Diseño y creación de infraestructura cloud para un sistema de control de acceso a edificio mediante temperatura y sistema de reconocimiento facial

Bastián Troncoso, Robinson Pardo, Alexandra Moreno

I. Visión General

La aplicación consiste en un sistema que controla la entrada a un edificio, midiendo la temperatura de las personas que ingresan para asegurarse de que no presenten fiebre, lo que podría indicar la presencia de una enfermedad contagiosa. El sistema también debe registrar la información de los usuarios y permitir el acceso solo a aquellos que cumplan con las medidas de seguridad sanitaria. La pandemia de COVID-19 ha tenido un impacto significativo en todos los aspectos de la vida diaria. En particular, las instituciones educativas, como las universidades, han enfrentado desafíos sin precedentes para asegurar la seguridad y el bienestar de su comunidad estudiantil, docente y administrativa.

La instalación de un sistema de monitoreo de temperatura se ha convertido en una medida crucial para evitar la propagación de enfermedades infecciosas en los campus universitarios. Se ha encontrado que la temperatura corporal elevada es un síntoma común de infecciones virales, incluida la COVID-19, y la detección temprana de este síntoma puede ayudar a identificar posibles casos y tomar medidas preventivas de manera oportuna. Se pueden obtener numerosos beneficios al instalar sistemas de detección de temperatura en la sede de la universidad de Albacete. En primer lugar, proporcione tranquilidad y seguridad adicional a los estudiantes, profesores y personal administrativo al identificar a las personas con temperaturas altas antes de entrar a espacios compartidos como aulas, bibliotecas o comedores. La implementación de un sistema de detección de temperatura y detección de rostros con Deep Learning en la plataforma de AWS puede proporcionar una capa adicional de seguridad en los campus universitarios, además de los beneficios mencionados anteriormente. El sistema puede identificar a las personas con precisión y medir su temperatura corporal con tecnologías avanzadas como Deep Learning. Esto ayuda a prevenir y contener brotes de enfermedades infecciosas en el campus al permitir una detección temprana y precisa de posibles casos. Además, para garantizar un rendimiento óptimo y una disponibilidad constante, el sistema puede aprovechar la escalabilidad y la confiabilidad de la nube al utilizar la plataforma de AWS.

Este sistema permitirá la detección de temperatura en la sede de Albacete también ayuda a prevenir y contener brotes en el campus. La identificación temprana de personas con fiebre permite tomar medidas rápidas como el aislamiento preventivo, la realización de pruebas diagnósticas y la creación de protocolos de seguimiento y seguimiento de contactos. siendo medidas cruciales para detener la propagación del virus y salvar la salud de toda la comunidad universitaria. El uso de la informática en la nube para aprendizaje profundo, hace incorporar y administrar. Permitiendo a los modelos ajustar su escala de manera eficiente y reducir costos con capacidad de procesamiento de CPU.

II. Componentes

La arquitectura propuesta consta de los siguientes componentes principales:

A. Base de datos DynamoDB

Se utilizará la base de datos NoSQL de AWS, DynamoDB, para almacenar los datos de los usuarios registrados, incluyendo su información personal, registros de acceso, temperatura y estado sanitario.

B. Amazon Rekognition

Se utilizara el servicio de reconocimiento facial de AWS, para identificar a los usuarios a través de una cámara conectada al sistema. Si un usuario no está registrado, se tomará una foto y se agregará a la base de datos para futuras visitas.

C. Servicio IoT de AWS

Se utilizará AWS IoT Core para la gestión de dispositivos y la comunicación con los dispositivos de medición de temperatura y cámaras. Los datos de temperatura se enviarán al servicio IoT para su posterior procesamiento y análisis.

D. AWS Lambda

Se utiliza una función especial de AWS que nos ayuda a manejar todas las tareas importantes detrás de escena. Esta función se encarga de recibir información, realizar verificaciones y guardar datos importantes en un lugar seguro. También nos ayuda a procesar imágenes para reconocer a las personas. Además, esta función es muy inteligente y se ajusta automáticamente según lo que necesitemos, para que todo funcione de manera eficiente.

E. Amazon S3

Se realizaran copias de seguridad automáticas periodicamente para garantizar la integridad y disponibilidad de los datos, ya sean los datos de temperatura y las imagenes obtenidas.

F. EC2

Para alojar la pagina web de control y estadísticas, hemos optado por un servidor virtual en EC2 (Elastic Computing Cloud) dentro de Amazon Web Services.

Nos ayuda a tener los servidores necesarios para que todo funcione correctamente en nuestro proyecto.

G. ELB

Grupo de auto escalado de EC2: Monitorea la carga de trabajo y aumenta o disminuye el número de instancias de EC2 según sea necesario.

H. Amazon Cloudfront

III. Frontend web

El frontend web es la parte visible y la interfaz de usuario del sistema de control de acceso. Proporcionará una experiencia intuitiva y fácil de usar para los usuarios que ingresen al edificio y deseen acceder a las instalaciones.

Se utilizará un sitio web como interfaz de usuario para el sistema de control de acceso. Los usuarios podrán registrarse, proporcionar su información personal y ver el estado de su acceso. También se mostrará la información de temperatura y el estado sanitario.

Características del frontend web:

- Interfaz de registro: Los usuarios tendrán la opción de registrarse en el sistema proporcionando su información personal, como nombre, dirección de correo electrónico, número de identificación, etc. Se implementará un formulario de registro donde los usuarios ingresarán sus datos y se validarán antes de ser almacenados en la base de datos.
- Acceso y estado: Después de registrarse, los usuarios podrán iniciar sesión en el sistema utilizando sus credenciales. Una vez iniciada la sesión, podrán ver el estado de su acceso actual, que incluirá información relevante como fecha y hora de ingreso, estado de temperatura, cumplimiento de las medidas sanitarias, entre otros. Esta información se obtendrá de la base de datos y se mostrará en una interfaz clara y fácil de entender.
- Visualización de temperatura: El frontend web mostrará la información de temperatura recopilada por el sistema. Esto puede incluir la temperatura actual del usuario registrado, el promedio de temperatura del edificio, gráficos de tendencias de temperatura, alertas de temperaturas anormales, etc. La presentación de la información se realizará de manera clara y visualmente atractiva para que los usuarios puedan comprender fácilmente su estado de temperatura y salud.
- Estado sanitario: Además de la información de temperatura, el frontend web mostrará el estado sanitario del usuario, que indicará si cumple con las medidas de seguridad establecidas. Esto podría incluir si el usuario ha completado un cuestionario de salud, si ha seguido las pautas de distanciamiento social, si lleva puesto un cubrebocas, entre otros. El estado sanitario se basará en la información almacenada en la base de datos y se actualizará en tiempo real según los registros y las acciones del usuario.
- Notificaciones y alarmas: El frontend web implementará un sistema de notificaciones y alarmas para alertar a los usuarios sobre eventos importantes. Por ejemplo, se puede enviar una notificación cuando un usuario registre una temperatura anormalmente alta, cuando se realice una actualización en su estado sanitario o cuando haya cambios en las medidas de seguridad del edificio. Las notificaciones se mostrarán en la interfaz del usuario y también se pueden enviar por correo electrónico o mensajes de texto.
- Diseño responsive: El frontend web se diseñará para ser responsive, lo que significa que se adaptará y se verá correctamente en diferentes dispositivos y tamaños de pantalla. Esto permitirá a los usuarios acceder al sistema desde sus computadoras de escritorio, laptops, tabletas o teléfonos móviles, garantizando una experiencia consistente y accesible en todos los dispositivos.

IV. Backend

Las función Lambda de AWS sera un protagonista clave para manejar la lógica empresarial y la interacción con otros servicios. Esta función se encargará de recibir y procesar las solicitudes del frontend, realizar la verificación de temperatura y acceder a la base de datos para almacenar y recuperar información de los usuarios.

La función Lambda será responsable de recibir las solicitudes provenientes del frontend y ejecutar el código correspondiente. Al ser una función serverless, no será necesario preocuparse por la administración de servidores, ya que AWS se encargará de proporcionar y escalar automáticamente la infraestructura necesaria para su ejecución.

En cuanto a la verificación de temperatura, la función Lambda será capaz de procesar los datos obtenidos a partir del dispositivo de medición de temperatura o del servicio IoT de AWS. A través de este proceso, se llevarán a cabo las comprobaciones necesarias para determinar si la temperatura registrada cumple con los criterios establecidos de seguridad sanitaria. De esta forma, la función Lambda tomará decisiones fundamentadas, como permitir o denegar el acceso al edificio, en función de los resultados obtenidos.

Además, la función Lambda interactuará con la base de datos para almacenar y recuperar información relevante de los usuarios. Mediante el uso del servicio de base de datos DynamoDB de AWS, la función Lambda consultará la base de datos para verificar la existencia de registros de usuarios y comprobar si cumplen con las medidas de seguridad sanitaria requeridas. Asimismo, la función Lambda actualizará los registros de acceso y almacenará información relacionada con las temperaturas registradas.

La elección de una función Lambda como backend serverless brinda diversas ventajas. Por un lado, la escalabilidad se logra de forma automática, ya que la función Lambda se ejecuta según la demanda sin requerir la intervención manual

del usuario. Esto asegura que el sistema pueda hacer frente a cargas variables de solicitudes de manera eficiente.

Por otro lado, el backend serverless con funciones Lambda permite una implementación ágil y un enfoque de desarrollo centrado en la lógica empresarial. Los desarrolladores podrán concentrarse en escribir el código que implementa la verificación de temperatura, la interacción con la base de datos y otras funcionalidades empresariales, sin tener que preocuparse por la infraestructura subyacente.

1) Base de datos DynamoDB: En el contexto del sistema propuesto, se ha decidido utilizar DynamoDB, la base de datos NoSQL de AWS, para almacenar los datos relacionados con los usuarios registrados. DynamoDB es una solución escalable y flexible que permite almacenar y recuperar datos de manera eficiente.

DynamoDB será utilizado para almacenar la información personal de los usuarios, como nombres, números de identificación, y cualquier otro dato relevante. Además, se registrarán los accesos realizados por los usuarios, incluyendo la fecha y hora, el resultado de la verificación de temperatura y el estado sanitario.

Esta elección de base de datos NoSQL tiene varias ventajas. En primer lugar, DynamoDB proporciona una alta escalabilidad y rendimiento, lo que significa que puede manejar grandes volúmenes de datos y soportar cargas de trabajo variables sin comprometer el rendimiento. Esto es especialmente importante en un sistema en tiempo real como el propuesto, donde se esperan múltiples solicitudes simultáneas.

Además, DynamoDB ofrece una modelación de datos flexible. No se requiere un esquema fijo y estricto, lo que permite adaptar fácilmente la estructura de los datos a medida que el sistema evoluciona. Esto resulta beneficioso en casos como la adición de nuevos campos o la actualización de la información requerida para los usuarios.

Otra ventaja de DynamoDB es su integración con otros servicios de AWS. En este caso, la función Lambda podrá interactuar directamente con DynamoDB para almacenar y recuperar información de manera eficiente, sin tener que preocuparse por la administración de la infraestructura subyacente.

2) Servicio de reconocimiento facial: Este servicio de reconocimiento facial avanzado permite detectar y analizar características faciales para verificar la identidad de las personas.

Cuando un usuario se acerque al punto de acceso del edificio, la cámara capturará su imagen y la enviará al servicio de Amazon Rekognition para su procesamiento. A través de algoritmos de reconocimiento facial, el servicio comparará la imagen capturada con las imágenes almacenadas en la base de datos de usuarios registrados.

Si el usuario ya está registrado, Amazon Rekognition identificará su rostro y confirmará su identidad. En este caso, el sistema permitirá el acceso al edificio, ya que se ha verificado que es una persona autorizada.

Por otro lado, si el usuario no está registrado en la base de datos, lo cual indica que es su primera visita al edificio, se tomará una foto y se agregará a la base de datos. Esta acción permitirá registrar su información personal y su imagen para futuras visitas, brindando un mayor nivel de seguridad y facilitando su identificación en visitas posteriores.

La utilización de Amazon Rekognition ofrece varias ventajas para el sistema de control de acceso. En primer lugar, brinda una alta precisión en el reconocimiento facial, lo que garantiza un control de acceso seguro y confiable. Además, el servicio es capaz de trabajar en tiempo real, lo que permite una respuesta inmediata al identificar a los usuarios.

Asimismo, Amazon Rekognition ofrece funcionalidades adicionales, como la detección de emociones y la estimación de edad, que podrían ser utilizadas para complementar la verificación de identidad y brindar información adicional sobre los usuarios.

3) Servicio IoT de AWS: Proporciona una plataforma escalable y segura que permite la conexión y administración de dispositivos IoT de manera eficiente. En este caso, los dispositivos de medición de temperatura y las cámaras se conectarán al servicio IoT Core para enviar los datos recolectados y establecer una comunicación bidireccional con el sistema.

Los dispositivos de medición de temperatura se encargarán de recolectar la información de temperatura de las personas que ingresan al edificio. Estos dispositivos enviarán periódicamente los datos de temperatura al servicio IoT Core a través de un protocolo de comunicación seguro. Los datos recolectados serán almacenados en una cola de mensajes en el servicio IoT Core, listos para su procesamiento posterior.

Por otro lado, las cámaras utilizadas para el reconocimiento facial también se conectarán al servicio IoT Core. Estas cámaras enviarán las imágenes capturadas al servicio IoT Core para su posterior análisis y procesamiento.

Una vez que los datos de temperatura y las imágenes se encuentren en el servicio IoT Core, se podrán aplicar diversas funcionalidades, como el enriquecimiento de los datos, el enrutamiento a servicios específicos y el análisis adicional.

El servicio IoT Core también facilita la integración con otros servicios de AWS, lo que permitirá, por ejemplo, utilizar los datos de temperatura recolectados para realizar análisis más avanzados mediante servicios de machine learning, como Amazon SageMaker.

A. Detalle de la propuesta

La propuesta arquitectónica presenta una solución integral y segura para el sistema de control de acceso y gestión de usuarios. A continuación, se detallan cada uno de los componentes y su funcionamiento:

- API Gateway para la comunicación entre el frontend y el backend: Se utilizará API Gateway, un servicio de AWS, para exponer una API RESTful que permita la comunicación segura y eficiente entre el frontend web y el backend serverless. API Gateway asegurará la autenticación de las solicitudes y la protección de los datos transmitidos.
- Función Lambda para la lógica empresarial y la interacción con la base de datos: El backend serverless estará

implementado como una función Lambda de AWS. Esta función se encargará de diversas tareas, como la autenticación de usuarios, la verificación de temperatura, el procesamiento de imágenes y la interacción con la base de datos DynamoDB. Con la escalabilidad automática proporcionada por AWS, la función Lambda asegurará un rendimiento óptimo en función de la demanda.

- Reconocimiento facial con Amazon Rekognition: Para garantizar la identificación precisa de los usuarios, se creará una colección en Amazon Rekognition, el servicio de reconocimiento facial de AWS. La cámara capturará imágenes de las personas que ingresan al edificio, y estas imágenes se enviarán a Rekognition para su análisis y comparación con la base de datos de usuarios registrados. Esto permitirá una verificación de identidad rápida y confiable.
- Seguridad y privacidad de los datos: Se aplicarán políticas y permisos adecuados para garantizar la seguridad y privacidad de los datos personales de los usuarios. Se cumplirán las regulaciones de protección de datos aplicables, como el cumplimiento del Reglamento General de Protección de Datos (GDPR) en Europa. Con medidas de seguridad sólidas, como el cifrado de datos en tránsito y en reposo, se salvaguardará la integridad de la información confidencial.

V. Arquitectura

La arquitectura propuesta para esta aplicación es la siguiente:

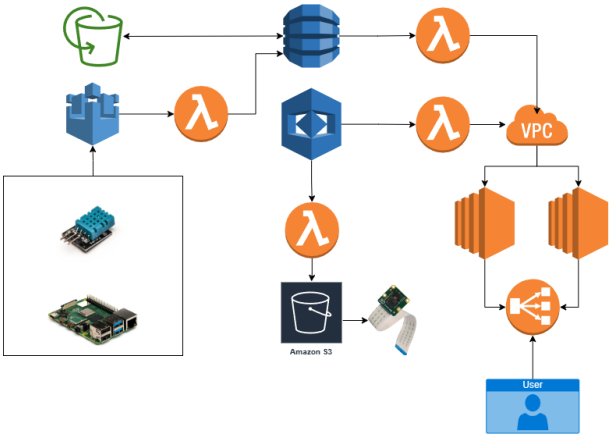

Fig. 1. Arquitectura propuesta

VI. Despliegue

Para desplegar de forma mas eficiente y segura, utilizaremos Terraform. Terraform es una herramienta de infraestructura como código (IaC) que permite definir y desplegar la infraestructura en la nube de forma automatizada y reproducible. Utilizando el lenguaje de configuración de Terraform, puedes describir todos los recursos necesarios para tu proyecto y luego utilizar Terraform para crear y administrar esos recursos en un proveedor de servicios en la nube, como AWS.

Para esto es necesario considerar los siguientes puntos:

- Configuración del proveedor: En primer lugar, debes configurar Terraform para utilizar AWS como proveedor de servicios. Esto implica proporcionar las credenciales de AWS y definir la región en la que deseas desplegar tus recursos.
- Definición de recursos: Es necesario definir los recursos que componen tu infraestructura, en este caso, basado en los servicios utilizados, algunos recursos son los siguientes:
  - CloudFront: Puedes utilizar el recurso aws_cloudfront_distribution para definir tu distribución de CloudFront, configurando los orígenes y los comportamientos adecuados.
  - Lambda Functions: Utiliza el recurso aws_lambda_function para definir tus funciones Lambda. Aqui encontraremos una función para la validación de temperatura, otra para la autenticación y una mas para la interaccion con amazon rekognition
  - IoT Service: Utiliza los recursos aws_iot_thing, aws_iot_topic_rule y aws_iot_policy para definir tu servicio IoT. Aqui se configuraran las reglas de envío de datos de temperatura y fotos a los servicios correspondientes.

VII. Conclusion

el proyecto implementa una solución integral de control de acceso y gestión de información sanitaria mediante el uso de tecnologías avanzadas. La arquitectura propuesta, que incluye componentes como el frontend web, el backend serverless, la base de datos DynamoDB, el servicio de reconocimiento facial, el lector de tarjetas, el servicio IoT de AWS y el servicio de Machine Learning, garantiza un sistema seguro, eficiente y escalable.

Al aprovechar las capacidades de Amazon S3, se logra un almacenamiento y distribución rápida del sitio web de interfaz de usuario. El uso de Amazon EC2 permite la ejecución de servidores virtuales flexibles y confiables, mientras que AWS Lambda como backend serverless permite una gestión simplificada de la lógica empresarial y la interacción con otros servicios.

La implementación de Amazon Rekognition permite la identificación precisa de usuarios a través del reconocimiento facial, mientras que la integración con la base de datos DynamoDB permite un almacenamiento seguro y eficiente de la información personal y los registros de acceso.

Además, el uso del servicio IoT de AWS facilita la gestión y comunicación con los dispositivos de medición de temperatura y cámaras, y el servicio de Machine Learning, a través de Amazon SageMaker, ofrece análisis y modelado de los datos de temperatura para detectar patrones y tendencias relevantes en la salud sanitaria.