Tercera evaluación Gestión de la IoT-2024
Solicitud de Ensayo sobre (IoT) y Propuesta de Solución.

Equipo Desarrollador
Matías Jesús Egaña Alfaro.

Asignatura
Gestión De Internet De Las Cosas.

Profesor
Juan Prudencio Torres Ossandon.

Introducción

Objetivo

El objetivo principal de este informe pretende dar cuenta sobre los conocimientos acerca de los dispositivos IoT (Internet Of Thing, Internet de la cosas) que fueron aprendidos a los largo de curso, explicando conceptos básicos sobre las tecnologías, junto con los desafíos que estos se ven enfrentados en términos de seguridad e infraestructura sobre la incorporación de estas.

Una vez dicha se propondrá una solución, en la cual se pueda ofrecer dispositivos IoT referente a un rubro en específico, justificando las tecnologías a utilizar. Para que pueda ser incorporado en un futuro.

Introducción del concepto de IoT

El término IoT, da a inicios del siglo XXI, el cual este propone la interconexión de dispositivos electrónicos por medio de un red, en este caso es la internet, permitiendo así la comunicación entre estos dispositivos.

La Internet de las cosas (IoT) describe la red de objetos físicos ("cosas") que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet. Estos dispositivos van desde objetos domésticos comunes hasta herramientas industriales más sofisticadas.

Ahora cabe preguntar ¿Por qué es tan importante el Internet de las cosas (IoT)?

En los últimos años, IoT se ha convertido en una de las tecnologías más importantes del siglo XXI. Puesto que, podemos conectar objetos cotidianos, electrodomésticos, termostatos, monitores de bebés, a Internet a través de dispositivos integrados, es posible una comunicación fluida entre personas, procesos y cosas.

Importancia de los dispositivos Iot en el contexto actual y sus posibilidades

Actualmente las tendencias muestran que esta tecnología llegó para quedarse. Según **Marketing4eCommerce**, los informes indican que habrá 35.82 mil millones de dispositivos IoT instalados en todo el mundo para 2021 y 75.44 millones para 2025.

En Chile. La adopción del internet de las cosas en Chile e hispanoamérica se ha visto en aumento siendo el 47% de las empresas implementan el IoT.

El 67% de los ejecutivos que se encuestaron señaló que la innovación como el principal beneficio de la adopción del internet de las cosas, seguida de la productividad y agilidad con el 49% de comentarios positivos y la eficiencia operativa con el 42%.

Pero, según el 45% de los encuestados, el desafío de implementar estas tecnologías se ha visto reflejado en el presupuesto para adoptar las tecnología del internet de las cosas.

Esto genera un desafío ante estas tecnologías, sin embargo el interés por adoptar estas tecnologías por parte de las empresas ha ido creciendo.

Los beneficios que pretende esta tecnología a nivel de las empresas es proponer soluciones digitales, entre estas resaltan: la analítica de video para monitoreo de personas y ambientes con un 49% de implementación, gestión de inventario y logística interna presentan el 27% de implementación y la geolocalización con 26%.

Desarrollo

Plataformas de IoT:

Para desarrollar conectividad entre los dispositivos IoT se necesita un lugar donde se puedan albergar los datos recolectados para su interpretación y uso conveniente.

Para esta tarea se utilizan distintas plataformas para que suceda esta conexión, distintas compañías ofrecen sus servicios por medio de pago, como lo son:

- Amazon Web Service (AWS).
- Oracle IoT Cloud.
- Microsoft Azure IoT.
- Google Cloud IoT.

Para la comparativa se realizó un cuadro comparativo de estos servicios, comprando lo que nos ofrece, junto con características propias de contratar cada servicio.

Característica	Amazon Web Services (AWS)	Oracle IoT Cloud	Microsoft Azure IoT	Google Cloud IoT
Servicio Principal IoT	AWS IoT Core	Oracle IoT Cloud Service	Azure IoT Hub	Google Cloud IoT Core
Escalabilidad	Altamente escalable; múltiples regiones	Escalable para necesidades empresariales	Altamente escalable y bien integrado con servicios	Altamente escalable, con soporte a big data
Integración de dispositivos	Compatible con MQTT, HTTPS, LoRaWAN	Compatible con MQTT y HTTP	Soporte para MQTT, AMQP y HTTP	Compatible con MQTT y HTTP
Analítica y Machine Learning	Servicios como SageMaker y AWS IoT Analytics	Integración con Oracle Analytics Cloud	Integración con Azure Machine Learning	Integración con BigQuery y Vertex AI
Almacenamiento	Amazon S3, DynamoDB, RDS	Oracle Cloud Infrastructure Object Storage	Azure Blob Storage, Cosmos DB	Google Cloud Storage, Firestore

Costo	Pago por uso; opciones gratuitas limitadas	Pago por suscripción con enfoque empresarial	Pago por uso; incluye capas gratuitas iniciales	Pago por uso; capa gratuita generosa inicialmente
Seguridad	AWS IoT Device Defender, cifrado AES 256	Seguridad integrada con Oracle Cloud	Azure Security Center para IoT	IAM, claves rotativas, cifrado AES 256
Facilidad de Uso	Amplia documentación y herramientas para desarrolladores	Complejo pero potente para soluciones empresariales	Intuitivo con integración con Visual Studio	Sencillo y bien integrado con GCP
Regiones y cobertura	Cobertura global con más de 30 regiones	Cobertura en múltiples regiones	Cobertura global con más de 60 regiones	Global, aunque menor cobertura que AWS y Azure
Casos de Uso Común	Agricultura inteligente, ciudades conectadas	Gestión empresarial, logística	Industria, manufactura, smart cities	Vehículos autónomos, análisis de IoT a gran escala

Estadísticas de IoT

El crecimiento de IoT es exponencial. Según **FindStack**, se espera que haya más de 75 mil millones de dispositivos conectados para 2025, lo que refleja su impacto global. En América Latina, el mercado IoT sigue en expansión, con sectores como la logística y la agricultura liderando la adopción. Estas cifras subrayan el potencial de IoT para transformar economías locales al ofrecer soluciones eficientes y escalables.

Adopción de IoT en Chile e Hispanoamérica

En Chile, IoT ha encontrado un terreno fértil en sectores como la minería y la agricultura inteligente, aprovechando la conectividad para optimizar recursos. Sin embargo, desafíos como la falta de infraestructura tecnológica y la brecha digital aún limitan su alcance. Según **Marketing4eCommerce**, países como México y Brasil lideran en adopción regional, mientras que en Chile las empresas están comenzando a reconocer el valor estratégico de IoT para mejorar la productividad y la sostenibilidad.

Pero el desafío principal que señala la fuente es la cultura organizacional es señalada por el 37% de los ejecutivos como la principal barrera en la adopción del Internet de las Cosas.

Seguridad en IoT

La seguridad sigue siendo un desafío crítico en IoT. Según **Kaspersky**, la proliferación de dispositivos aumenta el riesgo de ataques cibernéticos, desde accesos no autorizados hasta el robo de datos. Buenas prácticas como el cifrado de extremo a extremo y la autenticación de múltiples factores son esenciales. Por su parte, Azure resalta la importancia de implementar monitoreo continuo y actualizaciones automáticas para mitigar las vulnerabilidades.

Mientras más dispositivos conectados haya, más oportunidades tienen los cibercriminales de poner en riesgo la seguridad de esos datos

Ante esta situación, Kaspersky recomienda ciertas consideraciones y buenas prácticas para aumentar la seguridad de los dispositivos IoT. Entre ellos se encuentran:

1. **Actualizar software y dispositivos**: Mantener los dispositivos y su software actualizados protege contra vulnerabilidades explotadas en versiones antiguas.

2. **Cambiar contraseñas**: Es fundamental establecer contraseñas únicas y evitar usar las predeterminadas para dificultar el acceso a ciberdelincuentes.

3. **Usar contraseñas seguras**: Contraseñas largas, complejas y únicas para cada dispositivo.

4. **Renombrar el enrutador**: Cambiar el nombre del enrutador evita revelar la marca o modelo del dispositivo, dificultando los ataques dirigidos.

5. **Cifrado de red Wi-Fi**: Configurar el enrutador con métodos de cifrado modernos como WPA2 o posterior, asegura comunicaciones seguras.

6. **Red de invitados**: Crear una red separada para visitas evita comprometer la red principal en caso de dispositivos infectados.

7. **Revisar configuraciones de privacidad**: Personalizar las opciones de privacidad y seguridad de los dispositivos reduce el uso indebido de datos personales.

8. **Desactivar funciones no utilizadas**: Minimizar las superficies de ataque al apagar funciones innecesarias, como Bluetooth o NFC.

9. **Autenticación de múltiples factores (MFA)**: Implementar MFA añade una capa adicional de seguridad para el acceso a cuentas y dispositivos
.
10. **Inventario de dispositivos IoT**: Mantener un registro actualizado de los dispositivos en la red para identificar modelos antiguos que puedan ser reemplazados por opciones más seguras.

11. **Precaución con redes Wi-Fi públicas**: Evitar manejar dispositivos IoT desde redes públicas no seguras o usar una VPN para proteger la conexión.

Conclusión y Propuesta de Solución

Como hemos visto a lo largo de este informe.

La Internet de las Cosas ha transformado la manera en que interactuamos con los diferentes dispositivos y sistemas, conectando objetos cotidianos a través de redes. Su adopción masiva está impulsada por los beneficios que ofrece en términos de eficiencia, productividad y sostenibilidad, especialmente en sectores como la agricultura, la logística y las ciudades inteligentes.

A pesar de su potencial, la implementación de dispositivos IoT enfrenta desafíos significativos, como la falta de infraestructura tecnológica, presupuestos limitados y resistencia cultural dentro de las organizaciones. Estos factores son especialmente notables en regiones como América Latina, donde, aunque hay avances, persisten brechas tecnológicas y digitales.

A esto se le agrega que al aumentar los dispositivos conectados incrementan los riesgos en términos de ciberseguridad. Debido a que, los ataques cibernéticos pueden comprometer datos sensibles y operaciones críticas. Dicho lo anterior, es crucial seguir buenas prácticas.

Los siguientes son la utilización de plataformas como AWS, Microsoft Azure IoT, Google Cloud IoT y Oracle IoT Cloud ofrecen soluciones robustas para la implementación de IoT, cada una con características específicas de escalabilidad, analítica, almacenamiento y seguridad. La elección de una plataforma debe alinearse con las necesidades específicas del proyecto y el sector.

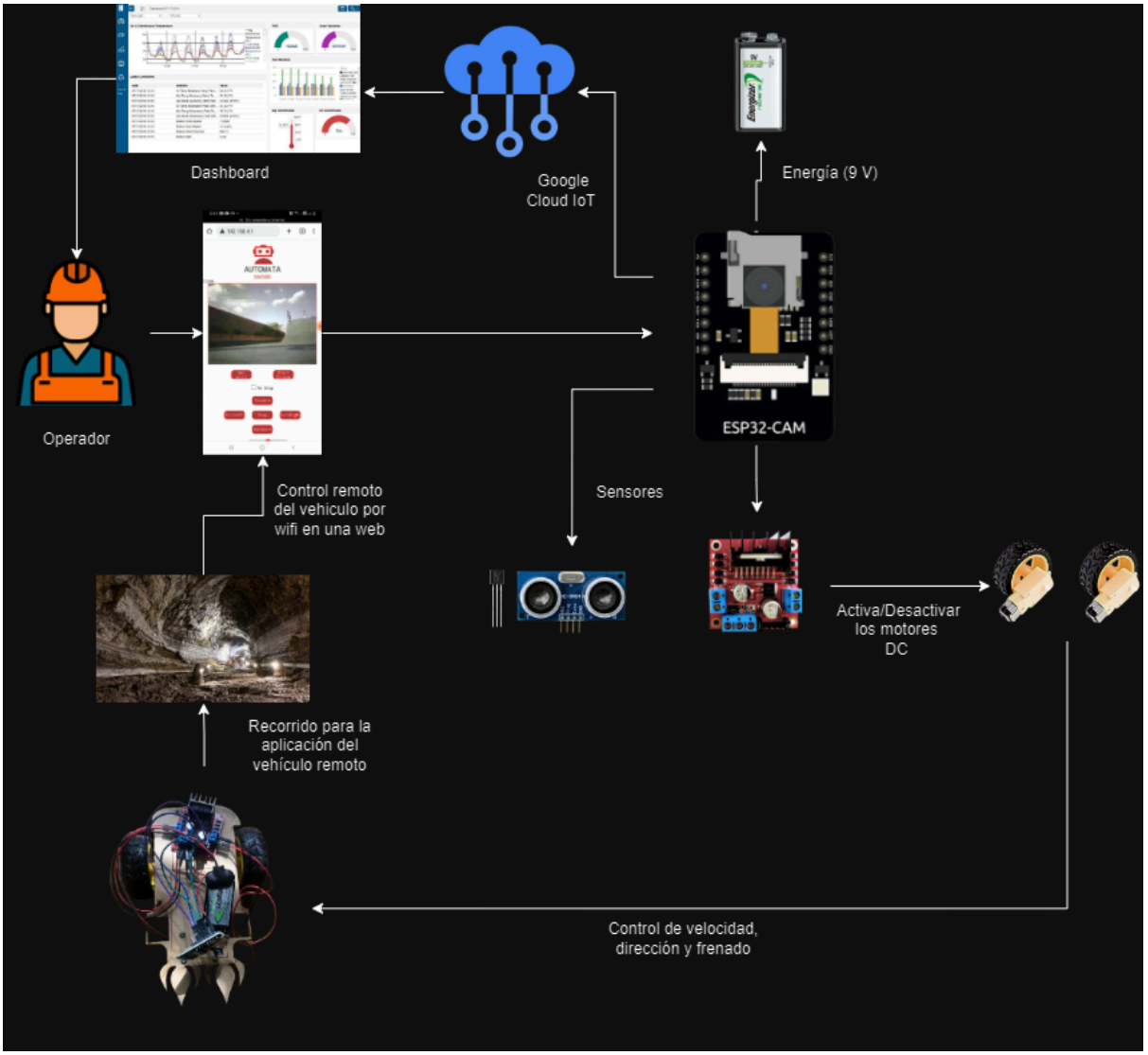
En la región, IoT tiene un papel prometedor para transformar sectores clave como la minería y la agricultura. Sin embargo, superar las barreras organizacionales y fomentar la inversión en infraestructura serán determinantes para maximizar su impacto en los próximos años.

Expuesto lo anterior, ahora se detallará la propuesta que es la exposición de trabajadores a zonas industriales peligrosas mediante la implementación de un vehículo controlado remotamente utilizando tecnologías IoT. Este vehículo, equipado con una ESP32-CAM, permitirá inspeccionar y monitorear áreas de alto riesgo en tiempo real, eliminando la necesidad de intervención humana directa.

La solución se basa en un diseño modular compuesto por los siguientes elementos clave:

1. **ESP32-CAM:** Este microcontrolador será el núcleo del sistema, proporcionando conectividad WiFi y capacidad de transmisión de imágenes en tiempo real gracias a su cámara integrada.
2. **Motores de corriente continua (DC):** Facilitarán el movimiento del vehículo en diferentes direcciones.
3. **Módulo L298N:** Controlador de motores que permite ajustar la velocidad y dirección de los motores mediante señales PWM.
4. **Motor paso a paso:** Se utilizará para ajustar la posición vertical de la cámara, brindando un rango de visión más amplio.
5. **Batería recargable de 9V:** Proporcionará energía suficiente para todos los componentes del sistema.
6. **Sensor de proximidad (HC-SR04):** Detectará obstáculos en el camino del vehículo, ayudando a prevenir colisiones.
7. **Sensor de temperatura (DHT11 o DHT22):** Medirá las condiciones ambientales en tiempo real, proporcionando datos importantes para la seguridad.

8. **Conexión a la Nube con Google Cloud IoT:**
    - La ESP32-CAM se conectará a Google Cloud IoT Core para enviar datos del sensor y el estado del vehículo.
    - Estos serán mostrados por medio de un Dashboard.



"Diagrama de Vehículo IoT."

El sistema permitirá que los usuarios controlen remotamente el vehículo y monitoreen áreas de riesgo desde una interfaz web o aplicación móvil, incrementando la seguridad operativa y reduciendo riesgos asociados al ingreso humano en estas zonas.

Para finalizar, la propuesta no solo busca mitigar peligros inmediatos, sino también optimizar procesos industriales al ofrecer una solución accesible y funcional con tecnologías IoT de bajo costo.

Referencias bibliográficas

- Benítez, C. (2023, febrero 18). Internet of things statistics. Findstack. Más de 21 estadísticas, hechos y tendencias de Internet de las cosas para 2024
- Ruiz, A. (2022, mayo 22). Así es la adopción del internet de las cosas en Chile e hispanoamérica: 47% de las empresas implementan el IoT. Marketing4eCommerce. https://marketing4ecommerce.cl/adopcion-del-internet-de-las-cosas-en-chile-e-hispanoamerica/
- ESP32 CAM Rover - Robot explorador
- Kaspersky. (n.d.). Mejores prácticas para la seguridad del IoT. Recuperado el 27 de noviembre de 2024, de Los riesgos de seguridad y las buenas prácticas de la Internet de las cosas
- IoT World Online. (n.d.). Concepto básico de Internet de las cosas o IoT. Recuperado el 27 de noviembre de 2024, de Concepto básico de Internet de las Cosas o IoT
- Amazon Web Services (AWS)**.** (n.d.). *AWS IoT Core.* Amazon. Recuperado de https://aws.amazon.com/iot-core/
- Microsoft**.** (n.d.). *Microsoft Azure IoT.* Microsoft. Recuperado de https://azure.microsoft.com/en-us/overview/iot/
- Google Cloud. (n.d.). *Google Cloud IoT.* Google. Recuperado de https://cloud.google.com/solutions/iot
- IBM**.** (n.d.). *IBM Watson IoT.* IBM. Recuperado de IoT Solutions | IBM