Desarrollo de aplicaciones en las nuevas plataformas móviles para la gestión de la seguridad del control de accesos.

Arturo Estudillo-Quilantán[1], Alberto-Israel Castellanos-Reyes[1], Erick Cacho-Rojas[1] y Ted Echeverria-Dionisio[1].

[1]Instituto Tecnológico Superior de Coatzacoalcos, Coatzacoalcos, Ver., México
a.estudillo@live.com.mx
Paper received on 25/07/12, Accepted on 07/09/12.

Resumen. El presente proyecto es resultado del estudio e investigación de estas nuevas tecnologías para mejorar la seguridad de acceso a hogares y negocios, siendo su objetivo principal, incrementar la seguridad a través de la integración de herramientas computacionales, innovando en el uso de las tecnologías de la información y la comunicación mediante el empleo de aplicaciones para dispositivos móviles que operan bajo plataformas de última generación. De esta manera, implementa una aplicación smartphones que sustituye las llaves tradicionales por claves digitales que se envían mediante Bluetooth a la cerradura, para que ésta las evalúe identificándolas como permitidas o denegadas; un sistema de control encargado de configurar las llaves y aplicar restricciones de horarios, aspectos que se notifican a la cerradura electrónica usando Wi-Fi, que recibe y evalúa las llaves enviadas desde el dispositivo movil, permitiéndole o no el acceso, y registrando el evento ocurrido para enviarlo al sistema de control.

Palabras Clave: Seguridad, Aplicaciones móviles, sistemas embebidos**.**

1 Introducción.

En la actualidad, uno de los temas que causa mayor interés social en nuetro país es la inseguridad. En los últimos años, los registros de incidencia de delitos, ha incrermentado considerablemente en las diferentes entidades de la republica, lo que a su vez ha obligado a las autoridades dirigir la mirada a esta situación, que cada vez es más alarmante. Estadísticamente en el 2010 fueron robadas 287.6 viviendas a diario a nivel nacional [1], de acuerdo con las estadísticas del Sistema Nacional de Seguridad Pública. Las cifras muestran que en las Procuradurías de Justicia Estatales y del Distrito Federal se denunciaron 94 mil 254 robos cuando las personas estaban ausentes de sus viviendas. Así el robo a casa habitación se convirtió en la tercera modalidad del ilícito con mayor incidencia en el país. Estos actos son planeados por estas personas la cual saben por dónde atacar, ya que algunos estudios han demos-

Advances in Intelligent and Information Technologies.
Research in Computing Science 60, 2012, pp. 189 -199.

trado que, el 27% de los casos, se lleva acabo brincando las bardas, mientras que el 24% forzar las puertas [2]. Lo cual nos indica que, una de las vulnerabilidades que más explotan los amantes de lo ajeno es la entrada principal o secundaria de nuestros hogares. Debido a lo anterior, la misma sociedad ha tenido la necesidad de buscar opciones que incrementen su seguridad personal y patrimonial, en un mercado donde existen numerosas alternativas, tanto para el hogar como en oficinas de diferentes instituciones; sin embargo suelen ser costosas y aun así son vulnerables.

El surgimiento de tecnologías emergentes y la consolidación de las ya existentes, permiten desarrollar aplicaciones que ofrezcan solución a problemáticas como la de la inseguridad. Las Tecnologías de la Información y la Comunicación (TIC) han facilitado el intercambio de información entre diferentes aplicaciones, permitiendo a los usuarios tener mayor disponibilidad de la misma. Estas tecnologías mantienen un vínculo entre ellas, lo que hace posible su interacción con sistemas heterogéneos como dispositivos electrónicos y móviles a través de redes, por lo que las TIC ofrecen una amplia gama de soluciones en automatización, domótica e inmótica.

Uno de los equipos de las TIC mayormente utilizados en la actualidad son los teléfonos móviles. Según datos arrojados por la COFETEL [3], para afínales del 2011 en México habría más de 94.5 millones de usuarios de telefonía móvil, tal y como se observa en la figura 1.

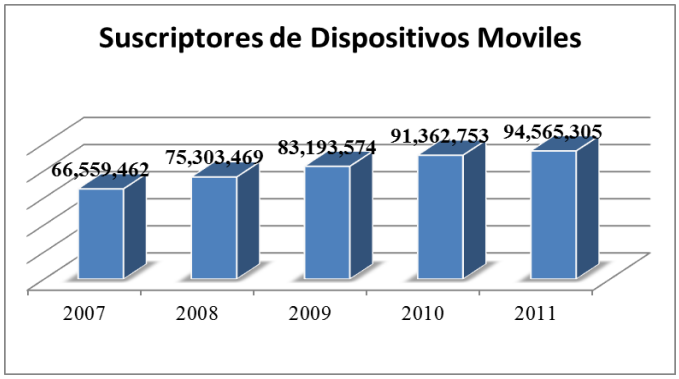

Figura 1. Usuarios de telefonía móvil según COFETEL[1].

De esta manera se aprecia que la telefonía móvil es ampliamente utilizada por más del 75% de la población, con una penetración en 2008, de 77.4 usuarios por cada 100 habitantes en todo el país [4]. Lo que ha propiciado que los desarrolladores de software hayan incursionado en el mundo de estos dispositivos, y que cada vez sea más frecuente emplearlos como portadores de sistemas complejos de gran diversidad, ya sea p comodidad, diversión o para efectos laborales.

Estos cuatro aspectos: Necesidad de seguridad en los hogares, cerraduras electrónicas robustas, administración de accesos mediante sistemas computacionales y el empleo masivo de celulares; nos permite concebir la idea del presente proyecto para solucionar el primer punto (seguridad) mediante el empleo de la tecnología existente (celulares, cerraduras electrónicas y administración computacional). De esta forma se desarrolla un sistema integral, que administre accesos mediante horarios

a partir de llaves encriptadas (claves) construidas en los celulares y controladas mediante software, que una vez enviadas a las cerraduras electrónicas verifiquen la coincidencia con aquellas que fueron dadas de alta por el sistema y suministradas únicamente por celulares igualmente registrados. En la figura 2 se puede apreciar en forma gráfica, la manera en que interactúan estos elementos del sistema en su conjunto.

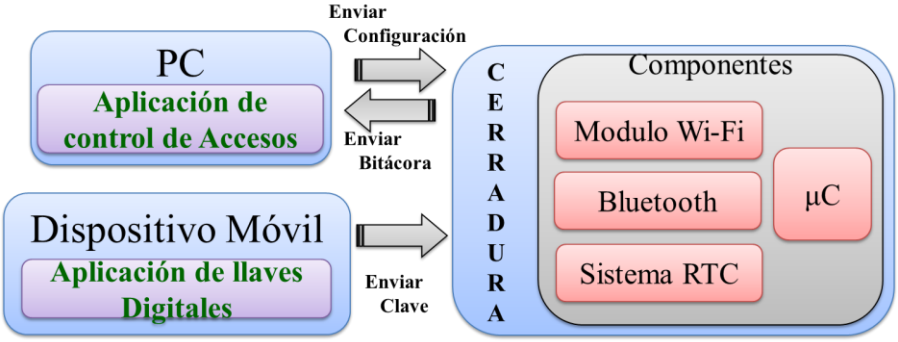

Figura 2. Diagrama de flujo de datos

De esta manera, los delincuentes no solo se enfrentarán a adivinar una clave; sino que para irrumpir sería necesario adquirir el dispositivo móvil, entrar al sistema (el cual también requerirá de una contraseña), enviar la llave (que sólo debe ser conocida por el usuario autorizado) a la cerradura, y por si fuera poco, usarla en el periodo en el que se ha permitido el acceso mediante la misma. Lo que se pretende a través de este proyecto, es reducir el riesgo de que nuestro patrimonio se vea comprometido y que todo el esfuerzo que hacemos día a día para hacernos de pertenencias que nos provean de comodidad, se vean afectadas por aquellos que gustan de arrebatar lo que no les pertenece.

2 Desarrollo.

El robusto sistema que se propone, integra la utilización de tres subsistemas que ofrecen un control apropiado de la seguridad de accesos, reduciendo la posibilidad de entrada a personas no autorizadas al incluir varios niveles de autenticación. La integración de estos subsistemas incrementa la seguridad al utilizar cerraduras electrónicas especiales, que reciben una clave digital vía Bluetooth, haciendo que no sea suficiente con ingresar un código o deslizar una tarjeta, sino que ahora se requiere la presencia de un celular previamente registrado (por la aplicación de escritorio) que ejecute una aplicación especial mediante la cual se envía una llave digital, que debe coincidir con las que el sistema registró en la memoria de la cerradura.

De esta forma existen niveles de seguridad adicionales: la presencia de celulares específicos, la utilización de aplicaciones especiales y la coincidencia con una llave encriptada para que la cerradura electrónica permita el acceso de las personas a la casa-habitación.

2.1. Aplicación de llaves digitales en dispositivos móviles.

Durante muchos años, la gran mayoría de los equipos celulares incluían una máquina virtual de Java, denominada KVM (Kilo Virtual Machine) incrustada de fábrica, la cual permitía a los teléfonos móviles ejecutar aplicaciones y juegos con un mínimo de recursos consumidos [5]. Esta pequeña máquina virtual corresponde al perfil de desarrollo MIDP (Mobile Information Device Profile, Perfil de Dispositivos de Información Móviles), por lo que cualquier aplicación para dispositivos móviles (MIDlet) desarrollada en java, puede funcionar en estos dispositivos.

Sin embargo, en los últimos años, el avance tecnológico y la demanda de equipos más sofisticados y con mayores capacidades, han permitido ofrecer un abanico más amplio de aplicaciones más cercanas al usuario para los bien llamados *smarthphone* [6]. El lanzamiento de Android como nueva plataforma para el desarrollo de aplicaciones móviles, han causado gran expectación, y está teniendo una importante aceptación tanto por los usuarios como por las industrias.

Considerando la popularidad, la evolución del mercado de esta tecnología y la posible obsolescencia de las aplicaciones en java con perfil MIDlet, el durante la presente investigación se decidió migrar el desarrollo a la plataforma Android. De esta forma, se desarrolló una aplicación que nos permitiera enviar a través del puerto Bluetooth, la llave de acceso a la cerradura, al mismo tiempo que mantuviera los niveles de seguridad del usuario.

Para poder controlar el Bluetooth, el perfil MIDlet requiere el uso de la JSR (Java Specification Request) 82, un paquete que contiene el núcleo del API (Application Programming Interface, Interfaz de Programación de Aplicaciones) para Bluetooth con los métodos necesarios para esta tarea, sin embargo, esta no está disponible en todos los equipos, aun cuando estos tengan un puerto Bluetooth disponible. Por su parte, Android, a través de una Bluetooth API, permite la administración del puerto Bluetooth del smarthphone, el cual codificará la llave de acceso y la enviará hacia la cerradura, a través de un flujo de datos serial por el protocolo RFCOMM. El proceso de conexión para el envió de esta llave cifrada involucra: a) encender y poner visible el puerto Bluetooth del equipo, b) realizar una búsqueda de aquellos dispositivos con puerto visible y con la clase de dispositivo acorde al de la cerradura, y mostrarlas en pantalla, c) seleccionar el dispositivo al cual se enviara la llave, d) solicitar la llave al usuario, y por ultimo e) establecer la conexión y enviar el flujo de datos serial; como se ejemplifica en la figura 3.

Para poder evitar la suplantación de identidad, al momento de generar la llave, no solo basta con que el usuario introduzca su palabra secreta, sino que además, el programa agrega a la cadena, datos que identifiquen el equipo de donde se está generando. Así, cuando el usuario envía su llave, esta no podrá ser reproducida desde otro teléfono al que no se le haya asignado, aun con el mismo password. Otra medida de seguridad con la que cuenta la aplicación, es un módulo de autenticación como se puede observar en la figura 4, donde el usuario deberá ingresar su nombre de usuario y contraseña para acceder, disminuyendo el riesgo de que alguien pueda generar una llave desde ese dispositivo.

Figura 3. Proceso de establecimiento de la conexión bluetooth.

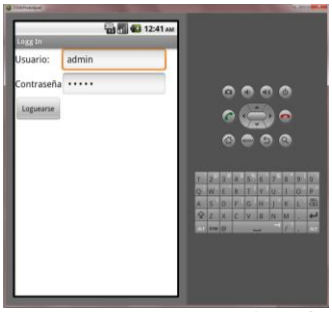

Figura 4. Ventana de autentificación**.**

El Perfil MIDlet de Java y los limitados recursos de almacenamiento que pueden contar los teléfonos móviles, impedían el uso de bases de datos complejas. En contraparte, Android incluye una librería SQLite para el uso de bases de datos, que permite almacenar los datos de una forma sencilla y potente, pero con un bajo consumo de recursos del sistema, con la cual se puede agregar la persistencia de los datos a la aplicación desarrollada. La aplicación cuenta también, con un módulo que le permite al usuario cambiar de forma periódica sus credenciales de acceso al sistema como se observa en la figura 5, con lo que los niveles de seguridad se incrementan.

2.2 Aplicación de control de accesos.

El sistema de seguridad cuenta con una aplicación que permite administrar los accesos y configurar la cerradura mediante el envío de instrucciones propias utilizando Wi-Fi. Desarrollada bajo la arquitectura de N capas y apegándose a la metodología RUP, la aplicación se encuentra desarrollada en ambiente Microsoft Visual Studio 2008, utilizando una frontera (interfaz gráfica) en Windows Presentation Foundation, una persistencia basada en el motor Microsoft SQL Server 2005 y fun-

damentando el código de la lógica de negocios, control y entidades en C#. En la figura 6 se puede observar el diagrama de casos de uso de este subsistema.

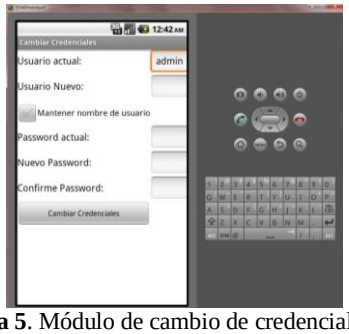

Figura 5. Módulo de cambio de credenciales**.**

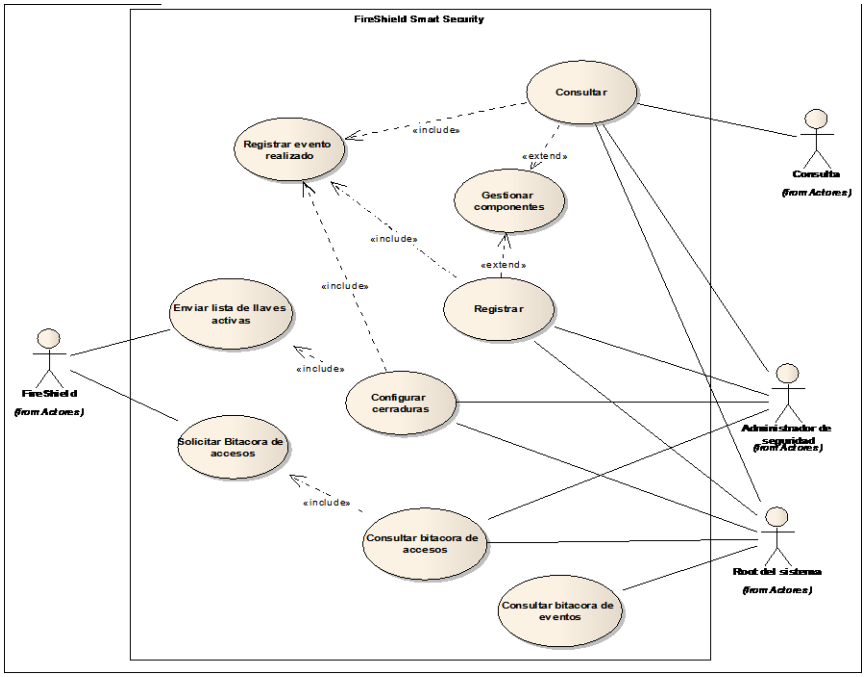

Figura 6. Diagrama de casos de uso de la Aplicación de Control.

En la figura 7 se muestra el módulo que permite capturar los datos de los usuarios del sistema. Estos usuarios dados de alta, se encargarán de registrar los equipos celulares que podrán accesar al recinto, previa autenticación a partir de atributos como su número, Bluetooth address y número de serie. Es necesario que cada vez que se agregue un celular se capturen también los datos de su dueño para consultas posteriores.

Figura 7. Módulo Registro de Usuarios

Esta aplicación tiene la capacidad de administrar diversas cerraduras, es decir que no se limita sólo a una, por lo que también cuenta con un módulo que permite agregar las cerraduras a las que podrá configurar con los horarios y equipos autorizados. Como se puede apreciar en la figura 8, de las cerraduras instaladas se registra su número de serie y DNS con el que cuenta para establecer la comunicación vía red inalámbrica.

Figura 8. Módulo Registro de Cerraduras

Una vez que existan en la base de datos los teléfonos celulares autorizados y las cerraduras existentes, se procede a capturar las llaves lógicas que serán recibidas por la cerradura desde el celular vía Bluetooth, permitiendo o denegando su entrada. Para dar de alta una llave, se debe elegir primero el celular que estará ligado a ella y la cerradura que podrá abrir, una vez hecha esta relación, se ingresa una clave alfanumérica de máximo 6 caracteres, así como la fecha inicial y de vencimiento para determinar el intervalo de tiempo en que será efectiva dicha clave. Con estos datos se construye la llave lógica que será almacenada en las cerraduras y con las cuales se verificará la posibilidad de acceso por parte de los solicitantes.

Uno de los aspectos más relevantes de la aplicación es la configuración de las cerraduras. Para ello es necesario elegir una de ellas del listado general y seleccionar la opción "configurar", con lo que se detallará en una tabla todas las llaves que habrán de registrarse, modificarse, eliminarse o permanecer intactas en la cerradura. El estado de las mismas también es mostrado en la tabla, es decir se muestra si la llave es nueva, modificada o ya existente, en caso de que una llave previamente registrada en la cerradura no se muestre en la tabla, significaría que ha sido eliminada

y por ende se dará de baja. En la misma tabla se muestran los horarios de acceso permitidos para cada llave por día, así como la fecha de inicio y expiración. Una vez que el usuario elija la opción enviar, se inicia el proceso de conexión mediante la red inalámbrica con la cerradura a través de la búsqueda del DNS de la misma y su autenticación a través de un diálogo de presentación en el que se utiliza el mecanismo de reto-respuesta. Una vez efectuada de manera adecuada la autenticación de ambas partes, la aplicación envía una secuencia de instrucciones a ser efectuadas por la cerradura. Como parte importante de la aplicación, es posible también pedir a la cerradura, la bitácora de solicitudes de acceso concedidos y denegados almacenados en su memoria. De esta forma, es necesario indicar primero a la aplicación el nombre DNS con el que se identifica a la cerradura a nivel de usuario, para que una vez elegida la opción "actualizar", se establezca la conexión con la cerradura seleccionada, y después de su respectiva autenticación, se le notifique mediante el comando apropiado, la requisición de la bitácora, la cual se recogerá en la aplicación y se mostrará en una tabla para ser analizada por el usuario. Esta bitácora muestra la fecha de la solicitud de acceso, la hora en que ésta se realizó, el nombre de la persona que se tiene registrado como dueño del equipo celular y si se le concedió o no el acceso. De manera continua, la aplicación registra todas las actividades realizadas por todos los usuarios dentro de la misma, para efectos de auditoría o revisión posterior exclusivamente por parte del root. Por último, como cualquier aplicación que utiliza información delicada, se cuenta, como se muestra en la figura 9, con la posibilidad de efectuar respaldos y restauraciones para maximizar la funcionalidad del sistema.

Figura 9. Módulo de Configuración y Respaldos

2.3 Cerradura electrónica.

Se desarrolló una interfaz receptora de la llave enviada por el celular, con la capacidad de almacenar las diferentes combinaciones válidas para cada uno de los usuarios, así como el registro de los eventos ocurridos. Los aspectos que se consideraron son que la cerradura debía recibir vía Wi-Fi la configuración desde el sistema central en el interior del domicilio, almacenar esa información y compararla con los datos que se reciban por el puerto Bluetooth. Utilizando un microcontrolador AT89C51 y multiplexando su puerto serial a los módulos Bluetooth MTS2BTSMI y Wi-Fi MT800SWM de Multitech, se recibe el flujo de datos provenientes del teléfono móvil o de la computadora, interpretando mediante el uso de interrupciones la

fuente de los datos. En la figura 10 se observan los módulos Bluetooth y Wi-Fi en la placa, junto al microcontrolador AT89C51.

Cuando la interrupción generada se produce por parte del módulo Bluetooth, la cerradura está recibiendo una llave de acceso, se almacena la cadena de caracteres de forma temporal y se compara con los registros existentes en la memoria. Si la llave es localizada, ahora deben evaluarse las restricciones de acceso y la caducidad de la misma. Para esto, la cerradura cuenta con un RTC (Real Time Clock, Reloj de Tiempo Real) DS1302 y un microcontrolador AT89C2051 que está programado de tal manera que sincroniza las señales que el reloj necesita para guardar y solicitar la fecha y hora para validar el acceso.

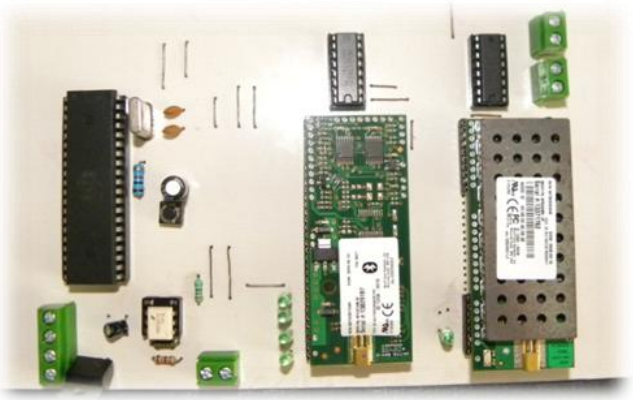

Figura 10. Módulos Bluetooth y Wi-Fi conectados al Microcontrolador AT89C51

De esta forma, el primer microcontrolador (identificado como maestro) solicita al segundo microcontrolador (identificado como esclavo) la fecha y la hora, respondiéndole este último, una cadena de caracteres que lleva la fecha y hora actual. Siguiendo un elaborado algoritmo, se efectúa la validación de las restricciones, verificando que se encuentre dentro del rango establecido por el sistema de control para ese día específico. Al terminar, el microcontrolador maestro puede resolver si le otorga el acceso o no, al usuario que lo ha solicitado, almacenando en el registro de eventos la llave recibida, la hora, la fecha y su resolución (falso o verdadero).

La elaboración del circuito de la etapa de potencia es fundamental para el funcionamiento de la cerradura al momento de que la clave sea validada. Para esto se cuenta con un MOC3010, un Triac MAC223, resistencias de 330 Ohms, 180 Ohms y 1.2 KOhms, capacitores cerámicos de 0.1 uF, un transformador de 12 VCA y por su puesto una contra eléctrica. Al pin número 1 del MOC3010 le corresponde al ánodo y es el que va a ir conectado directamente uno de los puertos del microcontrolador maestro de donde va a salir el bit en alto al momento en que se valide la clave, a su vez con el pin número 2, que le corresponde al cátodo del MOC3010 conectado a tierra, se provocará que los pines numero 4 y 6 se pongan en un nivel de alto activando la terminal 2 y el GATE del Triac MAC223 ocasionando un disparo que activa la contra. La figura 11 ejemplifica esta conexión. En caso de que el acceso sea denegado, el microcontrolador maestro encenderá un led, indicando que la llave no es válida.

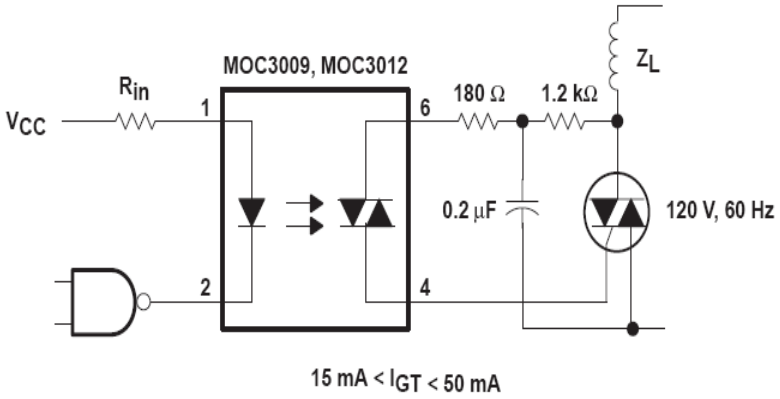

Figura 11. Sistema de la etapa de potencia.

3 Conclusiones.

El Sistema de Control de Acceso propuesto, es una respuesta a la demanda social existente en carácter de seguridad. La existencia de un delito genera una importante pérdida económica que alcanza a víctimas directas e indirectas, por lo que el objeto de la realización de este proyecto fue poder ofrecer una alternativa que permita ayudar a reducir estas mermas. Con este conjunto de aplicaciones propuesto, se busca dar solución a las necesidades básicas de seguridad que se detectan en hogares y negocios, teniendo entonces la encomienda de realizar un software adaptable al medio en que se desenvuelva.

El proyecto se encuentra en una etapa temprana de desarrollo, aun cuando los componentes de software están prácticamente terminados, la parte de la cerradura aun no ha sido finalmente desarrollada. Si bien los aspectos básicos de la comunicacion entre las aplicaciones ya han sido resueltos, aun quedan pendientes algunos detalles como el mecanismo secundario de acceso, en caso de que la carga del dispositivo móvil o el mismo celular fallen; asi como una mejora en el sistema de energía de reserva de la cerradura, en caso de que el suministro de energía falle, ya que la que actualmente cuenta, solo brinda 10 horas de respaldo en modo de espera.

Este proyecto innova en el uso de las tecnologías de la información y la comunicación en campos poco usuales, como la resolución de problemas sociales y específicamente la inseguridad, al mismo tiempo que combina diferentes áreas de las TIC, como redes inalámbricas y los sistemas embebidos. El aprovechamiento de todas las herramientas que ofrece el campo de la informática y la versatilidad de las comunicaciones a través de radiofrecuencias, en conjunto con el soporte de la electrónica, permite dar origen a una de las soluciones de software más creativas y revolucionarias en la región, al mismo tiempo que se explota la creciente dependencia de la sociedad en el uso de tecnologías de nueva generación, como lo es la vanguardia de los dispositivos móviles inteligentes, y la relación que estas guardan con sus actividades diarias.

Referencias.

1. L. Brito (2012,Junio). Robo a casa-habitacion repunto. *Criterio*. Disponible: http://www.criteriohidalgo.com/notas.asp?id=15997
2. V. Alvares (2011,Junio). Los robos mas frecuentes. *Periodico correo.*
3. COFETEL. *Suscripciones a teléfonos celulares móviles. Serie Anual a partir de 1990*. México: COFETEL, 2012.
4. COFETEL. *Telefonia movil penetracion 1990-2010*. México: COFETEL, 2008.
5. S. Galvez y L. Ortega. *Java a tope: J2ME (Java 2 Micro Edition).* España : S. Gálvez, 2003
6. J.Tomas Girones. *El gran libro de Android*. Mexico: Alfaomega, 2011.