

Sistema prototipo basado en IoT para el apoyo a la detección de acceso ilegal a una casa habitación

Trabajo Terminal No. 2020-B075

*Alumnos: *Ramos Mesas Edgar Alain, Simón Hernández Cristian, Vázquez Cruz Fernando Darwin*

Directores: M. en C. Jiménez Ruiz Rene Baltazar Dr. Ramírez Romero Tonáhtiu Arturo

**email: eramosm1200@alumno.ipn.mx*

Resumen – El internet de las cosas, o IoT, ha permitido en los últimos años la conexión y automatización de actividades tanto a nivel doméstico como a nivel industrial. La implementación de diversos sensores electrónicos, sistemas embebidos, y dispositivos como Raspberry Pi permiten controlar a través de una red conectada a internet, distintos aspectos que requieren de constante atención humana, como la seguridad. Por tal razón, se pretende implementar un sistema de apoyo para la detección de acceso no autorizado haciendo uso de cámaras, sensores y algoritmos de cómputo.

Palabras clave: IoT, sensores, detección de acceso, algoritmos computacionales, actuadores.

1. Introducción

Es posible definir al internet de las cosas (Internet of Things, IoT) como una red de objetos físicos conectados a través de internet, los cuales logran interactuar entre sí vía sistemas embebidos, redes de comunicación, mecanismos de computación de respaldo y aplicaciones típicamente en la nube [1]. En otras palabras, IoT une los objetos del mundo real con el mundo virtual, para así facilitar la conectividad en cualquier momento y en cualquier lugar para cualquier cosa, no sólo considerando a las personas. Se refiere a un mundo donde los objetos físicos y los seres, los datos y los entornos virtuales; estarían todos ellos interrelacionados entre sí temporal y espacialmente [2].

Dentro de las ventajas que ofrece el Internet de las cosas, una de las más notables y con mayor presencia en los últimos años, no solo en la industria sino también en aspectos de la vida diaria, es la capacidad de automatizar tareas específicas. Para tener una idea del alcance que puede tener la implementación del IoT en un sistema, basta con consultar la definición de una herramienta comúnmente asociada con el desarrollo de IoT, los sistemas embebidos. Se dice que un sistema embebido es la combinación de software y hardware que tiene una aplicación en particular y que puede formar parte de un sistema aún más grande [3], todo de manera automática (programada a través del software embebido) y con la menor cantidad de intervención humana posible. En otras palabras, en conjunto la implementación de IoT con el desarrollo de sistemas embebidos ofrecen una puerta abierta a la construcción de sistemas cada vez más robustos para dar solución a problemas cada vez más complejos.

Actualmente existe una larga lista de dispositivos y sensores que aportan datos, generando así nuevo conocimiento que puede ser manejado y procesado a través de algoritmos de cómputo desde dispositivos como Raspberry Pi; al mismo tiempo, esto hace posible implementar sistemas de control que permitan usar como entrada los datos obtenidos y automatizar procesos a través de ellos. Así, por ejemplo, si se hace uso de cámaras para el análisis de imágenes, es posible transformar y analizar los datos obtenidos a través de estos dispositivos y generar un algoritmo que permita tomar decisiones y desencadenar un proceso determinado.

La seguridad ha tomado una importancia imprescindible en todos los sectores; es por ello, que no es de extrañar la constante innovación que muestran, en materia tecnológica y en funcionalidades, los sistemas de control de acceso.

Dentro de los escenarios empresariales e incluso de ciertos hogares, la necesidad de regular el acceso de personas a edificios o recintos delimitados, es uno de los centros de actividad más importantes; y como consecuencia los sistemas de control de acceso se vuelven una prioridad. Estos sistemas de protección previenen la entrada o salida de personas no autorizadas en determinados lugares. Por lo que, la identificación de los individuos es la primera premisa para poder determinar si están o no autorizados, ya sea mediante un sistema de tarjeta, llavero, contraseña, su propia huella dactilar, puntos biométricos de la cara, entre otros

Hablando de situaciones más específicas, el robo a casa habitación es uno de los delitos que más nos afectan por diversas razones, una de ellas es porque se realiza en nuestro hogar, el espacio en el que se supone estamos más seguros, en donde vive nuestra familia. El atraco nos deja vulnerables, pues ya no nos sentimos seguros en ningún

lugar, debido a que creemos que violaron nuestro espacio y que existe un gran riesgo.

De acuerdo con datos de la Procuraduría General de Justicia de la Ciudad de México, entre enero y noviembre de 2018 se registraron 6 mil 924 denuncias por robo a casa-habitación, de las cuales, 93 por ciento fue sin violencia. Esto significa que aproximadamente cada mes robaron en 629 casas, 21 por día, o casi un hurto cada hora.

Tal como era de esperarse, esto no sólo ocurre en la capital del país, pues de acuerdo con cifras del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, durante el primer cuatrimestre de 2019 el robo a casa habitación con violencia creció 11 por ciento en todo el territorio nacional. [4]

Ante lo anteriormente expuesto, este proyecto consiste en el desarrollo e implementación de un sistema que sea capaz de brindar apoyo para la prevención de incidentes de seguridad en un hogar haciendo uso de cámaras de video y sensores de presencia conectados mediante una red interna. El sistema tendrá como núcleo una tarjeta Raspberry Pi, en la cual se creará el servidor para procesar las imágenes con ayuda de algoritmos para el procesamiento de los datos recopilados por los sensores, además de algoritmos de procesamiento de imágenes para posteriormente subir los datos obtenidos a una base de datos en la nube. Adicionalmente, los sensores de a diseñar, que serán colocados en ventanas, puertas y exteriores permitirán llevar un control de acceso de las personas previamente identificadas a través de las cámaras, además de que por las noches tendrán la tarea especial de controlar actuadores en caso de detectar algún acceso no autorizado.

Al mantener una conexión con internet, se pretende enviar notificaciones al usuario a través de una aplicación en la que se muestre la hora y fecha exacta en las que se registró alguna visita al hogar, identificando de ser posible, la persona que realizó la visita al domicilio y registrándose al sistema si no ha sido registrado con anterioridad. Se pretende que, de detectar actividad sospechosa, el sistema genere una alerta tanto para el usuario como para las autoridades, permitiendo así dar apoyo al apartado de seguridad en los hogares.

Estado del Arte

Actualmente la mayor parte de los sistemas existentes coinciden en el uso de sensores para puertas y ventanas, así como la implementación de sensores de movimiento en exteriores, sin embargo, muy pocos sistemas proponen el uso de algoritmos de cómputo para el análisis de la información recopilada a través de los sensores.

A continuación, se presenta una lista de los sistemas similares existentes en el mercado:

- SimpliSafe Wireless Home Security System - Compatible con Alexa y Google Home[5]
- SmartThings Home Monitoring Kit (F-MON-KIT-1) - Samsung[6] Alarmas Tera
- (A20)- Compatible con Alexa, Google Home, Smart Life, TuyaSmart [7]
- TT 2019-B046 “Prototipo de Sistema de detección de intrusión a casa habitación”

Tabla 1. Cuadro comparativo de los sistemas de seguridad domésticos.

Características	SimpleSafe Wireless Home Security	Smart Things Home Monitoring Kit	Alarmas Tera Modelo A20	TT 2019-B046 “Prototipo de Sistema de detección de intrusión a casa habitación”	TT 2020-B075 “Sistema prototipo basado en IoT para el apoyo a la detección de acceso ilegal a una casa habitación”
Aplicaciones Compatibilidad	Alexa y Google Home	Alexa y Google Home	Alexa y Google Home	Plataforma Propia.	Plataforma Propia

Sensores (puertas y ventanas)	Si	Si	Si	Si	Si
Sensor de movimiento	No	Si	Si	Si	Si
Cámaras de video	No incluido	No incluido	No	No	Dos
Detección de personas con análisis de imágenes.	No	No	No	Si	Si
Alarma de Seguridad	Si	Si	No incluida	No	Si
Notificaciones por correo y mensaje.	Si	No	Si	Si	Si
Monitoreo Remoto	No	Si	No	Si	Si

2. Objetivos

Diseñar un sistema para la detección del acceso ilegal a una casa habitación utilizando diferentes tipos de sensores y poder determinar la ejecución de determinadas acciones de seguridad.

- Diseñar varios nodos sensores.
- Diseñar un sistema basado en Raspberry Pi que permite conectar de manera física los diferentes equipos (cámaras y sensores) a una red doméstica.
- Recolectar la información de los diferentes sensores.
- Implementar una base de datos para almacenar los datos obtenidos por los sensores y por las cámaras.
- Diseñar la etapa de potencia para los actuadores que se necesiten.
- Diseñar la interfaz de usuario.
- Diseñar el manual técnico.

3. Justificación

La seguridad siempre ha sido un tema de gran importancia dentro de la historia humana, la necesidad de tratar de asegurar un lugar que tenga el menor número de situaciones de riesgo nos obliga a siempre buscar nuevas formas de tratar de mantenernos seguros, haciendo uso de todas las herramientas que estén a nuestro alcance y que resulten fáciles de adquirir o emplear para dar solución a dicha necesidad.

Con el avance de la ciencia y la tecnología, principalmente con la implementación de las nuevas tecnologías inalámbricas y ante la necesidad de mantener todo conectado, nos ha sido posible desarrollar nuevas ideas que permiten ofrecer apoyo en este apartado haciendo uso de nuevas herramientas, siendo el caso de la domótica y por ende la seguridad inteligente, algunos de los aspectos con mayor desarrollo en los últimos años. No obstante, en la actualidad la mayor parte de sistemas existentes en el mercado se limitan a ofrecer dispositivos en puertas y ventanas dejando de lado el apartado de detección perimetral, algo que en el sistema que se propone, será fundamental [8].

Con el desarrollo e implementación de este sistema se busca hacer una mejora en el apoyo a la seguridad que ofrecen los sistemas existentes en el mercado, haciendo uso de nuevas tecnologías que ofrezcan al usuario un apoyo más completo en el ámbito de seguridad en el hogar.

Algunos de los beneficios ofrecidos por el sistema:

- Monitoreo en tiempo real del estado de puertas y entradas.
- Alarma de emergencia ante detección de situaciones de riesgo.
- Encendido automático de luces ante detección de movimiento.
- Actualización de lista de personas conocidas.
- Panel de control principal para la visualización de las imágenes obtenidas por las cámaras.

La propuesta del sistema incluye tanto la implementación y acondicionamiento del hardware necesario, como la implementación de la interfaz principal de control.

4. Productos o Resultados Esperados

La arquitectura que se utilizará en el sistema es la siguiente:

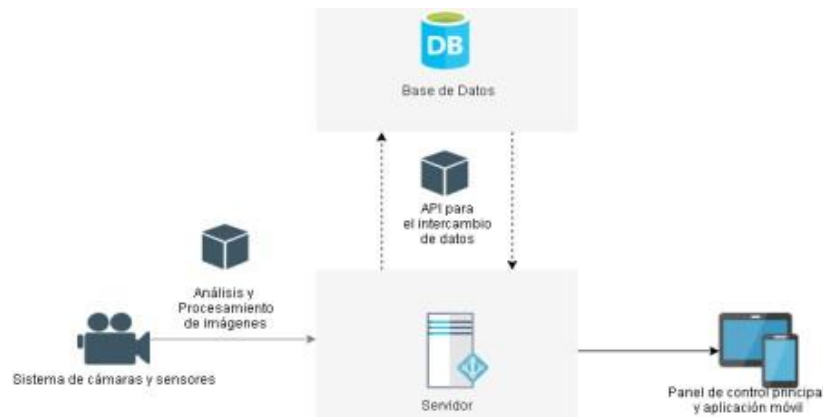


Diagrama 1. Arquitectura del sistema.

Los productos esperados al final son los que se enlistan a continuación:

- Red local de cámaras y sensores.
- Servidor montado en Raspberry Pi para la conexión de cámaras y sensores y el envío de datos a la base de datos en la nube.
- Interfaz de usuario para el monitoreo del sistema.
- Documentación y manual técnico del sistema.

5. Metodología

Para este proyecto se planea usar una metodología de prototipado evolutivo ya que se centra en una representación de aquellos aspectos del sistema que serán visibles para el cliente o el usuario final. Este diseño conduce a la construcción de un prototipo, el prototipo se prueba y modifica cuando es necesario, y los resultados se anotan en la revisión de los bosquejos y los dibujos en funcionamiento, conllevando a diversos beneficios como las mejoras a la calidad, la reducción del ciclo de desarrollo. Además, al pertenecer al modelo de desarrollo evolutivo, permite simplificar las pruebas en cada componente del sistema por separado antes de probar el conjunto completo de componentes ensamblados y ofrece grandes ventajas al momento de dar mantenimiento al sistema.[9] Se trata de una metodología en la que se adaptan e incorporan las diferentes funcionalidades a medida que están sean implementadas

y habilidades en la parte física del sistema, permitiendo así, ofrecer mejoras significativas en cada versión del sistema tanto en el apartado de hardware como en el de software.

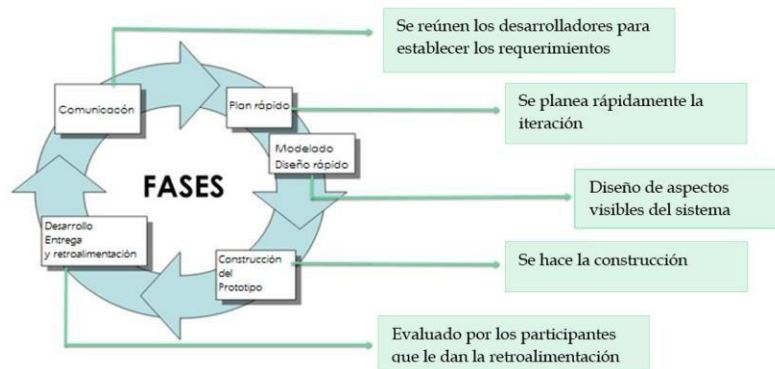


Diagrama 2. Modelo por Prototipos

Además de lo ya mencionado, se ha optado por el desarrollo evolutivo debido a que, de existir un débil acoplamiento entre componentes, existe la posibilidad de actualizar y/o agregar componentes y funcionalidades en cada iteración según sea necesario, sin afectar otras partes del sistema, lo cual ofrece una gran ventaja ante posibles problemas a lo largo del desarrollo del sistema.

Como ya fue mencionado, al tratarse de modelos de desarrollo con enfoque iterativo, se pretende generar diferentes prototipos con diferentes alcances tal como se muestra en la tabla 2.

Iteración	Alcance
Iteración 1	<ul style="list-style-type: none"> ■ Delimitación de los componentes de hardware y software a utilizar. ■ Diseño de la arquitectura general del sistema. ■ Diseño de los nodos sensores a implementar. ■ Diseño de la base de datos para la gestión de los estados de los nodos sensores. ■ Diseño de la etapa de potencia de los actuadores que se necesiten. ■ Diseño de la interfaz de usuario.
Iteración 2	<ul style="list-style-type: none"> ■ Preparación del ambiente de desarrollo sobre Raspberry Pi. ■ Construcción y pruebas del prototipo de los nodos sensores. ■ Construcción y pruebas de los prototipos para los actuadores. ■ Montaje del servidor o broker sobre Raspberry. ■ Preparación del prototipo para la recolección de información por parte de los sensores.
Iteración 3	<ul style="list-style-type: none"> ■ Pruebas de alarma y encendido de luces ante la detección de accesos no autorizados. ■ Despliegue de la interfaz de usuario. ■ Integración de las notificaciones basadas en eventos. ■ Implementación de notificaciones a servicios de emergencia. ■ Control de acceso desde la interfaz de usuario.

Tabla 2. Iteraciones de los prototipos.

6. Cronograma

CRONOGRAMA Ramos Mesas Edgar Alain

[illegible]

CRONOGRAMA Simón Hernández Cristian

[illegible]

CRONOGRAMA Vázquez Cruz Fernando Darwin

[illegible]

7. Referencias


- [1] O. Quiñonez Muñoz, Internet de las cosas (IoT), Ibukku, 2019.
- [2] D. A. G. Eduardo O. Sosa, «Internet del futuro: Desafíos y perspectivas,» *Revista científica y tecnológica (Versión Online)*, n° 21, 2014.
- [3] R. Kamal, Embedded Systems: Architecture, Programming and Design, New Delhi: Tata McGraw-Hill Education, 2011.
- [4] "Robo a casa-habitación, crece y se moderniza", La Razón, 2020. [En línea]. Available: <https://www.razon.com.mx/opinion/robo-a-casa-habitacion-crece-y-se-moderniza/>. [Accessed: 06- Nov 2020].
- [5] UsableNet Inc., «SimpliSafe,» SimpliSafe, Inc., 2020. [En línea]. Available: <https://simplisafe.com/home-security-system-bunker>. [Último acceso: 04 11 2020]
- [6] «Samsung,» Samsung Electronics Co., 1995-2020. [En línea]. Available: <https://www.samsung.com/us/support/owners/product/home-monitoring-kit>. [Último acceso: 04 11 2020].
- [7] «Alarmas Tera,» Mercado Libre, [En línea]. Available: https://alarmastera.mercadoshops.com.mx/MLM-699647762-a20-wifi-alarma-telefono-gsm-app-casa-negocio-inalambrica-_JM?quantity=1#position=4&type=item&tracking_id=bfd60614-cc20-4bfb-8672-2aab1a1b18e3. [Último acceso: 04 11 2020]
- [8] J. M. Huidobro Moya y R. J. Millán Tejedor, Manual de Domótica, España: Creaciones Copyright S.L, 2010
- [9] Roger S. Pressman, Ingeniería del Software. Un enfoque Práctico, Madrid: McGraw-Hill, 2002

8. Alumnos y directores

Ramos Mesas Edgar Alain. - Alumno de la carrera de Ing. en Sistemas Computacionales en la ESCOM, Especialidad sistemas, Boleta: 2013090243, Tel 5525293345, email: eramosm1200@alumno.ipn.mx

Firma: 

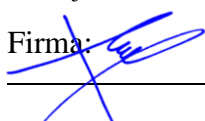
Simón Hernández Cristian. - Alumno de la carrera de Ing. en Sistemas Computacionales en la ESCOM, Especialidad sistemas, Boleta: 2017631501, Tel 7721384448, email: csimonh1600@alumno.ipn.mx

Firma: 

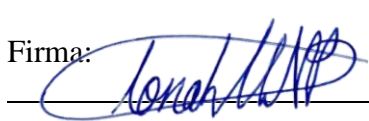
Vázquez Cruz Fernando Darwin. - Alumno de la carrera de Ing. en Sistemas Computacionales en la ESCOM, Especialidad sistemas, Boleta: 2013090157, Tel 5542578844, email: fvazquezc1200@alumno.ipn.mx

Firma: 

Rene Baltazar Jiménez Ruíz. - Obtuvo el grado de M. en C. en Sistemas Computacionales Móviles en ESCOM, IPN en septiembre de 2015. Obtuvo el grado de Ingeniero en Mecatrónica en UPIITA, IPN en enero de 2011. Es profesor de la academia de sistemas digitales en ESCOM, IPN desde 2015. Áreas de interés: Robots móviles, sistemas mecatrónicos y sistemas digitales. Teléfono 57296000, Ext. 52032, 52051. email: izn_rjimenez@hotmail.com

Firma: 

Tonáhtiu Arturo Ramírez Romero. - Doctor en Ingeniería de Sistemas, profesor investigador, jefe de la sección de estudios de posgrado e investigación de la ESCOM. Áreas de interés: Inteligencia artificial, bases de datos, desarrollo de sistemas web y sistemas complejos. Publicaciones en congresos nacionales e internacionales, así como en revistas científicas arbitradas. SEPI, Escuela Superior de Cómputo, Tel. 57296000, ext 52028 email: tonahtiu@yahoo.com

Firma: 

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.
PARTES CONFIDENCIALES: Número de boleta y teléfono.