술이다. 인공지능의 기술은 기계 학습의 알고리즘으로써 입력 데이터를 분석하고, 그 분석의 결과를 학습하며, 그 학습의 결과에 기초하여 판단이나 예측을 할 수 있다. 또한, 기계 학습의 알고리즘을 활용하여 인간 두뇌의 인지, 판단 등의 기능을 모사하는 기술들 역시 인공지능의 범주로 이해될 수 있다. 예를 들어, 언어적 이해, 시각적 이해, 추론/예측, 지식 표현, 동작 제어 등의 기술 분야가 포함될 수 있다.

[0031] 기계 학습은 데이터를 처리한 경험을 이용해 신경망 모델을 훈련시키는 처리를 의미할 수 있다. 기계 학습을 통해 컴퓨터 소프트웨어는 스스로 데이터 처리 능력을 향상시키는 것을 의미할 수 있다. 신경망 모델은 데이터

사이의 상관 관계를 모델링하여 구축된 것으로서, 그 상관 관계는 복수의 파라미터에 의해 표현될 수 있다. 신경망 모델은 주어진 데이터로부터 특징들을 추출하고 분석하여 데이터 간의 상관 관계를 도출하는데, 이러한 과정을 반복하여 신경망 모델의 파라미터를 최적화해 나가는 것이 기계 학습이라고 할 수 있다. 예를 들어, 신경망 모델은 입출력 쌍으로 주어지는 데이터에 대하여, 입력과 출력 사이의 매핑(상관 관계)을 학습할 수 있다. 또는, 신경망 모델은 입력 데이터만 주어지는 경우에도 주어진 데이터 사이의 규칙성을 도출하여 그 관계를 학습할 수도 있다.

[0032] 인공지능 학습모델 또는 신경망 모델은 인간의 뇌 구조를 컴퓨터 상에서 구현하도록 설계될 수 있으며, 인간의 신경망의 뉴런(neuron)을 모의하며 가중치를 가지는 복수의 네트워크 노드들을 포함할 수 있다. 복수의 네트워크 노드들은 뉴런이 시냅스(synapse)를 통하여 신호를 주고받는 뉴런의 시냅틱(synaptic) 활동을 모의하여, 서로 간의 연결 관계를 가질 수 있다. 인공지능 학습모델에서 복수의 네트워크 노드들은 서로 다른 깊이의 레이어에 위치하면서 컨볼루션(convolution) 연결 관계에 따라 데이터를 주고받을 수 있다. 인공지능 학습모델은, 예를 들어, 인공 신경망 모델(Artificial Neural Network), 컨볼루션 신경망 모델(Convolution Neural Network: CNN) 등일 수 있다. 일 실시예로서, 인공지능 학습모델은, 지도학습(Supervised Learning), 비지도학습(Unsupervised Learning), 강화 학습(Reinforcement Learning) 등의 방식에 따라 기계 학습될 수 있다. 기계 학습을 수행하기 위한 기계 학습 알고리즘에는, 의사결정트리(Decision Tree), 베이지안 망(Bayesian Network), 서포트 벡터 머신(Support Vector Machine), 인공 신경망(Artificial Neural Network), 에이다부스트(Ada-boost), 퍼셉트론(Perceptron), 유전자 프로그래밍(Genetic Programming), 군집화(Clustering) 등이 사용될 수 있다.

[0033] 이중, CNN은 최소한의 전처리(preprocess)를 사용하도록 설계된 다계층 퍼셉트론(multilayer perceptrons)의 한 종류이다. CNN은 하나 또는 여러 개의 합성곱 계층과 그 위에 올려진 일반적인 인공 신경망 계층들로 이루어져 있으며, 가중치와 통합 계층(pooling layer)들을 추가로 활용한다. 이러한 구조 덕분에 CNN은 2차원 구조의 입력 데이터를 충분히 활용할 수 있다. 다른 딥러닝 구조들과 비교해서, CNN은 영상, 음성 분야 모두에서 좋은 성능을 보여준다. CNN은 또한 표준 역전달을 통해 훈련될 수 있다. CNN은 다른 피드포워드 인공신경망 기법들보다 쉽게 훈련되는 편이고 적은 수의 매개변수를 사용한다는 이점이 있다.

[0034] 컨볼루션 네트워크는 묶인 파라미터들을 가지는 노드들의 집합들을 포함하는 신경 네트워크들이다. 사용 가능한 트레이닝 데이터의 크기 증가와 연산 능력의 가용성이, 구분적 선형 단위 및 드롭아웃 트레이닝과 같은 알고리즘 발전과 결합되어, 많은 컴퓨터 비전 작업들이 크게 개선되었다. 오늘날 많은 작업에 사용할 수 있는 데이터 세트들과 같은 엄청난 양의 데이터 세트에서는 초과 맞춤(outfitting)이 중요하지 않으며, 네트워크의 크기를 늘리면 테스트 정확도가 향상된다. 컴퓨팅 리소스들의 최적 사용은 제한 요소가 된다. 이를 위해, 심층 신경 네트워크들의 분산된, 확장 가능한 구현예가 사용될 수 있다.

[0035] 이상에서 설명된 실시예들은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치, 방법 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0036] 도 1은 일실시예에 따른 시스템의 구성을 설명하기 위한 도면이다.

[0037] 도 1을 참조하면, 일실시예에 따른 시스템은 통신망을 통해 서로 통신 가능한 사용자의 단말(10) 및 장치(30)를 포함할 수 있다.

[0038] 먼저, 통신망은 유선 및 무선 등과 같이 그 통신 양태를 가리지 않고 구성될 수 있으며, 서버와 서버 간의 통신과 서버와 단말 간의 통신이 수행되도록 다양한 형태로 구현될 수 있다.

[0039] 사용자의 단말(10)은 본 발명에 따른 위협 행위 감지 기반 보안 솔루션 서비스를 제공받는 사용자가 사용하는 단말일 수 있다. 사용자의 단말(10)은 데스크탑 컴퓨터, 노트북, 태블릿, 스마트폰 등일 수 있다. 예를 들어, 도 1에 도시된 바와 같이, 사용자의 단말(10)은 스마트폰일 수 있으며, 실시예에 따라 달리 채용될 수도 있다.

[0040] 사용자의 단말(10)은 통상의 컴퓨터가 가지는 연산 기능, 저장/참조 기능, 입출력 기능 및 제어 기능을 전부 또는 일부 수행하도록 구성될 수 있다. 사용자의 단말(10)은 장치(30)와 유무선으로 통신하도록 구성될 수 있다.

[0041] 사용자의 단말(10)은 장치(30)를 이용하여 서비스를 제공하는 자 내지 단체가 운영하는 웹 페이지에 접속되거나, 장치(30)를 이용하여 서비스를 제공하는 자 내지 단체가 개발·배포한 애플리케이션이 설치될 수 있다. 사용자의 단말(10)은 웹 페이지 또는 애플리케이션을 통해 장치(30)와 연동될 수 있다.

[0042] 사용자의 단말(10)은 장치(30)에서 제공하는 웹 페이지, 애플리케이션을 등을 통해 장치(30)에 접속할 수 있다.

[0043] 청구항에 기재된 단수의 표현은 복수를 포함하는 것으로 이해될 수 있다.

[0044] 장치(30)는 인공지능 모델을 이용하여 사용자의 3D 모션 데이터를 기반으로 위협 행위 여부를 판단하고, 상황에 따라 보안 알림 및 회피 경로를 제공하는 AI 기반 보안 솔루션을 수행할 수 있다.

[0045] 구체적으로, 장치(30)는 3D 모션 인식 센서로부터 수집된 모션 데이터를 분석하여, 사용자의 행동 패턴을 생성하고, 미리 학습된 위협 행동 패턴과 비교함으로써 위협 행위 여부를 감지할 수 있다. 장치(30)는 위협이 감지된 이후, 사용자의 움직임 속도, 방향성, 반복성, 가속도, 자세 변화 등 다양한 요소를 분석하여 위험 지수를 산출하며, 이를 기반으로 해당 사용자를 주요 사용자 또는 주변 사용자로 분류할 수 있다.

[0046] 또한, 장치(30)는 가해자 및 피해자 식별을 위해 미리 학습된 인공지능 모델을 적용하고, 주변 사용자들의 시선, 음성, 행동 패턴을 분석하여 관심도를 평가함으로써 보안 알림의 범위 및 전달 순서를 동적으로 조정할 수 있다.

[0047] 장치(30)는 위협 발생 시점 이후의 사용자 간 행동 패턴, 관심도 변화, 공간 내 위험도와 보안 수준 등을 종합적으로 분석하여 Skeleton 기반의 변환 애니메이션 영상이나 블러링 처리된 모니터링 영상을 생성할 수 있다.

[0048] 장치(30)는 인근에 위치한 근접 사용자들의 현재 위치, 목적지, 회피 지수 등을 분석하고, 이를 경로 최적화 인공지능 모델에 입력하여 각 근접 사용자에게 위험 회피가 가능한 안전 이동 경로를 제공할 수 있다. 이때 생성된 경로는 사용자 단말(10)의 지도 UI 또는 AR 기반 인터페이스에 시각적으로 표시될 수 있다.

[0049] 이때, 위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션을 제공하는 과정에 대한 설명은 도 2를 참조하여 후술하기로 한다.

[0050] 장치(30)는 장치(30)를 이용하여 서비스를 제공하는 자 내지 단체가 보유한 자체 서버일수도 있고, 클라우드 서버일 수도 있고, 분산된 노드(node)들의 p2p(peer-to-peer) 집합일 수도 있다. 장치(30)는 통상의 컴퓨터가 가지는 연산 기능, 저장/참조 기능, 입출력 기능 및 제어 기능을 전부 또는 일부 수행하도록 구성될 수 있다.

[0051] 장치(30)는 사용자의 단말(10)과 유무선으로 통신하도록 구성될 수 있으며, 사용자의 단말(10)의 동작을 제어하고, 사용자의 단말(10)의 화면에 어느 정보를 표시할 것인지에 대해 제어할 수 있다.

[0052] 한편, 설명의 편의를 위해 도 1에서는 사용자의 단말(10)만을 도시하였으나, 단말들의 수는 실시예에 따라 얼마든지 달라질 수 있다. 장치(30)의 처리 용량이 허용하는 한, 단말들의 수는 특별한 제한이 없다.

[0053] 일실시예에 따르면, 장치(30) 내에는 데이터베이스가 구비될 수 있으며, 이에 한정되지 않고, 장치(30)와 별도로 데이터베이스가 구성될 수 있다. 장치(30)는 기계 학습 알고리즘의 수행을 위한 다수의 인공 신경망을 포함할 수 있다.

[0054] 도 2는 일실시예에 따른 위협 행위 감지를 위한 AI(인공지능) 기반 3D 모션 분석 및 보안 솔루션을 제공하는 과정을 설명하기 위한 순서도이다.

[0055] 도 2를 참조하면, 먼저 S201 단계에서, 장치(30)는 3D 모션 인식 센서로부터 사용자의 모션 데이터를 획득할 수 있다.

[0056] 장치(30)는 사용자의 신체 움직임을 실시간으로 감지하고 분석하기 위해, 공간 내 설치된 3D 모션 인식 센서로부터 모션 데이터를 수집할 수 있다.

[0057] 장치(30)는 사람의 움직임을 단순한 2D 영상이 아닌 입체적이고 정량화된 데이터로 분석함으로써, 위협 행위로

판단될 수 있는 복합적 행동 특성을 고정밀로 감지하고자 한다.

[0058] 사용자의 모션 데이터는 시간, 위치, 각 관절의 위치 좌표(x, y, z), 관절 간 거리, 이동 속도, 가속도 등의 다양한 형태로 정형화될 수 있으며, 이는 향후 AI 기반 분석에 활용될 수 있는 정제된 형태로 저장 및 전처리된다.

[0059] 장치(30)는 3D 모션 인식 센서 또는 센서 네트워크와 통신 가능하도록 설계될 수 있으며, 3D 모션 인식 센서는 ToF(Time-of-Flight) 카메라, 적외선 기반 Depth 카메라, LiDAR, mmWave 레이더 등을 포함할 수 있으나, 이에 한정되지는 않는다.

[0060] 예를 들어, 3D 모션 인식 센서는 RGB-D 카메라, LiDAR 센서, 적외선(IR) 센서, 초음파 센서 등을 포함할 수 있으나, 이에 한정되지는 않는다. 3D 모션 인식 센서는 RGB-D 카메라, LiDAR 센서, 적외선(IR) 센서, 초음파 센서 등의 기술을 적용하여 객체의 3차원 좌표 데이터를 생성할 수 있다. 장치(30)는 3D 모션 인식 센서를 통해, 기존의 2D 영상 기반 감시 시스템이 가지는 깊이 정보 부족 및 프라이버시 침해 문제를 해결할 수 있다.

[0061] 센서에서 수집된 원시 데이터는 장치(30) 내의 전처리 모듈에서 신호 노이즈 제거, 프레임 정렬, 동기화 등의 과정을 거친 후 모션 벡터 및 스켈레톤 형태로 변환될 수 있다. 또한, 복수의 센서로부터 데이터가 수집되는 경우에는 장치(30)는 이를 통합하여 다중 사용자 환경에서 사용자 식별 및 분리 처리를 수행할 수 있다.

[0062] 구체적으로, 3D 모션 인식 센서는 사용자의 위치(X, Y, Z), 속도, 이동 방향, 자세 변화 등을 실시간으로 수집하고, 이를 시간 순서대로 기록하여 사용자의 동선 및 행동 패턴을 분석할 수 있다.

[0063] 모션 데이터란 공간 내에서 객체(사람, 사물, 로봇 등)의 위치, 이동 경로, 속도, 방향, 자세 변화 등의 동적인 특성을 시간과 함께 기록한 정보를 의미한다. 본 발명에서는 3D 모션 인식 센서(RGB-D 카메라, LiDAR, IR 센서 등)를 활용하여 사용자의 움직임을 실시간으로 감지하고, 이를 3D 좌표 데이터로 변환하여 분석할 수 있다.

[0064] 예를 들어, 장치(30)는 사용자 손목의 좌표가 짧은 시간 내에 어깨 높이 이상으로 급격히 상승하고, 이후 다시 하강하는 패턴을 감지함으로써 '팔 휘두름'과 같은 모션 데이터를 수집할 수 있다. 이러한 형태의 움직임은 이후 행동 패턴 생성 및 위협 판단의 기초 정보로 활용된다.

[0065] 공공장소, 학교, 병원 등 다양한 장소에 설치된 고정형 센서에서 수행될 수 있으며, 사용자 단말(10)에 부착된 웨어러블 기기 또는 모바일 카메라를 통해서도 수행 가능하나, 이에 한정되지는 않는다. 센서 종류와 해상도, 환경 조도 등에 따라 데이터 정밀도는 달라질 수 있으나, 장치(30)는 다양한 하드웨어 플랫폼에서 유연하게 적용될 수 있다.

[0066] 본 발명의 실시예에 따라, 3D 모션 데이터 획득 방식은 특정 환경에 따라 다양한 변형이 가능하다.

[0067] 장치(30)는 3D 모션 인식 센서로부터 수집한 사용자의 모션 데이터를 객체와 매칭하여 데이터베이스에 저장할 수 있다.

[0068] S202 단계에서, 장치(30)는 모션 데이터를 기반으로 사용자의 행동 패턴을 생성할 수 있다.

[0069] 장치(30)는 시간 축을 따라 연속된 3D 좌표 데이터를 분석함으로써 단일 동작이 아닌 하나의 연속된 '행동 단위'를 구성하고 이를 벡터화할 수 있다.

[0070] 장치(30)는 신체 부위별 좌표 변화량, 관절 간 상대 거리, 속도, 가속도, 회전각 등을 정량화하고, 일정 시간 구간 내에서의 통계적 특징을 추출하여 고유한 행동 특징 벡터를 생성할 수 있다. 이 벡터는 행동의 종류를 대표하는 패턴으로 저장되며, 딥러닝 기반의 행동 인식 모델(CNN, LSTM, GCN 등)에 의해 특징 추출 및 분류가 수행될 수 있다.

[0071] 예를 들어, 사용자가 빠르게 팔을 앞쪽으로 뻗은 후 뒤로 당기고 몸을 회전시킨 경우, 장치(30)는 해당 일련의 동작을 '밀침' 또는 '공격 시도'로 분류할 수 있는 행동 패턴으로 구성한다. 이를 위해 각 관절의 이동량과 속도를 고려한 다차원 벡터가 생성되고, 이는 다음 단계에서 위협 패턴과 비교되는 기준이 된다.

[0072] 행동 패턴은 사용자별로 누적 학습되어 개인 특성을 반영하거나, 집단 데이터를 기반으로 일반화된 분류 모델을 적용할 수 있다. 장치(30)는 실시간 행동 패턴 생성을 통해 지속적인 모니터링과 이상행동 탐지를 지원할 수 있으며, 비일상적 동작(예: 급격한 점프, 회피, 공격 등)에 대해서는 즉시 경보 대상 패턴으로 등록될 수 있다.

[0073] S203 단계에서, 장치(30)는 미리 학습된 위협 행동 패턴과 행동 패턴을 비교하여 위협 행위를 감지할 수 있다. 장치(30)는 단순한 이상행동 감지가 아닌, 학습된 위협 동작의 특징을 기준으로 공격적인 의도를 가진 행동을

식별하고자 한다.

[0074] 장치(30)는 사전에 수집된 다양한 위협 행동 데이터셋(예: 주먹질, 발차기, 밀기, 칼 들기 등)을 바탕으로 학습된 AI 모델을 기반으로, 입력된 행동 패턴과의 유사도를 계산하여 일정 임계값 이상일 경우 위협 행위로 판정할 수 있다. 이 과정에서는 CNN 기반 행동 인식, GCN 기반 Skeleton 그래프 분류, 또는 attention 기반의 시계열 분석 모델이 사용될 수 있으나, 이에 한정되지는 않는다.

[0075] 미리 학습된 위협 행동 패턴은, 본 발명에 따른 장치(30)가 사용자의 행동 패턴을 위협 행위 여부와 비교·판별하기 위한 기준 정보로서, 사전에 수집된 다양한 위협 동작 데이터를 기반으로 인공지능 모델에 의해 학습된 행동 특성 벡터 또는 분류 모델을 의미한다.

[0076] 위협 행동 패턴은 인간의 공격적 또는 폭력적 의도를 나타내는 행위 유형(예: 주먹을 휘두름, 밀침, 발차기, 무기 휘두름, 목 조르기 등)을 중심으로 구성되며, 각 행위는 3D Skeleton 구조 상에서 시간에 따른 관절 위치 변화, 움직임의 방향성과 속도, 가속도, 회전 패턴 등을 포함하는 다차원 특징으로 정형화되어 있다.

[0077] 예를 들어 장치(30)에서 사용되는 위협 행동 패턴은, Graph Convolutional Network(GCN), Long Short-Term Memory(LSTM), 3D-CNN, Transformer 기반 행동 인식 모델 등을 통해 학습될 수 있으나, 이에 한정되지는 않는다.

[0078] 학습 데이터는 실제 폭력 장면 영상, 시뮬레이션 데이터, 게임 기반 행동 캡처, 인체 행동 데이터셋(Kinetics, NTU RGB+D 등)을 포함하여 구축되며, 이들 데이터로부터 추출된 행동 시퀀스를 바탕으로 AI 모델이 각 위협 행위의 대표 특징을 추론하고 일반화된 패턴으로 정리한다.

[0079] 이 과정은 단순히 단일 포즈가 아닌, 일정 시간 동안의 연속된 움직임 시퀀스를 학습함으로써, 명확한 위협 의도가 내포된 행동과 일반적인 격한 움직임(예: 체조, 운동 등)을 구분할 수 있도록 한다.

[0080] 장치(30)는 이러한 미리 학습된 위협 행동 패턴을 저장하고 있다가, 실시간으로 입력되는 사용자 행동 패턴과 비교하여 일정 유사도 이상인 경우 위협 행위로 판별할 수 있다.

[0081] 유사도는 예측 확률, 코사인 유사도, 다중 클래스 분류 결과 등 다양한 방식으로 계산될 수 있으며, 위협 패턴은 특정 장소나 대상에 따라 맞춤형으로 학습 및 업데이트될 수도 있다. 또한, 장치(30)는 위협 행동의 종류에 따라 가중치를 다르게 적용하거나, 특정 사용자 집단(예: 아동, 노인)에 적합한 위협 기준을 별도로 설정함으로써, 다양한 공간 및 사용자 환경에 대응하는 유연한 보안 판단이 가능하다.

[0082] 장치(30)는 위협 행동과 유사한 일반적인 움직임(예: 스트레칭, 스포츠 동작, 춤, 장난스러운 접촉 등)을 비위협 행동으로 구분하기 위해, 동작의 맥락적 특징과 주변 반응 데이터를 함께 고려하는 복합 판단 기준을 적용할 수 있다.

[0083] 예를 들어, 사용자의 팔이 빠르게 휘둘리는 동작이라 하더라도, 해당 동작이 짧은 시간 내 반복되지 않거나, 타인과의 거리가 일정 이상 유지되는 경우에는 위협 가능성을 낮게 판단할 수 있다.

[0084] 또한, 장치(30)는 주변 사용자들의 시선 방향, 이동 반응, 음성 감정 분석 등을 함께 연동하여, 공격적 상황에서 일반적으로 발생하는 긴장된 반응이나 회피 행동이 나타나지 않으면 비위협 행동으로 간주할 수 있다.

[0085] 장치(30)는 오탐(오경보) 방지를 위해 실시간 보정 로직을 포함한 다단계 필터링 구조를 적용할 수 있다.

[0086] 예를 들어, 1차로 행동 패턴 유사도 기반 예비 판단을 수행한 후, 2차로 주변 맥락 데이터(시선, 음성, 위치 변화 등)를 분석하여 위협 여부를 재검증하며, 최종적으로 일정 시간 이상 위협 행동이 지속되거나 반복될 경우에만 보안 알림을 활성화한다.

[0087] 이러한 구조는 순간적인 격한 움직임이나 장난성 접촉으로 인한 경보 발생을 최소화하고, 실제 위험 상황에 대한 민감도는 유지하는 데 효과적이다. 실시간 판단 로직은 시간 기반 슬라이딩 윈도우, 예측 확률 누적 모델, 또는 주기적 리샘플링을 기반으로 작동하며, 상황 변화에 따라 자동으로 위험 지수를 갱신하고 보안 대응 수준을 조정할 수 있다.

[0088] 예를 들어, 사용자의 행동 패턴이 ‘팔을 빠르게 뻗음 + 상대방과 거리 좁힘 + 몸 중심이 전방으로 이동’ 하는 조합으로 인식되었을 경우, 장치(30)는 이를 사전에 학습된 ‘폭력 행위’와 유사하다고 판단하고, 위협 행위로 감지한다. 감지된 결과는 이후 알림 생성 단계의 핵심 인풋이 된다.

[0089] 장치(30)는 단일 행동뿐만 아니라, 반복적이거나 연속된 위협 행위도 탐지할 수 있으며, 동일 공간 내에서 유사

한 패턴이 연쇄적으로 발생할 경우 상황의 심각도를 상향 조정하여 판단할 수 있다. 또한, 피해자 행동(회피, 도주, 방어)도 함께 분석함으로써 감지의 신뢰도를 높일 수 있다.

[0090] S204 단계에서, 장치(30)는 감지된 위협 행위를 기반으로 보안 알림을 생성하여 제공할 수 있다.

[0091] 장치(30)는 단순 경고 수준의 알림에 그치지 않고, 상황의 심각성, 가해자·피해자 식별, 주변 사용자의 반응, 공간의 위험도 등을 종합 분석하여 맞춤형 알림을 생성하고자 한다.

[0092] 장치(30)는 감지된 위협 행위의 유형과 강도, 가해자의 행동 지속성, 피해자의 반응, 주변 사용자의 시선 및 음성 반응 등을 종합하여 위험 지수를 산출하고, 이 지수를 기반으로 알림 범위, 전송 대상(보안 요원, 관리자, 경찰, 응급 연락처 등), 전송 순서 등을 결정할 수 있다. 또한, 알림 수단은 스마트폰 푸시 알림, 문자, 음성 호출, 전광판 경고 등 다양한 방식으로 설정 가능하다.

[0093] 예를 들어, 피해자가 심각한 부상을 입은 것으로 판단되고, 가해자가 계속 공격 행동을 시도하고 있다면, 장치(30)는 가장 가까운 보안 인력에게 우선 알림을 전송하고, 동시에 피해자의 보호자 또는 관리자에게 알림을 순차적으로 제공할 수 있다. 또한, 공간 위험도가 높거나 유동 인구가 많은 경우에는 주변 사용자들에게도 회피 안내 경로를 포함한 알림을 전송할 수 있다.

[0094] 본 발명의 실시예에 따라, 경찰 출동 자동 요청, CCTV 추적 모드 전환, 출입문 자동 잠금, 드론 추적 출동 등 다양한 후속 보안 조치와 연계될 수 있다. 장치(30)는 실시간 데이터를 기반으로 알림 내용을 지속적으로 갱신함으로써 위협 상황 종료까지 대응 효율성을 극대화할 수 있다.

[0095] 이때, 보안 알림을 생성하여 제공하는 단계는 도 3을 참조하여 자세히 후술하기로 한다.

[0096] 도 3은 일실시예에 따른 보안 알림을 생성하여 제공하는 과정을 설명하기 위한 순서도이다.

[0097] 도 3을 참조하면, 먼저 S301 단계에서, 장치(30)는 위협 행위가 감지된 환경에서 행동 패턴으로부터 위험 지수를 산출할 수 있다.

[0098] 위험 지수는 사용자의 움직임이 위협적 상황으로 이어질 가능성을 정량적으로 평가한 값으로, 보안 알림의 긴급도 결정 및 후속 분류 판단에 활용될 수 있다.

[0099] 장치(30)는 단순히 위협 행위 감지만 하는 것이 아니라, 행동의 ‘강도’, ‘의도성’, ‘반복성’을 수치화하여 보다 정교한 보안 판단이 가능하도록 하고자 한다.

[0100] 장치(30)는 사용자의 행동 패턴 데이터를 기반으로, 속도, 방향성, 반복성, 가속도, 자세 변화 등 다양한 요소를 분석하여 종합적인 위험 지수를 계산할 수 있다. 일실시예에 따르면, 장치(30)는 위협 행위가 감지된 환경에서 사용자의 행동 패턴으로부터 사용자의 움직임 속도, 방향성, 반복성, 가속도 및 자세 변화를 분석하여 위험 지수를 산출할 수 있다.

[0101] 장치(30)는 사용자의 움직임 속도가 바를수록, 움직임 방향의 변화도가 높을수록, 반복성이 높을수록, 가속도가 높을수록, 자세 변화도가 높을수록 위험 지수를 높게 산출할 수 있다.

[0102] 예를 들어, 사용자가 특정 공간 내에서 반복적으로 빠른 속도로 이동하며, 팔을 넓게 휘두르고 몸의 균형이 급격히 변하는 패턴이 감지된 경우, 장치(30)는 해당 사용자의 속도, 가속도, 자세 변화량 등을 기반으로 높은 위험 지수를 산출할 수 있다. 반대로, 같은 공간에서 천천히 걷는 사용자나 일시적으로 한 번 손을 흔든 사용자에게는 낮은 위험 지수가 부여될 수 있다.

[0103] 위험 지수는 실시간으로 변화할 수 있으며, 일정 시간 내에 재계산되어 누적 방식으로 적용될 수도 있다. 또한, 장소의 성격(학교, 병원, 공항 등)이나 사용자 그룹(어린이, 노약자 등)에 따라 위험 지수 산정 기준이 조정될 수 있다.

[0104] S302 단계에서, 장치(30)는 위험 지수가 미리 설정된 기준 이상인 경우, 해당 사용자를 주요 사용자로 분류하고, 위험 지수가 미리 설정된 기준 미만인 경우, 해당 사용자를 주변 사용자로 분류할 수 있다. 이때, 미리 설정된 기준은 환경, 시간대, 공간 크기, 사용자 특성 등을 고려하여 실시예에 따라 상이하게 설정될 수 있다.

[0105] 이에 따라, 장치(30)는 공간 내 수많은 사용자 중에서 보안 대응이 필요한 대상자를 우선 선별하여 시스템 자원 및 대응 속도를 최적화하고자 한다.

[0106] 예를 들어, 장치(30)는 운동장에서 격렬하게 움직이는 복수의 사용자 중, 특정 사용자 한 명만이 반복적으로 빠

른 전진 동작과 함께 주변인에게 근접한 동작을 취하는 것을 감지한 경우, 해당 사용자만을 주요 사용자로 분류하고 나머지는 주변 사용자로 분류할 수 있다. 이렇게 분류된 주요 사용자만을 대상으로 후속 가해자/피해자 판단 및 경보 생성 절차가 진행된다.

[0107] 이러한 분류 방식은 보안 리소스를 효율적으로 운용할 수 있게 하며, 오탐률을 줄이면서 대응 속도를 높이는 효과가 있다. 또한 장치(30)는 위험 지수 변동에 따라 실시간으로 사용자의 등급을 재조정할 수 있으므로, 정적인 설정이 아닌 동적인 분류 체계를 제공할 수 있다.

[0108] S303 단계에서, 장치(30)는 주요 사용자를 가해자 및 피해자로 분류할 수 있다.

[0109] 장치(30)는 위협 상황에서 단순히 위험 사용자만을 식별하는 것을 넘어, 그 사용자가 위협을 가한 주체인지, 당한 대상인지를 명확히 판단하여, 후속 대응 조치(예: 경보 대상, 응급 조치, 신고 대상 등)를 정확히 수행하고자 한다.

[0110] 구체적으로, 장치(30)는 사용자를 위협 행위를 가한 가해자 및 위협을 당한 피해자로 분류하도록 미리 학습된 인공지능 모델에 주요 사용자의 행동 패턴을 입력하여 주요 사용자를 가해자 및 피해자로 분류할 수 있다.

[0111] 인공지능 모델은 위협 행동 시의 동작의 방향성, 충격 유도 여부, 자세 반응, 이동 경로 등을 기반으로 판단하며, CNN, GCN, 또는 attention 기반 시계열 모델 등이 활용될 수 있다. 또한, 피해자의 특징(예: 방어 동작, 뒷걸음질, 쓰러짐 등)과 가해자의 특징(예: 지속적 전진, 공격 자세 등)을 명확히 분류할 수 있도록 훈련된 모델이 사용될 수 있다.

[0112] 미리 학습된 인공지능 모델은, 주요 사용자의 행동 패턴을 분석하여 해당 사용자가 위협 행위를 가한 가해자인지, 또는 위협을 당한 피해자인지를 자동으로 분류할 수 있도록 설계된 예측 모델이다.

[0113] 이 모델은 단순히 움직임의 유사도를 비교하는 수준을 넘어, 동작의 방향성, 충격 유도 여부, 자세 반응, 거리 변화 등 다양한 특징을 동시에 고려함으로써 사람 간의 상호작용 관계를 인지하고 판단할 수 있다. 즉, 단일 사용자 기반의 판단이 아니라, 상대적 행동 분석에 기반한 분류 로직을 내포한다는 데에 기술적 의의가 있다.

[0114] 해당 인공지능 모델은 가해자와 피해자 각각의 특징적인 행동 시퀀스를 학습 데이터로 활용하여 훈련된다.

[0115] 예를 들어, 가해자는 일반적으로 전진하면서 공격 동작(주먹 휘두르기, 밀기 등)을 수행하며, 피해자는 후퇴, 몸 움츠리기, 넘어짐, 방어 자세 등을 보인다. 이러한 데이터는 다자 간 행동 분석이 가능한 Skeleton 기반의 3D 좌표 시퀀스로 정제되어 학습되며, 딥러닝 알고리즘으로는 Graph Convolutional Network(GCN), LSTM, Transformer, Bidirectional GRU 등이 적용될 수 있다.

[0116] 특히 시간 축에서의 전후 관계를 정확히 파악하기 위해 시계열 기반 모델이 효과적으로 활용된다.

[0117] 실시예에 따르면, 두 사용자가 동시에 동작을 취하였더라도, 인공지능 모델은 행동의 선후 관계, 접촉 시점 이전·이후의 움직임, 상대방과의 거리 변화 등을 기준으로 판단을 수행한다.

[0118] 예를 들어, 한 사용자가 팔을 뻗은 직후 다른 사용자가 뒤로 물러나거나 쓰러지는 경우, 해당 시퀀스를 분석하여 전자를 가해자, 후자를 피해자로 분류할 수 있다.

[0119] 또한, 장치(30)는 이 모델의 분류 결과에 주변 사용자들의 시선 반응, 소리, 자세 등을 함께 반영함으로써 분류의 신뢰도를 향상시킬 수 있으며, 필요에 따라 지속 학습이 가능한 구조로 구현되어, 실시간 환경 변화나 새로운 행동 패턴에 유연하게 대응할 수 있다.

[0120] 예를 들어, 장치(30)는 서로 마주 보고 있는 두 사용자 중, 한 사용자가 팔을 먼저 뻗고 전진하며, 다른 사용자가 뒤로 물러나거나 쓰러지는 행동을 보이는 경우, 전자를 '가해자', 후자를 '피해자'로 자동 분류할 수 있다. 이때 주변 사용자들의 시선 방향과 반응(예: 피해자를 향한 시선, 놀람 표정 등)도 분석하여 분류의 신뢰도를 높일 수 있다.

[0121] 장치(30)는 상황에 따라 오분류 가능성을 줄이기 위해, 분류 결과에 가중치를 적용하거나 일정 시간 동안의 행동 누적 패턴을 분석하는 후속 검증 과정을 포함할 수 있다.

[0122] 또한, 복수의 주요 사용자가 있는 경우에는 상호 작용 관계, 접촉 위치, 시간 순서를 고려하여 다자 간 가해-피해 관계를 판단할 수 있다. 이처럼 장치(30)는 실제 위협 상황을 정밀하게 해석하여, 대응의 정확성과 신속성을 크게 향상시킬 수 있다.

[0123] S304 단계에서, 장치(30)는 주변 사용자의 시선 데이터, 음성 데이터 및 행동 패턴을 분석하여 주요 사용자에

대한 관심도를 산출할 수 있다.

[0124] 장치(30)는 위협 상황이 발생한 후 주변 사용자들이 가해자 또는 피해자 중 누구에게 더 주의를 기울이고 있는지를 분석하여, 상황의 중대도 및 대응 우선순위를 판단하는 데 활용할 수 있다.

[0125] 관심도는 보안 알림의 범위, 경보 강도 및 대응 속도 결정에 작용할 수 있다.

[0126] 모션 데이터에는 시선 데이터, 음성 데이터가 포함될 수 있다.

[0127] 장치(30)는 카메라 기반 시선 추적 기술을 통해 주변 사용자들의 시선 방향을 실시간으로 수집하고, 마이크 또는 음성 센서를 통해 감지된 발화 음성의 방향, 크기, 감정 상태를 분석할 수 있다.

[0128] 장치(30)는 주변 사용자의 행동 패턴(예: 접근/도주 방향, 가리키기, 뒤로 물러서기 등)을 Skeleton 기반 3D 데이터로 분석하여, 해당 사용자가 누구를 향해 반응하고 있는지를 종합 판단할 수 있다. 이러한 분석 결과를 바탕으로 가해자 및 피해자 각각에 대해 관심도 점수를 계산할 수 있다.

[0129] 예를 들어, 주변 사용자들의 시선이 지속적으로 특정 인물(피해자)에게 집중되고, 말소리의 방향도 피해자 쪽으로 향해 있으며, 일부 사용자가 해당 인물에게 접근하는 동작을 취하는 경우, 장치(30)는 피해자에 대한 관심도가 높다고 판단할 수 있다.

[0130] 반대로, 주변 사용자들이 가해자 방향으로 경계하거나 지켜보는 경우, 가해자에 대한 관심도가 높게 산정된다. 관심도는 개별 사용자별 판단 값을 가중 평균하는 방식으로 공간 전체의 시선을 요약할 수 있다.

[0131] 관심도는 정적 수치가 아니라 실시간으로 갱신되며, 위협 상황의 전개에 따라 상대적인 변화가 클 수 있다. 장치(30)는 관심도 산정 결과를 기반으로 위협의 중심이 어느 인물인지 판단하고, 이후 보안 대응에 반영될 수 있도록 구성된다. 또한 관심도 분석은 가해자·피해자 분류의 신뢰도를 높이거나, 오탐 방지를 위한 후속 판단 요소로도 활용될 수 있다.

[0132] S305 단계에서, 장치(30)는 주요 사용자에 대한 관심도에 기반하여 알림 범위를 결정할 수 있다. 장치(30)는 위협 상황에 따라 필요한 보안 대응 범위를 동적으로 설정함으로써, 불필요한 경고를 줄이고 효과적인 대응이 이루어지도록 할 수 있다.

[0133] 장치(30)는 가해자에 대한 관심도가 피해자에 대한 관심도 미만인 경우, 위험 지수에 따라 미리 설정된 기본 알림 범위를 확인할 수 있다.

[0134] 장치(30)는 우선, 가해자에 대한 관심도가 피해자에 대한 관심도보다 낮은 경우, 즉 피해자 중심으로 시선 및 반응이 집중되는 경우, 현재 상황이 피해자 보호에 집중되어야 한다고 판단하고, 기본 위험 지수에 따라 미리 설정된 기본 알림 범위를 그대로 적용할 수 있다. 기본 알림 범위는 관리자, 보안 요원, 피해자 보호자 등으로 구성될 수 있으나, 이에 한정되지는 않는다.

[0135] 예를 들어, 학교 내에서 학생이 폭력을 당한 직후 주변 친구들이 피해자를 둘러싸고 있는 경우, 보건실·교사·학부모에게 우선적으로 알림을 발송하도록 설정할 수 있다.

[0136] 장치(30)의 데이터베이스에는 위험 지수에 따른 기본 알림 범위가 매칭되어 저장되어 있을 수 있다.

[0137] 이 경우, 피해자가 위협을 직접적으로 당한 상태이거나, 위협 직후 회복 중이며 주변에서 도움이나 응급조치를 시도하는 것으로 해석될 수 있다.

[0138] 장치(30)는 가해자에 대한 관심도가 피해자에 대한 관심도 이상이면서, 피해자에 대한 관심도가 감소하는 경우, 기본 알림 범위에 피해자에 대한 관심도에 따른 감소 가중치를 적용하여 알림 범위를 결정할 수 있다.

[0139] 장치(30)는 주변 사용자들이 가해자 쪽으로 시선을 옮기고, 피해자에 대한 주의가 줄어드는 경우, 현재 위협의 중심이 가해자에게 있거나, 가해자가 아직도 위협을 계속 가하고 있는 상황으로 판단할 수 있다.

[0140] 피해자는 자리를 벗어났거나, 주변으로부터 일시적으로 관심을 받지 못하고 있는 상태일 수 있다.

[0141] 이 경우 장치(30)는 기본 알림 범위를 조정할 필요가 있다고 판단하고, 피해자에 대한 관심도 감소량을 고려해 감소 가중치를 적용한 알림 범위를 설정한다.

[0142] 예를 들어, 피해자가 현장을 이탈하고 가해자가 공간 내에서 계속 위협을 가할 가능성이 높은 경우, 장치(30)는 기존 알림 대상 외에 가해자 주변 구역의 보안 인력, 관리자, 도주 경로 상의 감시 장치에도 알림을 확장할 수 있다.

[0143] 이러한 방식은 위협이 종료되지 않고 다른 사용자에게로 확산되거나 2차 피해가 발생할 수 있는 상황을 방지하기 위한 전략으로, 위협의 지속성과 이동성을 고려한 동적 보안 대응을 가능하게 한다.

[0144] 장치(30)는 가해자에 대한 관심도가 피해자에 대한 관심도 이상이면서, 피해자에 대한 관심도가 증가하는 경우, 기본 알림 범위에 피해자에 대한 관심도에 따른 증가 가중치를 적용하여 알림 범위를 결정할 수 있다.

[0145] 장치(30)는 주변 사용자들이 가해자 쪽도 주시하고 있지만, 특히 피해자에게 집중된 관심이 점점 더 커지고 있는 경우, 해당 상황을 피해자의 상태가 점차 심각해지고 있거나 위급 상황으로 악화되고 있는 것으로 판단할 수 있다. 피해자가 쓰러지거나 울부짖는 등 명백한 이상 반응을 보이는 경우가 이에 해당한다.

[0146] 이와 같은 판단이 내려지면, 장치(30)는 피해자에 대한 관심도 증가율에 비례하여 증가 가중치를 적용하고, 알림 범위를 즉시 확장할 수 있다. 예를 들어, 단순 보안 요원 외에도 응급 구조대, 제휴 병원, 피해자 보호자, 경찰, 인근 공간 관리자 등에게까지 보안 알림을 확대 전송할 수 있다. 공간 내 일반 사용자에게는 피해자와의 충돌을 피할 수 있도록 회피 경로 안내 또는 주의 방송도 포함할 수 있다.

[0147] 이처럼 장치(30)는 상황의 심각도, 피해자의 상태 악화 여부, 실시간 주변 반응 등을 반영하여 위협 수준에 적합한 다계층 대응 구조를 갖추게 된다.

[0148] 알림 범위 조정 방식은 기존의 일률적 경보 방식과 달리, 실시간 반응성과 상황 맥락을 반영한 적응형 경보 체계를 구현할 수 있다는 점에서 기술적 효과가 크다.

[0149] 또한, 장치(30)는 알림 대상의 위치, 관계, 반응 시간 등을 종합 고려하여 단계적 알림 전파를 설정할 수 있으며, 필요 시 범위를 제한하거나 확장하여 개인화된 보안 대응도 가능하게 한다.

[0150] S306 단계에서, 장치(30)는 사용자의 단말(10)로부터 연락처 정보 및 현재 위치 정보를 획득할 수 있다.

[0151] 장치(30)는 사용자의 단말(10)로부터 수집한 연락처 정보 및 현재 위치 정보를 데이터베이스에 사용자와 매칭하여 저장할 수 있다.

[0152] 장치(30)는 사용자 단말(10)과 연동된 앱, 웨어러블 기기, 또는 위치 기반 API 등을 통해 사용자의 현재 좌표(GPS, Wi-Fi 기반 실내 위치 등)를 획득할 수 있으며, 사용자 프로필에 등록된 연락처 정보(보호자 번호, 응급 연락처, 관리자 계정 등)를 함께 수집할 수 있다. 수집된 정보는 내부 암호화 또는 보안 정책에 따라 보호되며, 긴급 상황 발생 시 자동 호출용으로 사용된다.

[0153] 예를 들어, 위협 상황이 감지된 학교 내에서 한 학생이 피해자로 판단되었을 경우, 장치(30)는 해당 학생의 단말에서 실시간 위치(GPS 기반 교실 위치) 및 등록된 보호자 연락처를 획득하고, 이를 기반으로 대응 대상자 및 알림 방식(전화, 문자, 앱 푸시 등)을 결정할 수 있다. 만약 보호자가 등록되지 않은 경우에는 학급 담임 교사 또는 보건실 담당자 연락처가 우선순위로 사용될 수 있다.

[0154] 정보 획득 단계는 추후 알림 전송 대상과 방식의 정밀도를 높이며, 개인정보 보호를 위한 조건부 접근이나 관리자 승인 기반 정보 활용 모델도 함께 연계될 수 있다. 다양한 사용자 단말의 환경(스마트폰, 태블릿, 스마트워치 등)에 적용 가능하며, 특정 IoT 기기와도 확장 연동할 수 있다.

[0155] S307 단계에서, 장치(30)는 연락처 정보 및 현재 위치 정보로부터 결정된 알림 범위에 따라 비상 연락처를 추출할 수 있다.

[0156] 장치(30)는 수많은 연락처 중 현재 상황과 위치, 사용자 상태에 적합한 대상만을 선별하여 효율적인 알림 전송 체계를 구성하고자 한다.

[0157] 장치(30)는 알림 범위 설정 결과를 토대로, 사용자별 우선순위, 공간 내 위치, 조직 내 역할 등을 기준으로 필터링을 수행한다. 예를 들어, 피해자 중심 알림이라면 보호자, 의료 담당자, 상담 교사 등을 추출하며, 가해자 중심일 경우 관리자, 보안 요원, 출입 통제 관리자 등이 추출될 수 있다. 추출 과정에서는 거리 기반 필터링(현재 위치와의 거리), 역할 기반 필터링(등록된 담당자 여부), 관계 기반 필터링(사용자 ID 기반 보호자 연동 여부) 등이 사용될 수 있다.

[0158] 실시예에 따르면, 특정 건물의 3층에서 위협 상황이 발생했을 때, 장치(30)는 현재 위치를 기준으로 같은 층에 있는 보안 인력의 연락처를 1차로 추출하고, 해당 사용자와 연계된 보호자나 교직원 번호를 추가적으로 추출할 수 있다. 이후 상황 전개에 따라 알림 범위가 확장되면, 2차 추출 대상으로 병원, 경찰, 응급기관 번호 등이 포함될 수 있다.

[0159] 이와 같은 추출 방식은 중복 알림 방지, 비효율적 알림 감소, 응답 불가자 제외 등의 효과를 가지며, 조직 구조가 복잡하거나 공간이 넓은 경우에도 적절한 대상만을 빠르게 확보할 수 있다. 또한, 이 단계는 정책 기반 템플릿에 따라 자동화될 수 있으며, 사용자 설정 또는 관리자 커스터마이징도 가능하다.

[0160] S308 단계에서, 장치(30)는 가해자에 대한 관심도와 피해자에 대한 관심도의 차이에 기반하여 알림 순서를 결정할 수 있다.

[0161] 장치(30)는 동일한 알림 범위 내에서도 우선순위를 정하여 보다 신속하고 효과적인 대응을 유도하고자 한다. 알림 대상이 다수인 경우, 순차적 전송 전략은 보안 대응의 질을 높이는 핵심 요소가 된다.

[0162] 구체적으로, 장치(30)는 가해자에 대한 관심도와 피해자에 대한 관심도의 차이가 미리 설정된 기준 이상인 경우, 가해자와 관련된 순으로 알림 순서를 결정할 수 있다. 이때, 미리 설정된 기준은 실시예에 따라 상이하게 설정될 수 있다.

[0163] 장치(30)는 관심도 차이가 미리 설정된 기준 이상인 경우, 가해자와 관련된 알림 우선순위를 설정한다. 예를 들어, 가해자가 지속적 위협을 가하거나 주변 사용자에게 확산될 가능성이 높은 상황이라면, 가해자 중심 대응이 중요하다고 판단되어 보안 인력, 관리자, 출입 통제 담당자 등에게 먼저 알림을 발송할 수 있다.

[0164] 반대로, 장치(30)는 가해자에 대한 관심도와 피해자에 대한 관심도의 차이가 미리 설정된 기준 미만인 경우, 피해자와 관련된 순으로 알림 순서를 결정할 수 있다.

[0165] 장치(30)는 관심도 차이가 기준 미만일 경우, 피해자와 관련된 알림 순서를 우선 설정하여 보호자, 의료진, 상담 교사 등에게 먼저 알림이 전송되도록 조정한다.

[0166] 실시예로는, 장치(30)가 피해자 관심도가 높고, 가해자 관심도가 상대적으로 낮은 상태에서 피해자가 쓰러져 있는 경우, 보호자 → 응급 구조 → 학교 관리자 순으로 알림을 전송하는 방식이 있다. 반대로, 가해자가 무기를 소지하거나 위협 동작을 반복하는 경우, 보안 인력 → 관리자 → 경찰 순으로 알림이 전송되며, 피해자 쪽 알림은 그 이후에 이뤄질 수 있다.

[0167] 장치(30)는 다양한 위험 상황에서 보안 대응 리소스를 적재적소에 배분하고, 사건의 진행 흐름에 따라 적절한 개입 우선순위를 실현할 수 있도록 한다. 장치(30)는 AI 기반 판단 모델을 통해 이 순서를 실시간 갱신할 수 있으며, 특정 상황에서는 병렬 전송이나 반복 전송 기능도 연계할 수 있다.

[0168] S309 단계에서, 장치(30)는 알림 범위 및 알림 순서에 따라 보안 알림을 생성하여 제공할 수 있다.

[0169] 장치(30)는 알림 대상에 따라 알림 내용을 달리 구성할 수 있다. 예를 들어, 피해자 보호자에게는 피해 위치와 상태, 대처 방법이 포함된 안내 메시지를, 보안 인력에게는 가해자의 특징, 이동 경로, 현재 위치 등이 포함된 대응 지시를 포함할 수 있다.

[0170] 알림 형식은 문자 메시지, 음성 통화, 모바일 푸시 알림, 전광판 안내, 앱 기반 실시간 지도 오버레이 등으로 다양화될 수 있다.

[0171] 실시예에 따르면, 피해자가 인근 공공시설 내에서 위협을 당한 경우, 장치(30)는 알림 순서에 따라 경찰 112 시스템과 연동하여 음성 및 문자 알림을 발송하고, 동시에 피해자 보호자에게 앱 기반 실시간 위치 공유 메시지를 전송할 수 있다. 또한, 상황이 확산되는 경우, 공간 내 일반 사용자에게는 회피 경로를 포함한 시각적 알림이 제공될 수 있다.

[0172] 이 단계는 전체 보안 시스템의 작동 효과성을 결정짓는 핵심이며, 불필요한 경보는 줄이고 필요한 대상에게 빠르게 정확한 정보를 전달함으로써 위협 대응의 품질을 높인다.

[0173] 장치(30)는 상황 변화에 따라 재전송, 전송 우선순위 재조정, 반복 알림 설정 등을 수행할 수 있다.

[0174] 한편, 장치(30)는 위협 행위가 감지된 환경의 모니터링 영상을 제공할 수 있다. 이를 통해 사용자는 위협 발생 시점의 현장 상황을 직관적으로 확인할 수 있으며, 보안 요원 또는 관리자에게는 사건의 정황을 신속히 파악하고 정확한 대응 결정을 내릴 수 있는 기반을 제공할 수 있다. 또한, 장치(30)는 영상에 대한 실시간 또는 사후 접근을 통해 증거 확보, 사후 분석, 보고서 작성 등 다양한 보안 목적에 활용될 수 있어 위협 대응의 효율성과 신뢰성을 동시에 높일 수 있다.

[0175] 이때, 모니터링 영상을 제공하는 과정에 대한 자세한 설명은 도 4를 참조하여 후술하기로 한다.

[0176] 도 4는 일실시예에 따른 위협 행위가 감지된 환경의 모니터링 영상을 제공하는 과정을 설명하기 위한 순서도이다.

[0177] 도 4를 참조하면, 먼저 S401 단계에서, 장치(30)는 위협 행위가 감지된 공간의 영상을 획득하고, 위협 행위가 감지된 시점을 기준으로 사용자의 위험 지수에 따라 결정된 공간 범위만큼 모니터링 영상을 추출할 수 있다.

[0178] 장치(30)는 전체 감시 영상 중에서 보안 대응에 실제로 필요한 시공간 구간만을 자동으로 선별하여 제공함으로써, 분석 효율성과 프라이버시 보호를 동시에 확보하고자 한다.

[0179] 장치(30)는 CCTV, 3D 카메라, IoT 감시 장치 등과 연동하여 특정 시간대의 공간 영상을 수집하며, 위협 행위가 감지된 사용자(가해자 또는 피해자)의 위험 지수(행동 강도, 반복성, 공격성 등)를 기반으로 영상 범위를 설정할 수 있다.

[0180] 장치(30)는 위험 지수가 높을수록, 시점 전후로 더 넓은 시간 간격과 공간 범위를 포함하는 영상을 추출하며, 이 범위는 실시간 또는 사후 판단으로 가변 설정 가능하다.

[0181] 예를 들어, 피해자의 위험 지수가 낮은 경우, 장치(30)는 위협 감지 시점 ±5초, 반경 3미터 이내의 영상만 추출할 수 있으며, 가해자의 위험 지수가 높고 주변 반응이 급격하게 변화한 경우에는 ±20초, 반경 10미터까지 확장된 영상이 추출된다. 이처럼 영상의 시공간 범위는 정적이지 않고, 위험성 평가에 따라 유동적으로 조정될 수 있다.

[0182] 장치(30)는 과도한 영상 노출로 인한 개인정보 유출을 방지하고, 보안 담당자의 분석 시간을 단축시킬 수 있으며, 필요 시 자동 편집된 증거 영상으로 저장하거나 실시간 스트리밍이 가능하다. 또한, 장치(30)는 영상 압축, 전처리, 익명화 모듈과 연계하여 해당 영상에 블러링, Skeleton 변환 등의 전처리를 병행할 수 있다.

[0183] 장치(30)는 수집한 모니터링 영상을 데이터베이스에 저장할 수 있다.

[0184] S402 단계에서, 장치(30)는 위협 행위가 감지된 이후, 주변 사용자의 주요 사용자에 대한 관심도의 변화를 확인할 수 있다.

[0185] 장치(30)는 위협 상황 발생 이후 현장 내 분위기와 위험도 변화를 실시간으로 파악하여, 후속 대응 조치를 정밀하게 조정할 수 있도록 하고자 한다. 특히, 관심도 변화는 위협 상황이 진정되고 있는지 또는 확산되고 있는지를 판단하는 핵심 기준이 된다.

[0186] 장치(30)는 카메라 및 마이크 기반 센서 데이터를 통해 주변 사용자들의 시선 방향, 음성 반응, 행동 패턴을 지속적으로 분석할 수 있다. 시선 방향 분석은 눈동자 추적 또는 머리의 회전 방향을 기반으로 수행되며, 음성 데이터는 발화 위치, 크기, 감정 상태를 포함하여 감지된다. 또한, 주변 사용자의 접근 또는 이탈 움직임, 자세 변화 등을 실시간으로 추적하여 누가 주요 사용자(가해자 또는 피해자)에게 관심을 가지는지 판단할 수 있다.

[0187] 예를 들어, 위협 행위 이후 특정 사용자가 쓰러진 피해자 주변으로 사람들이 몰리고, 시선과 음성이 피해자에게 집중된다면, 장치(30)는 피해자에 대한 관심도가 증가하는 것으로 판단할 수 있다. 반면, 사람들이 가해자를 향해 경계하거나 멀어지는 경우, 가해자에 대한 관심도 증가로 판단될 수 있다. 이러한 변화는 일정 시간 간격(예: 5초 단위)으로 갱신되며, 상황의 추세를 분석할 수 있다.

[0188] 관심도 변화 분석은, 영상 내 강조 대상 설정(Skeleton 애니메이션), 보안 알림 우선순위 결정, 회피 경로 안내, 증거 영상 편집 기준 등 다양한 후속 시스템에 영향을 준다.

[0189] 장치(30)는 해당 데이터를 시간축에 따라 시각화하여, 관리자나 분석자가 판단 흐름을 직관적으로 파악할 수 있도록 지원할 수 있으며, AI 기반 상황 인식 모델과 연동하여 향후 위협 재발 가능성 예측에도 활용할 수 있다.

[0190] S403 단계에서, 장치(30)는 확인 결과로부터 주변 사용자 및 주요 사용자를 변환할 수 있다.

[0191] 장치(30)는 위협 행위가 발생한 이후, 보안 상황을 정밀하게 분석하는 동시에 당사자 및 관련자들의 신체 정보와 얼굴 등의 민감한 시각 정보를 보호하고자 한다. 특히, 사용자의 신체 형상, 표정, 복장, 성별, 체형 등 개인 식별이 가능한 영상 정보를 그대로 노출하는 것은 사생활 침해나 2차 피해로 이어질 수 있으므로, 장치(30)는 이러한 요소를 제거한 Skeleton 기반 시각 정보 처리 방식을 적용함으로써, 보안성과 프라이버시를 보호할 수 있다.

[0192] 장치(30)는 확인 결과로부터 주요 사용자에 대한 관심도가 감소한 경우, 사용자의 모션 데이터를 3D 좌표 데이터로 변환하고, 3D 좌표 데이터를 이용하여 신체 특징이 포함되지 않은 스켈레톤(Skeleton) 기반 형상으로 변환

할 수 있다.

[0193] 장치(30)는 주요 사용자에 대한 관심도가 감소한 경우, 해당 사용자의 모션 데이터를 영상 프레임 기준으로 분석하여, 관절 단위의 좌표를 포함하는 3D 포인트 데이터로 변환할 수 있다. 이때 사용자의 얼굴, 복장, 배경 등의 원영상 정보는 제외되며, 어깨, 팔꿈치, 손목, 무릎, 발목 등 주요 관절의 위치 정보만 추출된다.

[0194] 3D 좌표는 일반적으로 X, Y, Z 축 기준으로 정의되며, 프레임별 시간 정보를 포함하여 구성된다. 장치(30)는 이러한 좌표 데이터를 기반으로, 각 관절 간 연결 구조를 생성하고, 신체 형상과 비식별화된 인체 표현인 Skeleton 구조로 시각화할 수 있다.

[0195] 장치(30)는 변환된 스켈레톤 데이터를 애니메이션화하여 주변 사용자 및 주요 사용자를 변환할 수 있다.

[0196] 예를 들어, 피해자에 대한 주변 사용자의 관심도가 급감한 경우, 장치(30)는 해당 피해자의 영상에서 인물 실루엣을 제거하고, 움직임만을 유지한 Skeleton 형태로 대체할 수 있다.

[0197] 이때 장치(30)는 Skeleton 구조를 시간 순서에 따라 연결하여 애니메이션화하고, 가해자, 주변 사용자 등과의 상호작용도 동시에 표현되도록 한다. 이 애니메이션은 사건 당시의 이동 경로, 동작 강도, 회피 동작 등을 직관적으로 파악할 수 있게 하며, 영상 내 시각적 집중을 높이기 위해 관절 선의 굵기나 색상, 움직임 선명도 등도 동적으로 조절할 수 있다.

[0198] 장치(30)는 확인 결과로부터 주요 사용자에 대한 관심도가 유지되는 경우, 주변 사용자를 관심도에 반비례하도록 결정된 변환 정도에 따라 변환하고, 주요 사용자는 변환하지 않을 수 있다.

[0199] 장치(30)는 사용자별 관심도 점수를 시간 단위 또는 프레임 단위로 계산하며, 주변 사용자에 대해서는 이 관심도 값이 낮을수록 Skeleton 또는 Blur, 픽셀화 등으로 변환 강도를 높이도록 구성할 수 있다.

[0200] 반면, 주요 사용자(가해자 또는 피해자)는 분석 또는 상황 이해에 핵심적인 인물이므로 변환하지 않고 원영상으로 유지한다. 이때 변환 강도는 선형 비례, 구간별 단계적 변환, 또는 가중치 기반 곡선 모델로 설정될 수 있다.

[0201] 예를 들어, 피해자에 대한 주변의 관심이 일정 수준으로 유지되는 경우, 장치(30)는 피해자를 그대로 영상에 표시하고, 그 외 사용자(예: 방관자, 지나가던 인물 등)는 시선이나 반응 수준이 낮은 순서대로 Skeleton 형태로 변환하거나 얼굴을 블러 처리하여 정보 노출을 제한할 수 있다. 특히 관심도가 10점 만점 중 2점 이하인 사용자는 완전 Skeleton화하고, 5점 이하인 경우에는 얼굴만 모자이크 처리하는 방식으로 계층적 표현이 가능하다.

[0202] 이와 같은 방식은 영상 시각화의 효율성과 정보 집중도를 높이면서도 관계없는 다수 사용자에 대한 개인정보 노출을 최소화할 수 있는 장점이 있다.

[0203] 장치(30)는 정책 설정 또는 AI 분석 목적에 따라 변환 알고리즘을 선택적으로 적용할 수 있으며, 필요 시 변환 정도를 시각화한 범례나 색상으로 표현하여 분석자에게 직관적인 이해를 제공할 수도 있다.

[0204] 장치(30)는 확인 결과로부터 주요 사용자에 대한 관심도가 증가한 경우, 주변 사용자 및 주요 사용자를 모두 변환하지 않을 수 있다. 관심도가 증가하는 경우에는 주변 사용자 및 주요 사용자 모두를 그대로 유지하여 영상 정보를 완전하게 보존할 수 있다.

[0205] 이는 현장의 위협 상황이 심각하거나 주목도가 급격히 증가하고 있는 상황으로 판단되는 경우로, 사건의 전체 흐름을 상세히 분석하고 증거로서의 영상 완전성을 확보하기 위한 판단이다.

[0206] 이때 장치(30)는 영상 내 모든 사용자(주요 및 주변)를 변형 없이 원형 그대로 유지하며, 고해상도 기반의 시각 정보를 그대로 보존할 수 있다.

[0207] 관심도 증가의 판단 기준은 시선 집중도 상승률, 주변 사용자의 언어 감정 변화, 사용자 이동 궤적 수렴 여부 등 다양한 요소를 종합적으로 고려하여 산출되며, 일정 임계값 이상일 때 영상 정보 비변환 원칙을 적용한다.

[0208] 예를 들어, 위협 상황 이후 피해자 주위로 다수의 사용자가 몰려들고, 시선과 음성이 집중되며, 보호 및 응급 반응이 급증하는 경우, 장치(30)는 해당 시점에서 Skeleton 또는 Blur를 적용하지 않고, 모든 사용자에 대한 상세 시각 정보를 보존한다. 이 영상은 사후 분석, 법적 증거, 관리자 보고에 사용될 수 있으며, 보안 기록 장치 또는 서버에 암호화 저장될 수 있다.

[0209] 장치(30)는 이와 같은 변환 배제 조건에서도 영상 접근 권한 제어, 암호화, 요청 승인 절차 등을 통해 정보 유

출 방지 기능을 병행할 수 있다.

[0210] 나아가, 사용자 요청에 따라 선택적으로 복원형 영상(Skeleton → 원형 복구)을 제공할 수 있는 옵션도 연동 가능하다. 이를 통해 본 발명은 보안성과 프라이버시 보호, 정밀 분석이라는 다중 요구를 모두 충족시키는 유연한 영상 처리 기술을 제공할 수 있다.

[0211] S404 단계에서, 장치(30)는 위협 행위가 감지된 공간의 보안 수준을 결정할 수 있다.

[0212] 구체적으로, 장치(30)는 위협 행위가 감지된 공간의 위협 행위 감지 횟수, 위험 행위 감지 빈도, 위협 행위 지속 시간, 보안 기관까지의 거리, 주변 보안 기관의 개수 및 유동인구 수를 확인하여 공간의 보안 수준을 결정할 수 있다.

[0213] 일실시예에 따르면, 장치(30)는 위협 행위가 감지된 공간의 보안 수준을 산출하기 위해, 해당 공간 내에서 기록된 위협 행위의 누적 감지 횟수와 시간 단위당 위험 행위 감지 빈도, 각 위협 행위의 지속 시간 정보를 로그 데이터 또는 이벤트 발생 기록으로부터 분석할 수 있으며, 동시에 GPS 또는 공간 매핑 정보를 기반으로 인근 보안 기관(예: 경찰서, 보안 요원 근무소 등)까지의 직선 거리 및 주변 반경 내 보안 기관의 개수를 계산하고, 공간 내 유동인구 수는 센서 기반 인원 계수 시스템 또는 카메라 기반 객체 인식 알고리즘을 통해 산정함으로써, 이들 요소를 종합하여 보안 수준을 정량적으로 평가할 수 있다.

[0214] 장치(30)는 단순히 위협 행위가 발생했다는 사실만으로 판단하지 않고, 해당 공간의 과거 위험 이력, 인프라 대응 가능성, 인구 밀도 등을 종합적으로 고려하여, 공간 자체의 위험성과 대응 취약성을 정량적으로 평가하고자 한다. 이를 통해 공간 특성에 맞는 맞춤형 보안 알림 전략, 영상 처리 강도 등을 유연하게 설정할 수 있다.

[0215] 장치(30)는 해당 공간에서 감지된 위협 행위의 누적 횟수, 최근 일정 기간 내 발생 빈도, 각 사건의 지속 시간, 인근 보안 기관까지의 거리, 인근 보안 기관 수(예: 경찰서, 보안실 등), 그리고 평균 유동 인구 수 등을 확인하여 보안 수준을 산출할 수 있다. 이때 각 요소는 가중치가 부여된 수치로 정규화되어 0~1 또는 0~100 단위의 보안 등급(score)으로 변환될 수 있다. 예컨대 위협이 잦고 보안 인프라가 멀리 있으며, 인구 밀도가 높은 공간은 낮은 보안 수준으로 평가된다.

[0216] 예를 들어, 도시 중심부의 공공광장에서 최근 30일 동안 위협 행위가 5회 이상 감지되고, 경찰서까지의 거리가 800m 이상이며, 유동 인구가 시간당 500명 이상이라면, 장치(30)는 해당 공간의 보안 수준을 “낮음”으로 평가할 수 있다. 반면, 학교 내부에서 발생했으나 과거 위험 이력이 거의 없고 보안실이 50m 이내에 있는 경우, “높음” 보안 수준으로 설정될 수 있다.

[0217] 장치(30)는 보안 수준을 영상 처리 단계(블러 강도, Skeleton 적용 여부), 경보 범위 설정, 사용자 알림 방식 등에 유동적으로 반영할 수 있다. 또한, 공간별 보안 수준 데이터는 장기적으로 누적 관리되어, 향후 특정 공간의 보안 취약 구역 자동 식별, 보안 요원 재배치, 순찰 경로 최적화 등 보안 시스템 전체 최적화에도 활용될 수 있다.

[0218] S405 단계에서, 장치(30)는 위협 행위가 감지된 시점에서 멀어질수록 블러 강도를 줄이되, 공간의 보안 수준을 고려하여, 블러 강도에 보안 수준에 기반하여 결정된 가중치를 적용하여 블러 강도를 조정할 수 있다.

[0219] 장치(30)는 위협 상황이 촬영된 영상 내에서 시간적 거리와 공간적 거리, 그리고 공간의 보안 민감도에 따라 비식별 처리 강도를 정밀하게 조정할 수 있다.

[0220] 장치(30)는 위협 감지 시점을 중심으로 시간 간격(예: ±10초)과 공간 반경(예: 10미터 이내)을 설정하고, 이 범위를 벗어나는 시점·구역으로 갈수록 블러 강도를 점진적으로 약화시킨다.

[0221] 이때 보안 수준이 낮은 공간일수록 강한 블러를 더 넓은 범위에 적용하며, 반대로 보안 수준이 높은 공간에서는 블러 범위를 좁히고 세기 또한 약하게 적용한다. 블러 강도는 선형, 지수, 로그, S-커브 등의 수학적 함수 기반으로 조정될 수 있다.

[0222] 실시예로, 쇼핑몰 내에서 위협 사건이 발생한 경우, 사건 발생 직후 10초 이내·반경 5미터 내 인물과 배경은 강한 블러를 적용하고, 30초 이후·15미터 이상 떨어진 배경은 블러 강도를 최소화하거나 제거할 수 있다. 그러나 동일 조건이라도 공간 보안 수준이 "낮음"으로 평가된 경우, 블러 범위는 30미터 이상으로 확대되고, 시간 범위 역시 ±60초로 늘어날 수 있다.

[0223] 이러한 방식은 사건과 무관한 주변 사용자의 개인정보 보호는 강화하면서도, 핵심 정보가 포함된 시공간 범위만을 효과적으로 강조하는 시각적 필터링을 가능하게 한다.

[0224] 장치(30)는 영상 내 시계열 정보, 객체 움직임, 카메라 시점 이동 등과 연동하여 블러 강도를 세밀하게 보간할 수 있으며, 관리자 설정 또는 자동 조정 옵션으로 운영될 수 있다.

[0225] S406 단계에서, 장치(30)는 블러 강도를 모니터링 영상의 배경 부분에 적용할 수 있다.

[0226] 장치(30)는 보안 분석 및 보고용으로 제공되는 모니터링 영상에서 사건 중심 인물 및 객체는 시각적으로 강조하고, 배경은 흐림 처리하여 정보 집중도와 프라이버시 보호를 동시에 달성하고자 한다.

[0227] 배경 블러는 영상 전체가 아닌 '사건과 무관한 시각 요소'를 제거 또는 약화시키기 위함이다.

[0228] 장치(30)는 앞서 계산된 블러 강도와 위치 정보를 바탕으로, 영상 프레임마다 배경 객체를 인식하고 해당 영역에 블러 효과(예: Gaussian Blur, Box Blur, Motion Blur 등)를 적용할 수 있다.

[0229] 배경 객체는 AI 기반 분할(segmentation) 또는 인물 추출 기술을 통해 인물과 분리되며, 사건 중심 인물(가해자·피해자)은 제외 대상으로 지정된다. 또한, 움직임이 거의 없는 정적 객체(예: 벽, 창문, 가구 등)는 블러 우선 적용 대상이 된다.

[0230] 예를 들어, 위협 행위가 발생한 교실에서 책상과 벽, 다른 학생들의 책가방 등은 블러 처리되지만, 가해자와 피해자의 실루엣, 동작, 표정은 선명하게 유지된다. 주변 사용자 중 관심도가 낮은 인물의 경우는 블러 또는 Skeleton으로 처리되며, 공간 전체가 흐려지지 않도록 중심 영역은 상대적으로 강조될 수 있다.

[0231] 이 단계는 사건 분석 시 핵심 행위와 배경 요소를 구분하는 데 큰 도움을 주며, 분석자의 시각 피로를 줄이고 판단 효율을 높이는 시각적 최적화 도구로 작용할 수 있다. 장치(30)는 블러 적용 범위를 관리자 UI를 통해 조정할 수 있도록 하거나, 자동 블러 제외 영역을 설정하여 사용자 정의형 보안 영상을 생성할 수도 있다.

[0232] 도 5는 일실시예에 따른 음성 데이터를 기반으로 모니터링 영상을 제공하는 과정을 설명하기 위한 순서도이다.

[0233] 도 5를 참조하면, 먼저 S501 단계에서, 장치(30)는 음성 센서로부터 공간 내 사용자의 음성 데이터를 획득하고, 음성 데이터를 분석하여 키워드를 추출할 수 있다.

[0234] 장치(30)는 공간 내 설치된 마이크로폰, 음성 센서 또는 스마트 디바이스의 음성 입력 인터페이스를 통해 특정 시간 동안의 다채널 음성 데이터를 수집할 수 있으며, 해당 데이터에 대해 음성 인식 엔진(STT: Speech-to-Text) 또는 자연어 처리(NLP) 기술을 적용하여 실시간으로 텍스트로 변환하고, 이 중 자주 등장하거나 의미 있는 단어를 키워드로 식별할 수 있다. 키워드 추출에는 음성 볼륨, 반복 횟수, 음절 강조도, 감정 톤 등이 반영될 수 있다.

[0235] 예를 들어, 공간 내에서 사용자가 "살려주세요", "하지 마", "폭력", "무서워" 등의 단어를 반복적으로 언급한 경우, 장치(30)는 해당 음성을 텍스트로 변환한 후 이를 키워드 후보로 등록하고, 추출된 키워드는 이후 단계에서 분석 및 분류 대상으로 사용된다. 발성자의 위치나 발화 방향도 병행 수집되어 특정 인물 또는 구역과 연동될 수 있다.

[0236] 장치(30)는 비정상적인 언어 반응을 조기에 포착함으로써, 움직임 기반의 위협 탐지보다 빠른 사전 경보 판단이 가능하게 하며, 시각적 분석이 제한되는 환경(야간, 장애물 존재 등)에서도 음성 기반 보안 감지가 유효하게 작동할 수 있도록 한다. 다양한 언어 모델, 방언 지원, 소음 환경에서의 노이즈 필터링 기술과 연계하여 범용성도 확보할 수 있다.

[0237] S502 단계에서, 장치(30)는 키워드가 미리 설정된 기준 이상으로 언급된 것에 해당하는 키워드를 주의 키워드로 분류할 수 있다. 이때, 미리 설정된 기준은 실시예에 따라 상이하게 설정될 수 있다.

[0238] 공간 내 다수의 발화 중에서도 보안 위협 또는 위험 상황과 직접 관련된 고위험성 키워드를 선별하는 과정으로, 이후 음성 데이터 저장, 영상 재생, 경보 연동 등에 중요한 판단 기준으로 작용한다.

[0239] 일실시예에 따르면, 장치(30)는 이전 단계에서 추출된 키워드 리스트에 대해, 시간 내 반복 빈도, 강세(발화 볼륨), 동시 발화자 수, 사용된 문맥 내 감정 표현, 키워드 목록 내 위험도 점수를 기반으로 해당 키워드의 위험 우선순위를 평가할 수 있다. 미리 설정된 기준은 정량적 값(예: 10초 내 3회 이상 등장, 평균 볼륨 80dB 이상 등) 또는 머신러닝 기반 유연 기준으로 설정될 수 있다.

[0240] 예를 들어, "위험해"라는 단어가 15초 이내에 서로 다른 두 사용자에게서 각각 2회 이상 반복적으로 발화되었고, 감정 분석 결과 부정 감정이 동반된 경우, 장치(30)는 이를 주의 키워드로 분류할 수 있다. 반면, 단발성 발화이거나 농담·일상 대화 문맥에서 발생한 유사 단어는 제외될 수 있다.

[0241] 이 단계는 오탐 방지를 위한 키워드 필터링, 알림 남용 최소화, 실제 위협과 무관한 상황에서의 자동 판단 억제에 효과적이며, 장치(30)는 상황에 따라 다르게 반응할 수 있는 키워드를 관리자가 직접 등록하거나, 인공지능이 현장 로그에 따라 학습하도록 구성할 수도 있다.

[0242] S503 단계에서, 장치(30)는 주의 키워드가 등장하는 경우, 주의 키워드가 등장하는 시점부터 주의 키워드의 언급 횟수 및 공간 내 사용자의 현재 위치에 해당하는 구역의 사용자 밀도에 기반하여 결정된 음성 추출 길이만큼 음성 데이터를 추출할 수 있다.

[0243] 장치(30)는 위협 상황과 관련된 대화 또는 감정 반응을 포함하는 음성 구간을 필요한 길이만큼 정확하게 잘라내어 저장 또는 재생 대상으로 지정하고자 한다.

[0244] 장치(30)는 주의 키워드가 감지된 시점을 시작점으로 하여, 이후 일정 시간 간격 동안 반복 언급 여부, 사용자 밀도(혼잡도 또는 시끄러운 정도), 구역 내 반향 정도 등을 고려해 최적의 추출 구간 길이(T길이)를 결정할 수 있다. 예를 들어, 밀집 구역에서는 짧은 시간 내 다수의 발화가 집중되므로 추출 구간이 짧아질 수 있고, 조용한 공간에서는 긴 대화를 보존할 수 있다.

[0245] 실시예에 따르면, “도와주세요”라는 키워드가 3초 간격으로 3회 이상 반복되고, 해당 구역의 사용자 밀도가 높아 주변 잡음이 많은 경우, 장치(30)는 노이즈 필터링을 고려한 6초 구간만을 추출하도록 설정할 수 있다. 반면, 동일 키워드가 비교적 조용한 공간에서 명확하게 2회 이상 들렸다면, 장치(30)는 10~12초 구간을 추출해 보존할 수 있다.

[0246] 이 방식은 전체 음성 녹음 대신 사건 관련 정보만을 압축적으로 보관함으로써 저장 공간을 절약하고, 모니터링 및 분석 시 불필요한 데이터 탐색 부담을 줄여 업무 효율성을 높인다. 또한, 추출 구간에 음성 감정 태그, 시점 정보, 발화자 위치 정보 등을 메타데이터로 함께 저장할 수도 있다.

[0247] S504 단계에서, 장치(30)는 모니터링 영상에 추출된 음성 데이터를 함께 재생되도록 제어할 수 있다.

[0248] 장치(30)는 추출된 음성 구간의 시작 및 종료 시점을 해당 모니터링 영상의 타임라인과 정렬(synchronization)시킨 후, 영상 재생 시 해당 음성을 동시에 출력하도록 설정할 수 있다. 재생은 단일 채널 또는 스테레오 출력으로 구성되며, 영상의 주요 사용자가 누군지에 따라 좌우 채널 분리, 사용자별 발화 추적 기능도 함께 제공될 수 있다.

[0249] 예를 들어, 피해자가 “무서워, 저 사람 이상해”라고 말한 음성이 영상의 1분 35초~1분 40초 구간에서 추출되었다면, 장치(30)는 영상이 1분 35초로 도달했을 때 해당 음성을 동시에 재생한다. 사용자가 영상을 일시 정지하거나 되감기할 경우에도 해당 음성은 정확하게 연동되어 재생된다.

[0250] 장치(30)는 분석자 또는 관리자에게 사건 당시의 정황과 감정 상태를 더 직관적으로 전달하며, 법적 판단이나 사후 대응에도 핵심 증거로 활용될 수 있다. 또한, 음성과 영상이 완벽히 동기화된 경우, 자동 보고서 생성이나 AI 기반 영상 요약 기능과도 연계될 수 있다.

[0251] S505 단계에서, 장치(30)는 음성 데이터에서 소리의 세기가 미리 설정된 기준 세기 미만인 경우, 음성 데이터를 텍스트 데이터로 변환하여 생성된 자막을 모니터링 영상에 표시할 수 있다. 이때, 미리 설정된 기준 세기는 실시예에 따라 상이하게 설정될 수 있다.

[0252] 장치(30)는 음성의 볼륨이 낮거나 잡음으로 인해 청취가 어려운 경우, 중요한 발화를 놓치지 않도록 자막으로 보완을 제공할 수 있다.

[0253] 장치(30)는 소리의 세기(dB)가 설정된 기준치(예: 60dB) 미만인 경우, 해당 구간의 음성 데이터를 STT(speech-to-text) 엔진을 통해 실시간 텍스트로 변환하고, 영상 하단 또는 발화 위치 근처에 자막 형태로 출력할 수 있다. 이때 텍스트 출력은 시간 코드에 동기화되며, 말한 인물의 위치에 따라 자막 위치를 동적으로 조절하는 것도 가능하다.

[0254] 예를 들어, 한 사용자가 속삭이듯 “제발, 말하지 마”라고 말했지만 볼륨이 낮아 들리지 않는 경우, 장치(30)는 이를 텍스트로 변환하여 영상 하단에 “제발, 말하지 마”라는 자막을 표시할 수 있다. 자막은 발화자의 ID나 색상 코드로 구분되며, 동시 발화 시 다중 자막이 분할되어 표시될 수도 있다.

[0255] 장치(30)는 청각적 분석의 한계를 보완하고, 음성 증거를 텍스트화하여 기록 가능하도록 하며, 영상 열람자에게 높은 가독성과 분석 정확성을 제공할 수 있다. 자막 표시 여부는 설정에 따라 자동, 수동 또는 상황 인식 기반

으로 전환될 수 있으며, 여러 언어로 실시간 번역된 다중 자막 출력도 지원 가능하다.

[0256] 도 6은 일실시예에 따른 안전 이동 경로를 생성하여 제공하는 과정을 설명하기 위한 순서도이다.

[0257] 도 6을 참조하면, 먼저 S601 단계에서, 장치(30)는 위협 행위가 감지된 공간에서 미리 설정된 기준 거리 내의 주변 구역에 존재하는 사용자 중 주변 사용자 및 주요 사용자를 제외한 근접 사용자를 추출할 수 있다. 이때, 미리 설정된 기준 거리는 실시예에 따라 상이하게 설정될 수 있다.

[0258] 장치(30)는 위협 발생 이후, 직접적인 관련은 없지만 잠재적으로 위험에 노출될 가능성이 있는 일반 사용자를 식별하여 사전 대응 정보를 제공할 수 있다.

[0259] 장치(30)는 위협이 발생한 위치를 기준으로, 공간 상에 설정된 반경(R미터) 내에 존재하는 사용자들의 위치 데이터를 수집하며, 해당 사용자 중 이미 분석된 주요 사용자(가해자·피해자) 및 관심도 기반의 주변 사용자를 제외한 인원을 근접 사용자로 분류한다. 기준 거리는 환경 특성, 장소 유형(예: 학교, 역, 공항 등), 공간 크기 등에 따라 다양하게 설정될 수 있다.

[0260] 예를 들어, 10미터 반경 내에서 위협 행위가 발생했을 때, 장치(30)는 이 반경 내에서 식별된 사용자 중에서 위험 반응이나 관심이 감지되지 않은 사용자 3명을 근접 사용자로 추출할 수 있다. 이들은 직접적인 관련은 없지만, 위협 확산 시 가장 먼저 영향을 받을 수 있는 대상이다.

[0261] 이 단계는 실시간 회피 안내, 알림 전송, 회선 분산 유도 등 사전 안전 대응 체계를 구성하는 핵심 구성으로, 군중 속 개별 사용자를 선별적으로 관리하기 위한 기술 기반이 된다. 또한, 장치(30)는 이 추출 정보를 후속 단계에서 안전 경로 안내, 회피 우선순위 설정 등으로 활용할 수 있다.

[0262] S602 단계에서, 장치(30)는 근접 사용자의 단말(10)로부터 목적지에 대한 정보를 수신할 수 있다.

[0263] 장치(30)는 위험 발생 구역에 가까이 있는 사용자의 이동 목적과 방향을 확인함으로써, 경로 재설정 또는 위험 회피 안내의 기반 정보를 수집할 수 있다.

[0264] 장치(30)는 사용자의 단말(10)로부터 직접 입력된 목적지 정보(앱 입력, 예약 정보 등) 또는 단말의 위치 이력, 블루투스 비콘 정보, Wi-Fi 신호 강도 분석 등을 활용해 자동으로 목적지 추정 정보를 획득할 수 있다. 위치 기반 서비스(LBS) API와 연동하거나, 건물 내 실내 지도를 참조하여 구체적인 좌표로 환산할 수 있다.

[0265] 예를 들어, 특정 건물 내에서 근접 사용자가 “4층 도서관”을 목적지로 설정한 경우, 장치(30)는 이를 인식하고 해당 목적지를 포함하는 이동 경로 상에 현재 위협 구역이 포함되는지 여부를 분석한다. 만약 회피 지수가 높다면 다른 층을 경유하거나 시간차 이동을 권장할 수 있다.

[0266] 이 단계는 사용자 맞춤형 회피 경로 안내, 동선 분산, 이동 속도 예측 등 위협 대응과 사용자 경험을 동시에 향상시키는 안전 내비게이션 기능의 핵심으로 작용한다. 장치(30)는 목적지 민감도(어린이, 노약자 관련 공간)나 이동 시급성도 고려하여 안내 메시지의 긴급성도 조정할 수 있다.

[0267] S603 단계에서, 장치(30)는 근접 사용자와 주요 사용자 사이의 거리를 확인할 수 있다.

[0268] 장치(30)는 근접 사용자 및 주요 사용자의 실시간 위치 좌표를 기반으로, 유클리드 거리 또는 장애물 기반 실거리(실내 도면 경로 길이)를 계산할 수 있다. 또한, 이동 방향이나 속도를 고려해 예상 충돌 가능성 또는 예상 도달 시간도 산출할 수 있다.

[0269] 예를 들어, 위협을 가한 가해자와 직선 거리로 3.2m 떨어진 근접 사용자가 가해자 쪽으로 이동 중인 경우, 장치(30)는 해당 사용자에게 즉시 회피 경로 안내 또는 대기 메시지를 전송할 수 있다. 반대로, 이동 방향이 반대이거나 물리적으로 차단된 경우에는 경고 우선순위를 낮출 수 있다.

[0270] 이 단계는 인물 간 거리 외에도 구조물(벽, 문, 출입구) 정보와 연계하여 실제 회피 가능성과 경로 유효성을 판단하는 데 효과적이며, 비상 탈출 알고리즘, 우선 알림 분배 정책 등과 결합될 수 있다.

[0271] S604 단계에서, 장치(30)는 공간 내 위험 지수, 주요 사용자에 대한 관심도, 사용자의 밀도, 확인된 거리를 기반으로 공간의 회피 지수를 결정할 수 있다.

[0272] 장치(30)는 해당 위치에서 사용자들이 실제로 회피하거나 벗어나야 할 필요성이 어느 정도인지를 정량적으로 판단할 수 있다.

[0273] 장치(30)는 기존에 산출된 공간 위험 지수(위협 빈도, 지속 시간 등), 주요 사용자에 대한 주변 반응(집중도,

경계도), 구역 내 사용자 밀도(혼잡도) 및 특정 사용자와의 거리 등 다양한 요소를 통합 분석하여, 0~1 또는 등급 체계(예: Low/Medium/High)로 표현되는 회피 지수를 계산할 수 있다.

[0274] 예를 들어, 공간의 위험 지수가 0.8, 주변 사용자들의 관심도가 증가 중이며, 사용자 밀도가 70% 이상이고, 근접 사용자와 가해자 사이의 거리가 2m 이내인 경우, 장치(30)는 회피 지수를 "High"로 설정하고 즉각적인 회피 경로 안내, 경고 알림, 속도 제한, 공간 차단 등의 조치를 시작할 수 있다.

[0275] 장치(30)는 개별 사용자뿐 아니라 공간 단위로 위협 회피 정책을 제어할 수 있게 해 주며, 건물 내 AI 경로 제어 시스템, 스마트 시그널, 드론 순찰 등과 연동되어 동적인 안전 대응 체계를 완성하는 데 중요한 기술적 기반이 된다. 회피 지수는 지속 업데이트되어 실시간 판단에도 반영될 수 있다.

[0276] S605 단계에서, 장치(30)는 근접 사용자의 현재 위치, 목적지에 대한 정보, 공간의 회피 지수를 안전한 이동 경로를 생성하기 위해 학습된 인공지능 모델에 입력하여 근접 사용자의 안전 이동 경로를 출력할 수 있다.

[0277] 장치(30)는 단순한 최단 경로 안내가 아니라, 실시간 위협 상황과 공간 위험도까지 반영된 회피 중심의 동적 안전 경로를 생성할 수 있다.

[0278] 장치(30)는 사용자 위치(GPS 또는 실내 좌표), 목적지(수신된 목적지 정보), 공간 회피 지수(위협 강도, 밀도, 거리 등 포함)를 입력값으로 사용하고, 이를 경로 예측을 위해 미리 학습된 딥러닝 기반 모델에 입력할 수 있다.

[0279] 본 모델은 CNN, RNN, LSTM, 또는 GNN(Graph Neural Network)을 포함할 수 있으며, 학습 데이터로는 건물 구조, 이동 경로 로그, 위험도 분포 지도가 사용될 수 있다.

[0280] 예를 들어, 사용자가 1층 매장 A에서 3층 출구 B로 이동 중이며, 2층에서 위협 행위가 감지되어 회피 지수가 높은 경우, 장치(30)는 이를 인식하고 엘리베이터 대신 우회 계단을 경유하는 경로를 산출할 수 있다. 또한, 복수의 경로가 존재하는 경우에는 위험 회피율, 거리, 예상 소요 시간, 사용자 상태(어린이, 장애인 등)를 기준으로 가중치를 반영한 최적 경로를 추천할 수 있다.

[0281] 장치(30)는 안전한 이동 경로를 생성하기 위해, 근접 사용자의 현재 위치 정보, 목적지 정보, 공간 내 회피 지수를 포함한 다양한 입력 데이터를 인공지능 모델에 제공할 수 있다.

[0282] 입력 데이터에는 이외에도 사용자 밀도, 주요 사용자와의 거리, 예상 체류 시간, 층간 이동 정보, 경로 상의 위험 구간 등이 포함될 수 있으며, 이를 통해 장치(30)는 가장 위험 요소가 적고 효율적인 이동 경로를 출력 데이터로 생성할 수 있다. 출력은 점 또는 구간 단위로 구성된 이동 경로 좌표, 회피 권고 구간, 경유 지점, 정차 또는 대기 위치 등의 형태로 구성될 수 있다.

[0283] 장치(30)는 이러한 입력 데이터를 기반으로, 딥러닝 기반의 경로 예측 모델 또는 강화학습 기반의 회피 경로 최적화 모델을 활용하여 안전 경로를 생성하도록 구성될 수 있다.

[0284] 예를 들어, 장치(30)는 이동 경로 최적화를 위해 Graph Neural Network(GNN), LSTM(Long Short-Term Memory), Transformer 기반 경로 시퀀스 생성 모델, 또는 DQN(Deep Q-Network) 기반 강화학습 모델을 학습시킬 수 있다.

[0285] 학습에는 실제 공간 이동 로그, 위협 발생 이력, 사용자 회피 성공률, 공간 구조 정보 등이 포함되며, 지도 학습 또는 비지도 학습 방식이 모두 활용될 수 있다. 학습 과정에서는 위험 구간 회피율, 경로 길이 최소화, 도달 시간 안정성 등을 복합 목표로 설정하여 모델 성능을 향상시킬 수 있다.

[0286] 장치(30)는 학습된 인공지능 모델을 이용해, 사용자의 실시간 이동 상황과 공간 내 위험 요소를 반영한 개인화된 안전 이동 경로를 동적으로 생성할 수 있다.

[0287] 예컨대, 동일한 목적지를 가진 근접 사용자라 하더라도, 가해자와의 거리, 주변 밀도, 보행 속도에 따라 각기 다른 경로를 추천할 수 있으며, 상황 변화(위협 확산, 회피 경로 차단 등)가 발생할 경우 즉시 경로를 재계산할 수 있다.

[0288] 장치(30)는 해당 모델을 기반으로, 복수 사용자 간의 경로 간섭을 최소화하고, 단체 회피를 위한 그룹 이동 경로를 생성하거나, 사용자의 상태(노약자, 아동 등)에 따른 위험 민감도 조절도 가능하도록 구현할 수 있다.

[0289] 본 발명에 따른 인공지능 모델은 단순히 최단 거리 또는 고정된 회피 동선이 아닌,

[0290] 공간 내의 위험 지수, 사용자 밀도, 위협 주체와의 거리, 목적지 정보 등을 종합적으로 고려하여

[0291] 실시간으로 회피 경로를 동적으로 생성하므로, 사용자 개개인의 위치와 상황에 최적화된 안전 이동 경로 안내가 가능하다.

[0292] 다수의 사용자가 동시에 이동하는 환경에서도 경로 간 충돌을 최소화하고 효율적인 이동 분산이 가능하다.

[0293] AI 모델은 공간 내 복수 사용자의 위치 및 경로를 함께 고려하여 경로 간 중첩 가능성을 줄이고, 사용자 간 충돌이나 혼잡도를 방지하면서도 개별 회피율을 극대화하는 방향으로 경로를 조정하므로, 군중 환경, 대형 시설, 복잡한 구조 내에서도 체계적이고 안전한 사용자 분산 이동이 가능하다.

[0294] 장치(30)는 공간 구조나 위협 상황의 변화에 따라 경로를 자동으로 재계산하고, 적응형 회피 전략을 실현할 수 있다.

[0295] 본 발명은 고정된 회피 매뉴얼이 아닌, 학습된 모델에 의해 상황 변화(위협의 확산, 경로 차단 등)에 유연하게 반응하여 경로를 즉시 수정할 수 있으며, 위협의 심각도, 사용자 유형(노약자, 장애인 등), 시간대에 따른 밀도 변화 등을 반영함으로써 적응형·지능형 보안 대응 시스템 구현이 가능하다.

[0296] 이 방식은 단순한 고정형 이동 경로보다, AI 기반의 맞춤형 회피 경로 안내가 가능하므로, 위협 상황 대응뿐 아니라 평시 안전 관리에도 활용될 수 있다. 또한, 장치(30)는 생성된 경로에 회피 영역, 경고구간, 정차 추천지점 등의 메타정보도 포함하여 시각적·음성 안내에 활용할 수 있으며, 다중 사용자에 대해 충돌 없이 개별 경로를 동시 처리하는 것도 가능하다.

[0297] S606 단계에서, 장치(30)는 공간에 해당하는 지도 상에 안전 이동 경로를 표시하여 근접 사용자의 단말(10)로 제공할 수 있다.

[0298] 장치(30)는 생성된 안전 경로를 직관적으로 시각화하여 사용자에게 전달함으로써 실시간 회피 행동을 유도하고, 사용자 혼란을 최소화할 수 있다.

[0299] 장치(30)는 건물 내부 지도(도면 기반 또는 실시간 구축형), 실외 지리 기반 지도, 또는 증강현실 기반 공간 맵에 안전 이동 경로를 표시할 수 있다.

[0300] 경로는 색상(예: 녹색 안전 경로, 노란색 경고 경로), 라인 두께, 깜빡임, 속도 가이드 등으로 시각적 강조가 가능하며, 해당 정보는 사용자의 단말(10)로 전송되어 모바일 앱, 스마트워치, 디지털 키오스크, HUD(Head-Up Display) 등에 출력된다.

[0301] 예를 들어, 쇼핑몰 내부에서 위협 행위가 발생한 경우, 장치(30)는 1층에서 3층 출구까지의 회피 경로를 지도 위에 녹색 실선으로 표시하고, “우측 계단으로 이동 후 직진, 에스컬레이터 이용 자제” 등의 안내를 자막 또는 음성으로 함께 제공할 수 있다. 사용자가 경로를 이탈할 경우, 실시간 재안내도 가능하다.

[0302] 장치(30)는 사용자에게 공간 이해력을 향상시키고, 공황 상태에서의 행동 혼란을 방지할 수 있다. 특히, 스마트폰 또는 웨어러블 기기와 연계된 실시간 반응형 UI와 결합할 경우, 현장 내 자율 대응력을 향상시킬 수 있으며, 단체 이동 시에도 각자의 경로가 충돌하지 않도록 분산 안내를 수행할 수 있다.

[0303] 도 7은 일실시예에 따른 장치의 구성의 예시도이다.

[0304] 일실시예에 따른 장치(30)는 프로세서(31) 및 메모리(32)를 포함한다. 일실시예에 따른 장치(30)는 상술한 서버 또는 단말일 수 있다. 프로세서(31)는 도 1 내지 도 6을 통하여 전술한 적어도 하나의 장치들을 포함하거나, 도 1 내지 도 6을 통하여 전술한 적어도 하나의 방법을 수행할 수 있다. 메모리(32)는 상술한 방법과 관련된 정보를 저장하거나 상술한 방법이 구현된 프로그램을 저장할 수 있다. 메모리(32)는 휘발성 메모리 또는 비휘발성 메모리일 수 있다.

[0305] 프로세서(31)는 프로그램을 실행하고, 장치(30)를 제어할 수 있다. 프로세서(31)에 의하여 실행되는 프로그램의 코드는 메모리(32)에 저장될 수 있다. 장치(30)는 입출력 장치(도면 미 표시)를 통하여 외부 장치(예를 들어, 퍼스널 컴퓨터 또는 네트워크)에 연결되고, 데이터를 교환할 수 있다.

[0306] 이상에서 설명된 실시예들은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치, 방법 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수

목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0307] 실시예에 따른 방법은 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 실시예를 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0308] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0309] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

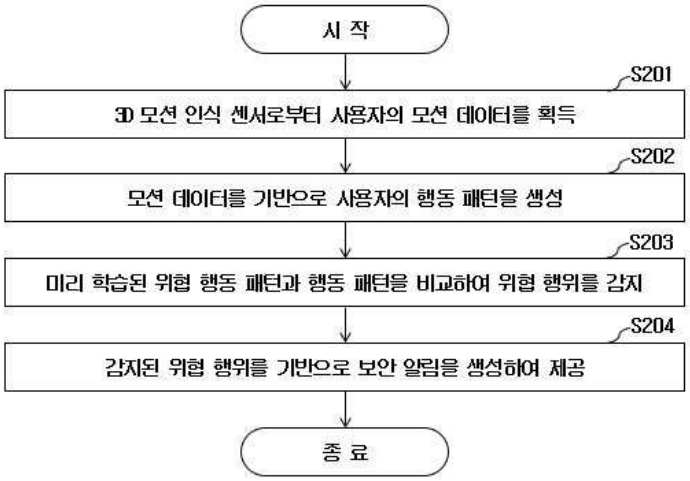
[0310] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

도면

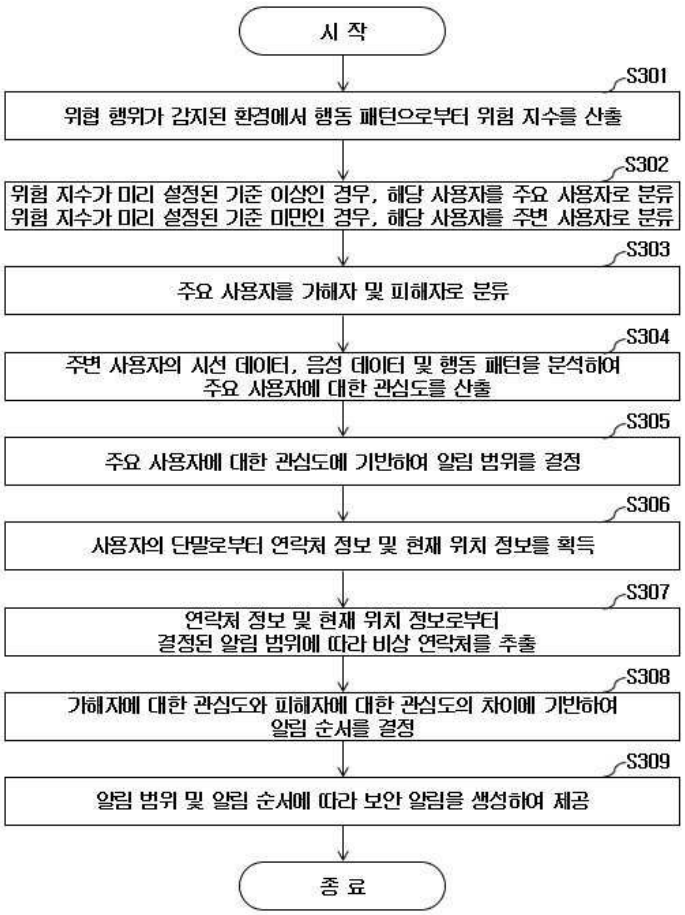
도면1



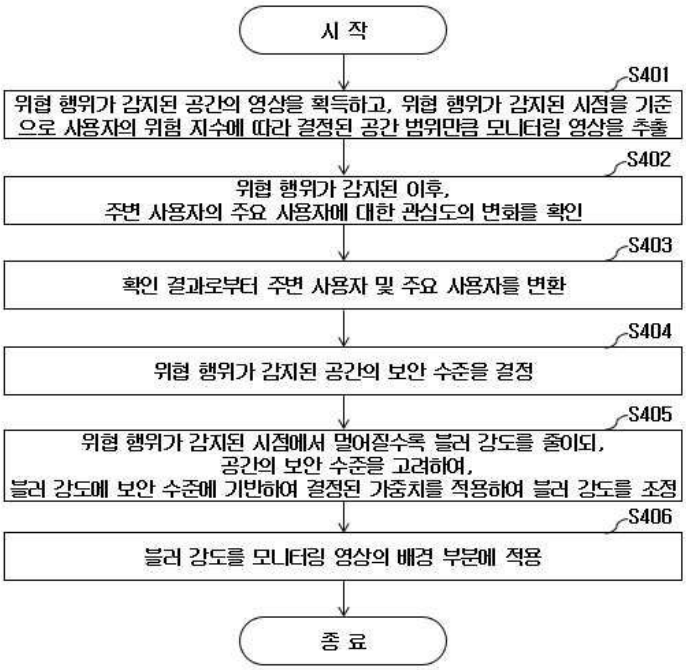
도면2


시 작
S201
3D 모션 인식 센서로부터 사용자의 모션 데이터를 획득
S202
모션 데이터를 기반으로 사용자의 행동 패턴을 생성
S203
미리 학습된 위협 행동 패턴과 행동 패턴을 비교하여 위협 행위를 감지
S204
감지된 위협 행위를 기반으로 보안 알림을 생성하여 제공
종 료

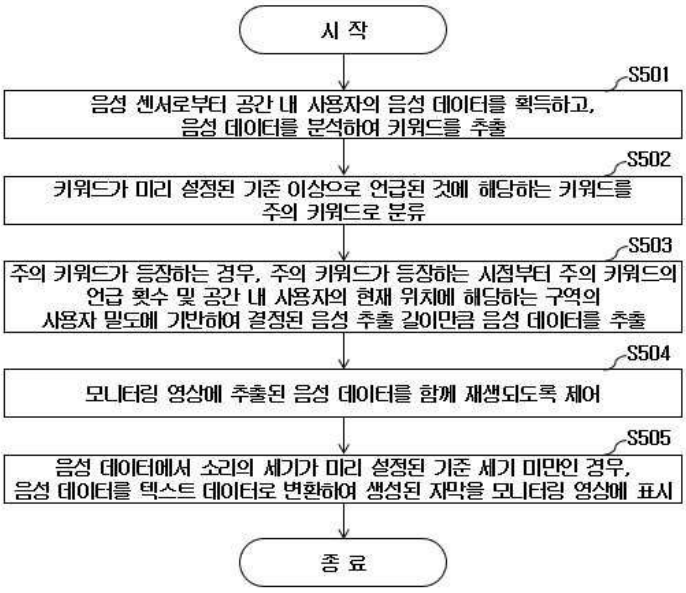
도면3


시 작
S301
위협 행위가 감지된 환경에서 행동 패턴으로부터 위험 지수를 산출
S302
위험 지수가 미리 설정된 기준 이상인 경우, 해당 사용자를 주요 사용자로 분류
위험 지수가 미리 설정된 기준 미만인 경우, 해당 사용자를 주변 사용자로 분류
S303
주요 사용자를 가해자 및 피해자로 분류
S304
주변 사용자의 시선 데이터, 음성 데이터 및 행동 패턴을 분석하여
주요 사용자에 대한 관심도를 산출
S305
주요 사용자에 대한 관심도에 기반하여 알림 범위를 결정
S306
사용자의 단말로부터 연락처 정보 및 현재 위치 정보를 획득
S307
연락처 정보 및 현재 위치 정보로부터
결정된 알림 범위에 따라 비상 연락처를 추출
S308
가해자에 대한 관심도와 피해자에 대한 관심도의 차이에 기반하여
알림 순서를 결정
S309
알림 범위 및 알림 순서에 따라 보안 알림을 생성하여 제공
종 료

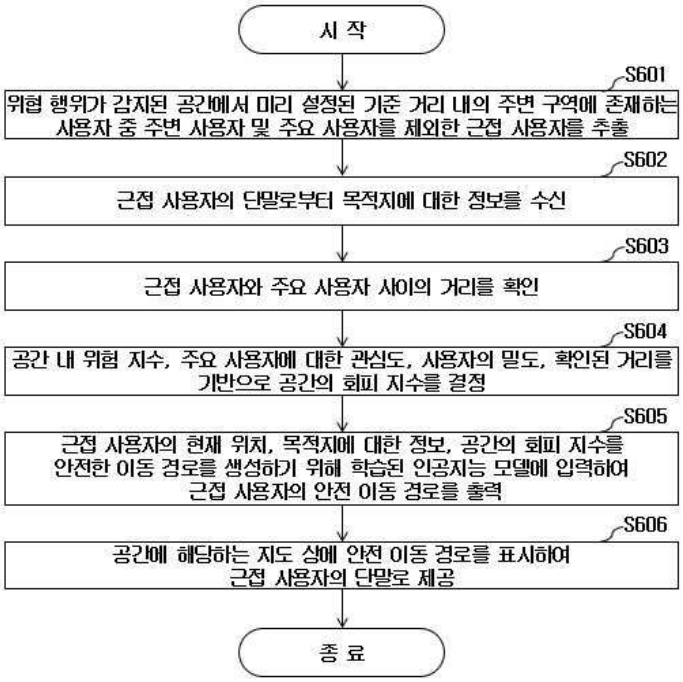
도면4


시 작
S401
위협 행위가 감지된 공간의 영상을 획득하고, 위협 행위가 감지된 시점을 기준으로 사용자의 위험 지수에 따라 결정된 공간 범위만큼 모니터링 영상을 추출
S402
위협 행위가 감지된 이후,
주변 사용자의 주요 사용자에 대한 관심도의 변화를 확인
S403
확인 결과로부터 주변 사용자 및 주요 사용자를 변환
S404
위협 행위가 감지된 공간의 보안 수준을 결정
S405
위협 행위가 감지된 시점에서 멀어질수록 블러 강도를 줄이되,
공간의 보안 수준을 고려하여,
블러 강도에 보안 수준에 기반하여 결정된 가중치를 적용하여 블러 강도를 조정
S406
블러 강도를 모니터링 영상의 배경 부분에 적용
종 료

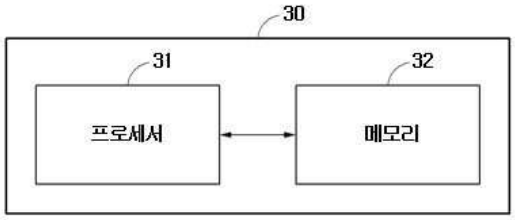
도면5


시 작
S501
음성 센서로부터 공간 내 사용자의 음성 데이터를 획득하고,
음성 데이터를 분석하여 키워드를 추출
S502
키워드가 미리 설정된 기준 이상으로 언급된 것에 해당하는 키워드를
주의 키워드로 분류
S503
주의 키워드가 등장하는 경우, 주의 키워드가 등장하는 시점부터 주의 키워드의
언급 횟수 및 공간 내 사용자의 현재 위치에 해당하는 구역의
사용자 밀도에 기반하여 결정된 음성 추출 길이만큼 음성 데이터를 추출
S504
모니터링 영상에 추출된 음성 데이터를 함께 재생되도록 제어
S505
음성 데이터에서 소리의 세기가 미리 설정된 기준 세기 미만인 경우,
음성 데이터를 텍스트 데이터로 변환하여 생성된 자막을 모니터링 영상에 표시
종 료

도면6


시 작
S601
위협 행위가 감지된 공간에서 미리 설정된 기준 거리 내의 주변 구역에 존재하는 사용자 중 주변 사용자 및 주요 사용자를 제외한 근접 사용자를 추출
S602
근접 사용자의 단말로부터 목적지에 대한 정보를 수신
S603
근접 사용자와 주요 사용자 사이의 거리를 확인
S604
공간 내 위험 지수, 주요 사용자에 대한 관심도, 사용자의 밀도, 확인된 거리를 기반으로 공간의 회피 지수를 결정
S605
근접 사용자의 현재 위치, 목적지에 대한 정보, 공간의 회피 지수를 안전한 이동 경로를 생성하기 위해 학습된 인공지능 모델에 입력하여 근접 사용자의 안전 이동 경로를 출력
S606
공간에 해당하는 지도 상에 안전 이동 경로를 표시하여 근접 사용자의 단말로 제공
종 료

도면7


30
31
32
프로세서
메모리