

SISTEMA INTEGRAL DE CONTROL DE ACCESO

CAMPO DE LA INVENCION

- 5 La presente invención se refiere a un sistema de información que permita hacer más eficiente el proceso de acceso a edificios de oficinas y otras instalaciones sin requerir un enrolamiento o registro en sitio, ni el uso de tarjetas de proximidad o similares.
- 10 La invención tiene aplicación en toda clase de locaciones donde se requiera un control de los visitantes, tales como edificios de oficinas, edificios de habitación, complejos médicos y consultorios, entre otros. La invención tiene aplicación a nivel mundial.

15 ESTADO DE LA TÉCNICA

- El objetivo principal de los sistemas de control de acceso es identificar y otorgar o revocar derechos de acceso a un visitante de una locación física o lógica (equipos, software, aplicativos). Actualmente hay una oferta grande de sistemas de control de
- 20 acceso, el común denominador está en un primer control personalizado donde el visitante típicamente se acerca a personal de vigilancia, entrega un documento de identidad válido y el personal de identidad lo valida o registra en el sistema, dándole un identificador físico que hace parte del sistema para poder acceder a las instalaciones (tarjeta de proximidad, sticker con código de barras, carnet de piso,
- 25 etc). En el proceso el personal de seguridad interactúa con un tercero que es típicamente el visitado, quien confirma el evento de visita y autoriza el ingreso. La administración de los identificadores físicos implica personal, logística y recursos que hacen más complejo y costoso el sistema de control de acceso.
- 30 Actualmente se plantean soluciones de control biométrico adicionales al ya tradicional lector de huella que permiten aumentar la confiabilidad de la validación. Estos lectores pueden o no implicar contacto físico con el visitante, por ejemplo, el

lector de mapa de venas de la mano implica contacto, idealmente son mejores los que evitan el contacto, como los lectores de iris, y los sistemas que usan micrófonos para hacer reconocimiento de voz.

- 5 Las compañías más importantes del mundo en producción de sistemas integrados de control de acceso son Siemens, HoneyWell, HID Solutions, Protection1, Stanley Security, ADT, Tyco y Vanderbilt Industries. Dentro de los sistemas que ellos ofrecen no encontramos alguno que ofrezca las ventajas de la invención propuesta.
- 10 En el estado de la técnica se conocen diversas tecnologías propuestas para el control y seguridad de acceso a instalaciones, que comprenden sistemas informáticos que ayudan a realizar un control rápido. Por ejemplo, la patente CO16-040673 que enseña un sistema y método para gestionar y controlar biométricamente personas internas en recintos de comportamiento especial y poder
- 15 identificar los objetos a los cuales dichas personas acceden por medio de un código, en donde el método es de tipo computarizado (programa) ejecutado por una serie de dispositivos electrónicos que están constituidos por un hardware y un software. Así, la solución propuesta por este documento se basa en el monitoreo de un recinto cerrado para poder controlar y gestionar las actividades que allí se llevan,
- 20 especialmente en espacios donde se llevan a cabo eventos o similares

- De otra parte, está el documento US2012221695 el cual divulga una serie de métodos y aparatos para controlar el acceso a una instalación o ubicación, en donde dicho método permite el acceso físico y el acceso lógico con base en una credencial
- 25 asociada con un dispositivo móvil, monitoreando el acceso lógico por medio del dispositivo móvil, y revocando un privilegio de acceso físico con base en la terminación del acceso lógico por parte del dispositivo móvil. Así, por medio de un dispositivo móvil (puede ser un teléfono inteligente o similar) se da acceso físico a una edificación (tal como un edificio o cualquier otra instalación) de acuerdo con los
 - 30 datos biométricos leídos desde dicho dispositivo móvil y enviados por la red a un servidor donde se almacenan los datos y se concede acceso.

Adicionalmente, se encuentra la patente de invención US2013017812 que enseña métodos y sistemas implementados por computador para suministrar control de acceso remoto a edificios residenciales o de oficinas, en donde los métodos permiten emplear funciones de portero virtual en edificios que no cuentan con porterías. Así, un método puede comprender: recibir una señal de llamada de una estación intercomunicadora, la señal de llamado comprende un identificador de residente que indica un residente con quien el visitante se intenta comunicar; recibir una señal de video generada por al menos una cámara, la señal de video comprende una o más imágenes del visitante; recuperar los datos del visitante asociados con el identificador del residente, los datos de visitante comprenden uno o más perfiles de visitante; y suministrar acceso al edificio para el visitante con base en uno o más criterios predeterminados.

Por su parte, el documento US2015279132 que divulga un sistema de identificación de seguridad que recibe y procesa múltiples credenciales de seguridad que se han configurado por diferentes autenticadores de red, dispositivos configurados para suministrar credenciales de seguridad a dispositivos de acceso de usuario, tal como teléfonos móviles y brazaletes. El sistema tiene múltiples certificados de seguridad que permiten que un empleado ingrese a diferentes instalaciones físicas bloqueadas mantenidas por un empleador cuando cada ubicación física bloqueada se ha asegurado por medio de un protocolo de seguridad diferente, incluyendo protocolos de seguridad provistos por diferentes proveedores de seguridad. El sistema así puede obtener las credenciales de seguridad por un servicio de nube en red, y además puede tomar varias formas tal como un brazalete, gafas, anillos, o audífonos, así como formas como un teléfono móvil. El sistema también puede incluir un dispositivo de lectura biométrica que mide el usuario para verificar que la persona que controla el dispositivo de acceso es su usuario autorizado.

La patente US2015347734 que se relaciona con un sistema y un método en el cual una persona puede utilizar un teléfono celular, un PDA o cualquier otro dispositivo portátil para realizar una compra (parte ejemplar únicamente), aunque el proceso se puede aplicar a cualquier escenario de acceso físico tal como una llave de acceso

a un área restringida o para ingresar a una instalación bloqueada o cerrada. Así, el método de autenticación de usuario permite determinar si el dispositivo de computación está asociado con el usuario enrolado, determinar la identidad del usuario con base en al menos un parámetro biométrico.

5

Por último, la patente US2017148241 que enseña un sistema de control de acceso que utiliza dispositivos electrónicos móviles de usuarios autorizados para transmitir identificadores biométricos en combinación con el uso de una tarjeta llave, para autenticar los privilegios de acceso del usuario para desbloquear una puerta

10 cerrada. El sistema puede además verificar la proximidad del dispositivo del usuario al lector de control de acceso, el cual verifica la correspondencia de la llave de acceso con las características biométricas transmitidas. El sistema además requiere el ingreso de un PIN en el dispositivo del usuario, para su transmisión al sistema de control de acceso para confirmación del acceso. Un escáner escanea el área

15 alrededor de su ubicación geográfica para buscar señales emitidas por dispositivos electrónicos móviles, e identifica una posición, un tipo, y una dirección de cada dispositivo, utilizando características de señales de búsqueda. El sistema también comprende una sección de video que permite correlacionar la imagen de las personas con los dispositivos electrónicos detectados.

20

En este sentido, es claro que el estado del arte requiere de dispositivos y sistemas que logren emplear cámaras de profundidad o cámaras convencionales como dispositivos biométricos a través de algoritmos de inteligencia artificial y que permita emplear varios modos de autenticación con un solo enrolamiento aumentando de

25 manera significativa la seguridad en los ingresos a los establecimientos y permita disminuir los atrasos cuando alguno de los lectores falla.

DESCRIPCIÓN DETALLADA DE LOS DIBUJOS

30 Figura 1. Muestra una descripción del Sistema integral de control de acceso de acuerdo con la presente invención.

Figura 2. Muestra el diagrama de flujo de la Operación de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCION

5

La presente invención se refiere a un sistema de información que entiende el acceso de un visitante como un proceso, y por lo tanto tiene un objetivo que es permitir el control de acceso a edificios de oficinas y otras instalaciones sin requerir un enrolamiento o registro en sitio, ni el uso de tarjetas de proximidad o similares. La integración del sistema incluye varios grupos de componentes para lograr un control de acceso físico a instalaciones minimizando el tiempo, personal, y costo.

10

Los componentes se agrupan así (Ver Figura 1):

1. Dispositivos:

15

- a. Cámaras de profundidad (elemento diferencial)
- b. Cámaras digitales rgb convencionales
- c. Lectores biométricos
- d. Dispositivos móviles inteligentes (smartphones, con o sin cámaras de profundidad y lectores de huella integrados)

20

e. Otros.

2. Soporte Lógico:

- a. Plataforma core basada en el CRM MICS propietario de Millenium
- b. App móvil de visitante
- c. Interfaz web de administración de la locación controlada
- d. Algoritmos de visión de máquina e inteligencia artificial

25

3. Partes físicas tangibles exclusivos para el sistema:

- a. PAV (Punto de Atención Virtual, dispositivo sobre el cual se centra la interacción con el visitante, diseño y desarrollo propio de Millenium BPO S.A.)
- b. Dispositivo de validación de identidad (lectura de cédula y validación de identidad propietario de Millenium).
- c. Torniquetes, barreras o puertas de control de acceso.

30

A nivel de componentes específicos de la invención propuesta, se encuentran dos dispositivos diferenciales, el primero es el PAV o Punto de Atención Virtual, es un dispositivo tipo Kiosko desarrollado por Millenium, este permite una interacción virtual personalizada con un determinado usuario en diferentes tipos de procesos de atención. En este caso el PAV se encontraría en el punto de acceso e incluiría una pantalla sensible al tacto de grado industrial, y los dispositivos periféricos de lector de huella, escáner de cédula, y cámara rgb y/o de profundidad. El dispositivo permite control remoto de los periféricos desde un back office a través de un servicio de videoconferencia. El PAV controlaría los dispositivos de barrera como torniquetes, o puertas. El segundo dispositivo diferencial es el escaner de cédula, desarrollo propio de Millenium que permite capturar gran cantidad de información estructurada y no estructurada de la cédula de ciudadanía. El dispositivo consta de cámaras de alta resolución, un sistema de iluminación y un microcomputador o sistema embebido que controla tanto las cámaras como la iluminación y se encarga de procesar la información que es enviada al PAV. Este dispositivo permite escanear el código de barras de la cédula, capturar la foto, la imagen de la huella, el texto de ambas caras y verificar algunas de las características de seguridad del documento de identidad.

20

En cuanto al flujo de proceso del sistema Integrado (ver Figura 2), el proceso o método de control de acceso llevado a cabo por el sistema integral de control de acceso de acuerdo con la presente invención, comprende los pasos de:

- A. Creación de una cita o evento de visita: El visitado crea el evento en el sistema, y envía la invitación a través del sistema o correo electrónico al visitante
- B. Enrolamiento del visitante. El visitante sigue las instrucciones de la invitación y descarga el app móvil o sigue el link en la página del sistema, el sistema va a dirigirlo hasta tener información suficiente y redundante para poder validar su identidad en el momento de la visita. Típicamente se creará en el sistema asociado a su número de identificación, escaneará, su cédula, se tomarán cerca de 300 cuadros de imagen de la cara con la cámara del dispositivo

móvil o del pc en el cual se está llevando a cabo el enrolamiento y si el dispositivo cuenta con lectores de huella y/o cámaras de profundidad se capturará esta información adicional.

- 5 C. El sistema asociará entonces la información del visitante enrolado a el evento y notificara al visitado que este proceso ha sido exitoso.
- 10 D. El día del evento, previo a la hora de la visita, el sistema alertará al visitado y al visitante sobre el evento, monitoreará las ubicaciones y podrá dar estimados de tiempo y tráfico tanto al visitado como al visitante para facilitar el cumplimiento del horario propuesto. La aplicación también podrá desplegar mensajes de recomendación personalizables por el visitado, tales como ubicaciones de parqueo, política de porte de armas, elementos prohibidos, etc.
- 15 E. En el momento en que el visitante se presenta en las instalaciones del visitado y sin tener que acercarse a ningún personal de seguridad o de recepción, podrá validarse en los torniquetes o puertas de control de acceso, dentro de la ventana de tiempo habilitada por el visitado, y presentándose ante el PAV quien lo guiará para autenticarse presentando su cara ante las cámaras rgb o de profundidad, este dispositivo guía la interacción con el visitante, permitiéndole recibir asistencia personalizada de ser requerida.
- 20 F. En el caso de validación utilizando los algoritmos de reconocimiento facial, el/los algoritmo(s) de visión de máquina procesarán al menos 8 cuadros de video del rostro del visitante e identificarán la identidad del visitante, si hay una concordancia, evaluará la confiabilidad de la misma, si está dentro de un umbral seguro le dará acceso al recinto y le notificará al visitado. Si no está dentro del umbral de alta confiabilidad, el sistema le pedirá a través del PAV que use un segundo método de validación, por ejemplo, la presentación de su cedula en el escáner o la captura de su huella en el lector.
- 25 G. Una vez validada la identidad, con el grado de confiabilidad mínimo exigido, el sistema otorgará el acceso al visitante o definitivamente lo negará, y se iniciará el proceso de asistencia a través del mismo PAV.
- 30 H. Una vez el visitante ha sido validado correctamente, el visitado será notificado para que reciba al visitante en la ubicación convenida y registrada

en el sistema. La aplicación podrá adicionalmente realizar la petición de ascensores y otros sistemas en la locación mediante el uso de NFC, BlueTooth o códigos QR.

- 5 I. Una vez el evento termina, el visitado crea esta novedad en el sistema y el sistema habilita la salida del visitante en una ventana de tiempo predeterminada, el sistema verificará la salida correcta del visitante y notificará al visitado cerrando el evento.

Ventajas del sistema de la presente invención,

- 10 1. El uso de cámaras de profundidad o convencionales, como dispositivos biométricos, gracias al uso de algoritmos de inteligencia artificial con sets grandes de entrenamiento (en el orden de 10^6), son algo no visto comercialmente en el país.
- 15 2. Los algoritmos de visión de máquina e inteligencia artificial permiten usar información no estructurada o semiestructurada y utilizarla como fuente de validación biométrica con un alto nivel de confianza, es el caso de las imágenes de la cara y la huella.
- 20 3. La posibilidad de usar varios modos de autenticación con un solo enrolamiento aumenta de manera significativa la seguridad en los ingresos a los establecimientos y disminuye los atrasos cuando alguno de los lectores fallas, por ejemplo los lectores de huella se ensucian, engrasan, rayan y empiezan a fallar requiriendo varias lecturas hasta lograr descifrar la huella, con un sistema multimodal la aplicación podría generar un código QR que sumado al reconocimiento facial sería suficiente para validar a la persona.
- 25 4. El uso de sensores que no requieren contacto o demasiada cercanía, como los propuestos de reconocimiento facial con o sin cámaras RGB son de mejor aceptación pública, los lectores de palma de mano o de iris o los mismos de huella presentan el inconveniente de requerir mucha cercanía o contacto.
- 30 5. Reducción de costos, al requerir mucho menos personal, espacio, e inmobiliario, los costos de operación asociados al proceso se disminuyen de manera importante.

6. Eficiencia en la operación, una cámara con el algoritmo de inteligencia artificial puede tomarse menos de 10 segundos reconociendo el rostro de un visitante, no hay tiempos de registro en recepción.
7. El enfoque del sistema hacia el proceso completo y no simplemente al control del acceso, mejora la experiencia de los involucrados y agrega valor al proceso disminuyendo los tiempos y sincronizando mejor las etapas del proceso.