risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 18/07/2016
Aceitação/Acceptance: 06/11/2016

Plataforma abierta de gestión de cámaras IP y aplicaciones móviles para la seguridad civil ciudadana

Juan P. D'Amato[1,2], Leonardo Dominguez[1,2], Alejandro Perez[1,3], Aldo Rubiales[1,3]

Juan.damato@gmail.com

[1] Instituto PLADEMA – UNCPBA, Campus Argentino, 7000, Tandil, Argentina.

[2] Consejo Nacional de Investigaciones Científicas y Técnicas, Av. Rivadavia 1917, Ciudad Autónoma de Buenos Aires, Argentina.

[3] Comisión de Investigaciones Científicas, Calle 526 e/10 y 11, La Plata, Argentina.

DOI: 10.17013/risti.20.48–61

Resumen: La inseguridad es un problema que afecta en mayor o menor medida a todas las ciudades del mundo. Las ciudades más informatizadas hacen uso de la video-vigilancia para combatirla, montando en muchos de los casos centros de monitoreo con cientos de cámaras. En su mayoría, estos centros cuentan con grupos de personas para realizar la tarea de observación, sin embargo, este método no es suficiente y los organismos públicos deben lidiar un reclamo social por mayor transparencia y eficiencia en el accionar ante un delito. En este contexto, es que surge el presente proyecto, una plataforma de administración de cámaras y sensores, para apoyar a la gestión integral de la seguridad. Esta plataforma complementa técnicas de análisis automatizado de video, junto con una API para registrar eventos de tipo alarmas o alertas por parte de la ciudadanía y permitir el acceso a otras entidades (policía, bomberos, organizaciones vecinales) a ciertos recursos (los videos). Toda la información se centraliza en un sistema georreferenciado, en una arquitectura abierta y escalable, organizado en diferentes capas de información, con un sistema de organización de roles de accesos. Se presenta una discusión de la estructura ideada, de los algoritmos utilizados para el seguimiento, problemas propios que se suceden en este tipo de sistemas y los resultados preliminares obtenidos.

Palabras-clave: Seguridad, Survillance, Plataforma abierta, Gobierno Digital.

Open platform managing IP cameras and mobile applications for civil security

Abstract: Insecurity is a problem affecting many cities in the world. Most developed cities are using video surveillance systems to fight crime, mounting huge monitoring centers with hundreds of cameras. Many of these centers have people observing cameras in order to detect suspicious situations. However, this is not enough and public governments must deal with a social demand for more transparency and efficiency in actions against crime. In this context, a camera and

sensor management platform to support comprehensive security management is presented. This platform complements automated video analysis techniques with a communicational API for recording alarms or alerts from applications. It also allows real-time access to protection forces (police, fire brigades, and neighborhoods) to resources such as maps and videos. All of the information is centralized in a geo-referenced system organized in different layers, and based on an open and scalable architecture with a role access system. This paper depicts typical challenges and problems of this kind of systems introducing a proposed structure and algorithms used for both monitoring and detecting events. Finally, preliminary results of implanting this platform in a real scenario are presented.

***Keywords**:* Security, surveillance, open platform, digital government.

1. Introducción

En los últimos tiempos, la seguridad se ha convertido en una de los intereses principales de las políticas de gobierno. La preocupación que generan en la sociedad los altos índices de violencia e inseguridad actuales (Kessler, 2009; Vásquez et al., 2016), motivan el estudio de nuevas tecnologías que permitan vivir con mayor tranquilidad a los habitantes. Este hecho se intensifica en grandes ciudades, donde estas lamentables situaciones son aún más frecuentes. Según (Dammert, 2010), entre el año 2000 y 2008, la tasa de población penitenciaria en América Latina, creció un 42%, y según las tendencias en los buscadores web, en los últimos 10 años el interés de las personas en términos como "Robo/Hurto" o "inseguridad" se encuentran en constante aumento.

Países como Estados Unidos, cuentan con agencias de investigación para la defensa de sus habitantes. En particular, la agencia DARPA, cuenta con más de 60 proyectos activos, de los cuales nos interesa mencionar a Satellite Remote Listening System y a *Combat Zones That See*, proyectos que tienen como objetivo registrar todo lo que se mueva mediante un sistema de videocámaras. Otro caso paradigmático es el de Reino Unido, que según (Watch Big Brother 2012), en su informe se estimaba que en Londres un individuo podía ser registrado en un día normal por aproximadamente 300 cámaras. Con un propósito similar, se inició el proyecto (Husim Project, 2012), el cual pretende a partir de una extensa red de sensores y dispositivos inalámbricos, controlar grandes áreas metropolitanas de forma inteligente.

En Latinoamérica, y en particular en Argentina, los municipios juegan un papel principal y activo en pos de lidiar con la inseguridad (Fernando Carrión, 2009). En general, para atacar este problema, se ha concebido el desarrollo de grandes centros de monitoreo, basados en tecnología de circuitos cerrados de cámaras. Este modelo comprende la instalación de una red compleja de video-cámaras distribuidas en toda la ciudad con una conectividad exclusiva, un software de gestión y almacenamiento de los videos. Estos videos se almacenan por períodos prolongados para su futura visualización o para ser utilizadas como evidencia judicial. La tarea de monitoreo la realizan grupos de personas observando y reportando sucesos tales como delitos o accidentes, de manera constante (24 horas al día), en horarios rotativos. En caso de un suceso, se recurre a los cuerpos policiales, ya sean del gobierno municipal o provincial, que realizan el control correspondiente y que actúan en conjunto a estos centros en la erradicación del delito.

1.1. Hacia un modelo de Gobierno Digital integrador

El nuevo modelo de gobierno digital pretende ser abierto y transparente, tal como lo plantea (Ixmatlahua, 2015). Un ejemplo: son las licitaciones, pago de impuestos, permisos, etc., los cuales son accesibles por cualquier empresa e interesado. Uno de los principales compromisos de los municipios es el acercamiento e interacción con sus habitantes, por lo que se desarrollan portales que ofrecen servicios digitales municipales para que los usuarios finales realicen los trámites en línea.

En el caso de la seguridad, el modelo de gestión basado en la observación de cámaras, ya adoptado en gran cantidad de ciudades del mundo y que hoy es un modelo que se sigue en Argentina, se ha visto que tiene muchas limitaciones.

Por un lado, en la metodología de trabajo. Ya es posible pensar en un software no solo de almacenamiento sino también con capacidades de análisis automático, que sea capaz de vigilar un área, emitir y registrar alarmas, clasificar y contar personas e incluso poder seguir sus movimientos. Este tipo de software, nos hace presuponer que será más ventajoso para los operadores, pues les permitirá focalizar su atención y estar alerta ante un evento importante. Existen variadas soluciones comerciales de Pelco® o Hanwha Techwin® que realizan estas tareas, pero son paquetes de software muy costosos y cerrados, es decir, los gobiernos quedan sujetos a la provisión y administración del software que provee la empresa que lo ha desarrollado. A su vez, los municipios suelen contar con otros sistemas que resuelven soluciones particulares (por ejemplo, botón de pánico o GPS para el seguimiento de patrullas o camiones recolectores de residuos), pero que no pueden integrarse al de monitoreo (o el costo es muy elevado). Ciertamente, este esquema de soluciones desacopladas atenta contra la transparencia del sistema y hace más complejo el mantenimiento e interacción entre ellas.

El siguiente tema importante es la infraestructura. Hoy en día, la responsabilidad de ampliar la red de cámaras y de gestionarla recae totalmente en el gobierno municipal. Esto significa incurrir en lentos y costosos procesos de adquisición e instalación de equipamiento y un costo elevado de manutención del mismo. En este sentido, la sociedad puede ser un partícipe más activo de la seguridad. Existen gran cantidad de cámaras IP privadas (es decir que pueden ser conectadas a una red en internet), que observan zonas públicas y que podrían ser utilizadas también en el proceso de monitoreo. Al mismo tiempo existen un sin número de smartphones con capacidades de grabación y transmisión que pueden generar información de valor.

Por otro lado, se cuestionan los mecanismos de acción seguidos ante un suceso delictivo. Los gobiernos dependen de su unidad de policías para accionar, siendo una entidad autónoma e independiente del centro de monitoreo. Esta separación de responsabilidades y metodologías para actuar ante un hecho de inseguridad hace que los procedimientos demanden a veces un tiempo muy elevado y que no puedan evitarse. Por ejemplo, si un operador de un centro de monitoreo municipal detecta un posible delito, debe realizar un llamado telefónico al departamento policial asociado, indicando el lugar y tipo del hecho. En esta comunicación surgen múltiples problemas que entorpecen la eficiencia de la acción, tal como diferencias de terminologías para describir el suceso. Al mismo tiempo, el acceso al "flujo de video" es vital para el rápido accionar de las partes. Esta información hoy es responsabilidad exclusiva de los centros de monitoreo, pero solo pasa a ser de dominio público cuando ha sucedido un hecho delictivo comprobado (ante una denuncia policial del individuo afectado). Ciertamente

esta secuencia es una acción "a posteriori", que termina haciendo lento el procedimiento de asistencia. Seguramente, si la información del video pudiese ser compartida en tiempo real entre los diferentes interesados, las acciones podrían ser más eficaces.

Por último, es importante nombrar que existen otras entidades privadas que comparten el mismo interés de protección ciudadana. Por un lado, las empresas privadas de seguridad, las cuales ofrecen servicios de control y acción privado. Ante una alarma, envía un vehículo de control para verificar la situación del inmueble de un individuo. En caso que se detecte un posible hecho delictivo, se llama al personal policial relacionado, el cual toma acción. Por otro, como una forma de control informal, existen organizaciones de individuos, que velan por la protección general. Estas organizaciones, trabajan en un radio geográfico muy cerrado y pueden llegar a tener una forma de comité de seguridad vecinal. Estos individuos trabajan en conjunto con el resto de las entidades, tanto públicas como privadas. Estas organizaciones también pueden aportar y aprovechar la accesibilidad a cierta información.

Entendiendo que la seguridad es un tema de interés, no solo en el ámbito social, sino también en el académico, es que ha surgido el presente trabajo. Nuestro proyecto es una plataforma distribuida que permite administrar y compartir a través de una solicitud web, un conjunto de cámaras IP en forma pública o privada, junto con una red de sensores. Esta idea surge como respuesta a esta creciente demanda social en materia de seguridad y en sintonía con el aumento constante en la instalación de cámaras de seguridad que apuntan a la vía pública. Sumando además una filosofía colaborativa que facilita el cumplimiento de una meta general: mayor seguridad social. El objetivo es permitir tanto a ciudadanos como a organizaciones públicas o privadas, administrar y compartir videocámaras utilizadas generalmente para vigilancia, de manera que otros individuos las puedan monitorear e integrar con otros sistemas de alertas. Utilizando los beneficios de montar el software en la nube, esta plataforma se vuelve escalable por lo cual la cantidad de cámaras a procesar y los usuarios para atender no serán un problema.

Esta plataforma contempla la automatización de tareas para la detección y seguimiento de personas y objetos en diferentes cámaras de video, de manera integral. Para esto, se trabaja con mapas geográficos que permiten ubicar un suceso en un mapa. Lo innovador de la plataforma es que se encuentra preparada para poder trabajar con múltiples técnicas de análisis automático. Su arquitectura abierta y distribuida, que contempla el uso de cámaras con procesamiento embebido, permite escalar el sistema para soportar muchas cámaras sin afectar el rendimiento global.

El trabajo se presenta de la siguiente forma. En la sección 2, se presentan las herramientas existentes con propósitos similares y un resumen del estado de arte. Posteriormente, en la sección 3 se mencionan los detectores utilizados y cómo se mapean al plano. En la sección 4 se presentan algunos resultados preliminares de los recorridos de una persona junto con las problemáticas encontradas, y en la sección 5 se presentan las conclusiones y los trabajos que quedan pendientes para un futuro.

2. Estado del arte

Actualmente existen una gran cantidad de sistemas de video vigilancia y en lo que respecta al seguimiento de personas hay mucha bibliografía reciente y es un tema muy estudiado en estos últimos años, en parte gracias al avance del poder de cómputo disponible en

los procesadores actuales. Desde el punto de vista algorítmico, en trabajos como (Serby, 2004), se detallan algunos de los métodos más comunes para la detección y seguimiento de objetos. En (Hall, 2005), se realiza una comparación interesante entre los distintos detectores, en donde se concluye que la combinación de los mismos puede ser muy útil para disminuir la tasa de falsos positivos sin comprometer el análisis en tiempo real. Más recientemente, en (Ojha, 2015) se revisan las estrategias generales para la clasificación y el seguimiento de personas en video y en (Kim, 2011) se plantea un método robusto en tiempo real, apto para el seguimiento de objetos a partir de predecir su velocidad y dirección. Además, en (Gómez-Conde, 2011) se describe un método denominado Motion Vector Flow Instance (MVFI), capaz de detectar actividades humanas complejas como "andar" o "hacer footing" en cámaras estáticas.

Considerando las soluciones integrales existentes, en (Gdansk, 2011) se hace una revisión de 18 sistemas de videovigilancia comerciales, y un resumen de los algoritmos más utilizados en etapas de detección, seguimiento, clasificación, detección de eventos y reconstrucción de trayectorias realizadas por distintos objetos. Por otra parte, debido al volumen de información que estos sistemas tienen que procesar, se discuten diferentes arquitecturas que abordan la problemática. En (Bramberger, 2006) se introduce un esquema distribuido basado en una red de procesadores con cámaras, que permite descentralizar el trabajo, pero se ve limitado en el tipo de cámaras soportadas. Si bien en trabajos como (Lin, 2012) y (Hassan, 2015) se utiliza la nube para resolver la escalabilidad de la plataforma, estos están orientados únicamente al procesamiento de video, descartando la integración de otros tipos de señales.

2.1. Legislación en Argentina

El esfuerzo de las autoridades por brindar mayor seguridad para sus ciudadanos, puede caer en un reto legal. Hoy en día existen debates sobre la vulnerabilidad de la privacidad por el aumento excesivo de sistemas de vigilancia. En Argentina, todavía nos debemos un gran debate para este tema.

La protección de datos en Argentina está tutelada en el artículo 43 de la Constitución Nacional y en la Ley 25.326 de protección de los datos personales del año 2000 y su decreto reglamentario 1558/2001.120. Con respecto a la regulación de la protección de datos personales es importante considerar no solo la normativa sino también el diseño institucional a cargo de implementar el contenido de la Ley Nacional de Protección de Datos Personales. El organismo encargado de velar por el cumplimiento de la ley es la Dirección Nacional de Protección de Datos Personales (DPDB). Esta Dirección se encuentra cuestionada y revisada a nivel social. Además, la Ley 26.388 modificó el Código Penal y agregó el artículo 157 bis, que contempla pena de prisión –agravada para funcionarios públicos que violen sistemas de confidencialidad y seguridad de datos. La Ley define como datos personales a la "Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables" y su artículo 10 dispone el deber de confidencialidad.

La normativa de protección de datos de Argentina fue calificada por la Comisión Europea como adecuada con arreglo a lo dispuesto por la Directiva del Parlamento Europeo.122. Con respecto a la propiedad de los datos de video, no existe normativa específica, acerca de la accesibilidad y disponibilidad de esta información. Según el artículo (Cejas, 2015), el 87,5% de las provincias argentinas no cuentan con una regulación adecuada o completa,

y sus autores destacan la gran disparidad en el plazo de almacenamiento establecido de las imágenes previo a su destrucción, que va desde los 30 días en Santa Fe, a los 2 años en Corrientes y San Luis. Además, señalan que la mayoría de las regulaciones no se adaptan a los principios establecidos por la disposición 10/2015 de la DNPDP.

Por último, es importante mencionar que el Ministerio de Seguridad Argentino en su resolución 12/2015, aprueba el protocolo de actuación para la implementación del sistema de alerta y localización georreferenciada de "Botón de Pánico". Este protocolo contempla los pasos de aprobación y las formas de presentación adecuadas, además de identificar los diferentes actores en la acción. Siguiendo la base de este protocolo, pueden concebirse otros protocolos para aplicarse en el desarrollo de la presente plataforma.

3. Plataforma propuesta

La plataforma contempla la integración de cámaras IP, junto con herramientas de análisis automático y un gestor de eventos geo-referenciados, preservando y controlando el acceso a los datos.

Esta funcionalidad, se agrupa por capas, cada una contemplando diferentes módulos y tecnologías distribuidas. En la Figura 1, se muestran los diferentes componentes de la arquitectura. En las siguientes secciones se describen en detalle cada uno de los módulos.

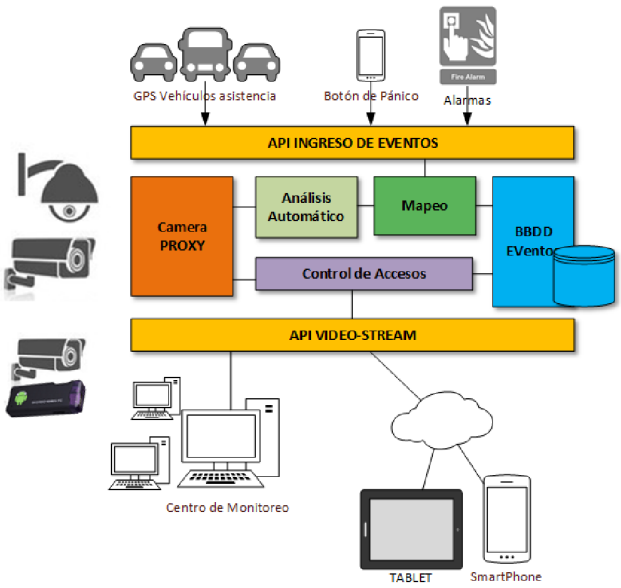

Figura 1 – Arquitectura en módulos

3.1. Servidor de cámaras.

Un servidor proxy hace de intermediario en las peticiones de recursos que realiza un cliente a un servidor. Esta situación estratégica de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a

determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc. Dependiendo del contexto, la intermediación que realiza el proxy puede ser considerada por los usuarios, administradores o proveedores como legítima o delictiva y su uso es frecuentemente discutido.

Cuando un equipo de la red desea acceder a una video-cámara, el proxy es quien realiza la comunicación, ocultando la dirección exacta de la cámara y a continuación traslada el resultado al equipo que la solicitó.

En este caso el que quiere implementar la política es el mismo que hace la petición. Es posible controlar el tráfico y establecer reglas de filtrado, e incluso generar videos de diferente resolución o con diferentes *codecs* (re-codificar).

En general, este servidor proxy permite:

- Control: se pueden limitar y restringir los derechos de los usuarios.
- Ahorro: los flujos de video, se pueden replicar para reducir la cantidad de conexiones.
- Velocidad: si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida.
- Filtrado: el proxy puede negarse a responder algunas peticiones si detecta que están prohibidas e incluso aplicar reglas dinámicas.
- Adaptabilidad: el servidor proxy puede adaptar las conexiones de video, de acuerdo al cliente. En caso una baja velocidad de conectividad, el servidor puede bajar la calidad del mismo, a fin de preservar la conexión.

3.2. Detección automática de eventos

El primer paso para la detección de eventos, es poder determinar si hubo o no movimiento a partir de una serie de imágenes. Este problema, es análogo al problema de sustracción de fondo, el cual se encuentra muy estudiado. Ya existen múltiples soluciones para poder calcular la variación entre imágenes consecutivas (Shaikh, 2014)(Piccardi, 2004). Los métodos varían en complejidad computacional y eficacia del resultado.

Cuando las cámaras son exteriores, se suceden otros factores que además varían dependiendo del momento del día, la nubosidad y la época del año. Para contrarrestar estos efectos, se suelen utilizar ventanas de movimiento como se menciona en (Kruegle, 2011), cuyo objetivo consiste en aplicar una operación lógica, para procesar únicamente los movimientos que se detecten dentro de sus dimensiones y descartar todos aquellos que se produzcan por fuera. En general, la salida de este paso es un conjunto de píxeles (agrupados o no) que han sido marcados como representativos de objetos en movimiento. Otro fenómeno que afecta la detección, es la sombra proyectada por los objetos. Hoy se están probando con otros algoritmos, tal como VIBE (Bouwmans, 2014) que apuntan a reducir estos problemas.

Estos algoritmos tienen un elevado costo computacional. Para mejorar la eficiencia del sistema general, se concibió la idea de llevar el procesamiento a la ubicación de la video-cámara. Para esto, se diseñaron gabinetes estancos, con la capacidad de alojar PCs reducidas, conectadas directamente a la cámara. Estas PCs, realizan el análisis de

los objetos y transmiten a la central el resultado obtenido, junto con la imagen del video. Las cámaras pueden ser gestionadas desde la central. Para la plataforma, se extendieron las capacidades de paquetes open-Source, como AForge®, OpenCV® y Accord®. Los algoritmos de seguimiento, se desarrollan en conjunto con herramientas de análisis por zonas o de barreras virtuales, como se muestran en la Figura 2.

Figura 2 – Visualización de zonas y barreras virtuales

En caso que se detecte un movimiento en cada zona, se determinan sus características (tamaño del objeto, frecuencia de aparición). En caso que estos objetos requieren atención, se generan alarmas visuales o sonoras para el operario. Esta misma alarma, se registra por duplicado (en el gabinete estanco y en el sistema central) como un evento y se geo-localiza en el mapa.

3.3. API para la notificación eventos

Los sistemas de monitoreo basados en video hoy se complementan con sistemas embebidos, tal como alarmas por robo, fuego, o accidente, siendo muchas veces aplicaciones para móviles. Las entidades públicas son las responsables de definir los protocolos y de centralizar los medios de comunicación, en pos de una plataforma abierta y extensible. En este sentido, el fin es permitir que cualquier desarrollador independiente o empresas privadas, pueda crear software para generación y observación de los eventos.

Por un lado, para conectar estos sistemas externos con la plataforma propuesta, se define una API de comunicación, que permita la carga de información de un evento y, en los casos permitidos. brindar acceso a una imagen de video cercana al suceso o emitiendo una nueva alerta. Por el otro, es necesario un proceso de aprobación del desarrollador y su propuesta.

La intención es preservar condiciones de seguridad y privacidad de los datos. De momento, para evitar que cualquier sistema se haga uso indebido de la API, se contempla que cada aplicación tenga una clave de autenticación provista por el usuario. En un futuro, se contempla aplicar un protocolo de registración y seguimiento de la aplicación y del equipo de desarrollo, tal como hoy se aplica en la legislación para el Botón de Pánico en Argentina (Ministerio De Seguridad, res. 12/2015).

Los sistemas externos generan información de los eventos. La información que debe entregarse es:

- Posición geográfica del suceso, en formato LAT-LONG
- Fecha de generación
- Tipo de evento (de acuerdo a una especificación de la plataforma)
- Código de registro de la aplicación
- Usuario

La plataforma internamente llevará información que hace al tratamiento del evento generado y a quién (o quienes) se debe recurrir en cada caso.

- Criticidad de su atención
- Recursos accesibles ante este evento
- Tiempo del permiso
- Información del responsable de atención

En la Tabla 1, se hace un ejemplo de tipos de eventos registrados y los responsables:

Evento	Criticidad	Responsable	Recurso	Acción
Accidente automovilístico	*Alta*	*Policía* *Sanidad* *Monitoreo*	*Cámaras cercanas* *Mapa de ubicación*	*Envío de alerta*
Intrusión en zona de exclusión	*Media*	*Monitoreo* *Organismo vecinal*	*Cámaras cercanas*	*Verificación visual*
Botón de pánico	*Alta*	*Policía*	*Mapa de ubicación*	*Envío de alerta*
Vehículo en camino rural	*Media*	*Monitoreo*	*Cámaras cercanas*	*Registro de la información* *Verificación visual*
Asistencia general	*Baja*	*Monitoreo* *Policía*	*Mapa de ubicación*	*Ninguna*

Tabla 1 – Ejemplos de eventos y las acciones relacionadas

3.4. API Video-Stream

De forma análoga a lo explicado recientemente, esta API define un modo de comunicación del sistema con los interesados en compartir sus videocámaras.

Mediante una solicitud web, el usuario ingresará la dirección de acceso a la cámara, su nombre y sus coordenadas para que un administrador del sistema, en caso de considerar que la cámara sea relevante, le envíe un usuario y una contraseña de acceso a la plataforma.

Dependiendo de la situación de cada usuario (cámara, tipo y velocidad de conexión, etc.), se podrá acceder a la cámara en forma directa mediante el protocolo RTSP o P2P. Actualmente, en la plataforma se utiliza el RTSP.

3.5. Control de accesos

Los videos y el acceso a mapas de ubicación contienen datos sensibles, los cuales deben ser manipulados cuidadosamente. Para el acceso a esta información se propone un esquema de roles/permisos limitados en un rango de distancia geográfica. Cada aplicación tiene

asociado un usuario/grupo de usuarios con rol, y cada rol tiene acceso a los recursos habilitados. Estos solo pueden ser accesibles en periodos determinados de tiempo, y no pueden ser reincidentes por ciertos plazos, para evitar el mal uso de esta información (por ejemplo, usar el mapa de ubicación de la policía para realizar un hurto).

Dependiendo de los casos, los recursos pueden ser gestionados manualmente, desde el centro de monitoreo asociado o de manera automática, siempre que cumpla las condiciones prefijadas.

Para agilizar las gestión y acceso de los usuarios/interesados en acceder a los recursos, se propone un esquema de organización por georreferencia. En caso de un evento/alerta, el sistema localiza el suceso y verifica las cámaras cercanas. A continuación, verifica los permisos de acceso y habilita o deniega el acceso de la solicitud. En caso que sea necesario, un operador puede hacer una validación previa.

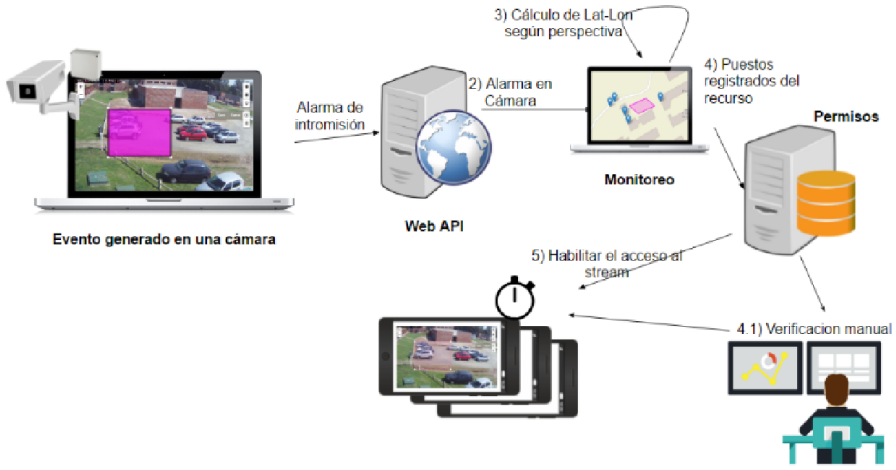

Figura 3 – Esquema de alerta y atención ante una alarma

En la figura 3, se muestra un esquema de cómo se gestiona un evento de intrusión, detectado de manera automática

4. Consideraciones para la puesta en marcha

La plataforma propuesta se encuentra en funcionamiento a nivel de prototipo y en constante desarrollo por parte del presente grupo. Se ha instanciado en un campus universitario, ubicado en la ciudad de Tandil, Argentina. Este campus tiene una superficie de más de 30 hectáreas, en la cual se han distribuido más de 10 cámaras de control de acceso y durante el 2017 se sumarán otras 40 más. Estas cámaras se conectan a través de una red interna de la universidad, con una velocidad promedio de 100 mbps. Para enriquecer la plataforma, también se han añadido 5 cámaras privadas, ubicadas dentro de la ciudad.

Todas los *streams* de los videos se registran y gestionan a través de una versión de escritorio de la plataforma, que puede ser administrada en su totalidad. La Base de Datos utilizada es SQL Server, con una licencia para educación, aunque puede funcionar en otras de licencia libre. A su vez, a través de un portal web, implementado en el framework AngularJS, se permite acceder a estas cámaras, y así detectar las zonas observadas. Este portal funciona conectado al servidor proxy que es gratuito y open source ("Camera Proxy", disponible en la WEB), ha sido configurado para bajar la resolución de las cámaras, en caso de una baja conectividad. Las capas de servicios (APIs) se implementaron en el framework ASP.NET Web API 2 de Microsoft. El control de acceso se implementa bajo el protocolo de autenticación OAuth2. El módulo web puede también ser accesible a través de móviles y tablets, con una interfaz adaptable, incluso en redes 3G. Este portal puede ser accesible en http://camaras.plademа.net/ (solicitar acceso al autor de referencia).

Figure 4 – (arriba) Herramienta para configuración y calibración de cámaras (abajo) vista del portal WEB para acceder a un flujo de video.

Los diferentes componentes de software de la arquitectura corren en un ambiente virtualizado (servidor proxy, api, herramientas de análisis automático, bases de datos), dentro de una red local. Al mismo tiempo, se desarrolló una aplicación Android del tipo "Botón de Pánico" y "Alarmas", la cual genera una señal de alerta indicando la posición geográfica donde se origina, utilizando la API nombrada. En base a un

evento de este tipo, se generan una serie de alertas que son manejadas en tiempo real. Dos de las cámaras, cuentan con capacidades de procesamiento embebido, por lo que toda la tarea de procesamiento se realiza en la misma. Estas cámaras son especialmente robustecidas para soportar las inclemencias del tiempo. Este modelo de procesamiento distribuido acelera los tiempos de detección de eventos automáticos y reduce las necesidades de conectividad de alta calidad. Este proyecto se encuentra en tratativas para la prueba en el municipio local, por lo cual los detalles técnicos no pueden ser aún publicados**.**

5. Conclusiones

En este trabajo se presentó una plataforma distribuida para la gestión de múltiples cámaras y sensores, con el soporte para la gestión integral de eventos. La plataforma contempla la definición de una API para integrar aplicaciones externas, la manipulación de cámaras IP propias de un organismo o externas, aplicando un control de los accesos a través de un servidor proxy.

A su vez, se han desarrollado y aplicado diferentes técnicas de sustracción de fondo para detectar objetos de interés y luego visualizarlos en un espacio georeferenciado, amigable para el usuario. La plataforma es muy configurable, permitiendo distribuir la funcionalidad de procesamiento, visualización y seguimiento en cualquier equipo. Las aplicaciones propuestas mantienen un enfoque orientado hacia una ciudad digital puesto que no son simplemente fragmentos heterogéneos sin ninguna conexión, sino que son elementos que forman parte de una estructura integral.

En un trabajo futuro, se pretende perfeccionar las técnicas de análisis y la incorporación de nuevos tipos de dispositivos que funcionen como disparadores de eventos. La idea es a su vez integrar otros protocolos de accesos a las cámaras basadas en P2P y tener capacidades de procesamiento que permitan ejecutar los distintos algoritmos en un entorno *cloud*.

Agradecimientos

Este proyecto se emplaza en la infraestructura de conectividad provista por la Universidad Nacional del Centro de la Prov. de Bs. As (UNCPBA). El presente proyecto ha recibido subsidios de la Secretaría de Políticas Universitarias de la Argentina (convocatoria Universidad y Transporte, proyecto 32-64-055).

Referencias

Big Brother (2012), Watch Big Brother. The price of privacy: How local authorities spent£ 515m on cctv in four years. A Big Brother Watch report.

Bouwmans, T., Porikli, F., Höferlin, B., & Vacavant, A. (Eds.). (2014). Background Modeling and Foreground Detection for Video Surveillance. CRC Press.

Bramberger, M., Doblander, A., Maier, A., Rinner, B., & Schwabach, H. (2006). Distributed embedded smart cameras for surveillance applications. *Computer*, 39(2), 68–75. DOI: 10.1109/MC.2006.55

Cejas, E., & González, C. C. (2015). Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales. In *Simposio Argentino de Informática y Derecho (SID 2015)*-JAIIO 44 (Rosario, 2015).

Dammert L., Salazar F., Montt C., and González P. (2010) Crimen e inseguridad: indicadores para las américas. *FLACSO-Chile/Banco Interamericano de Desarrollo (BID)*. Ediciones Flacso

Fernando Carrión M., Jenny Pontón C., Blanca Armijos V. (2009), 120 Estrategias y 36 experiencias de seguridad ciudadana, *Revista Latinoamericana de Estudios de Seguridad*. Ediciones Flacso.

GDANSK (2011). Review of existing smart video surveillance systems capable of being integrated with ADDPRIV project.

Gómez-Conde, I., Olivieri, D. N., & Vila, X. A. (2011). Método espacio-temporal para el reconocimiento de acciones humanas en el espacio canónico. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (8), 1–14.DOI: 10.4304/risti.8.1-14

Hall, D., Nascimento, J., Ribeiro, P., Andrade, E., Moreno, P., Pesnel, S., ... & Crowley, J. L. (2005, October). Comparison of target detection algorithms using adaptive background models. In *2005 IEEE International Workshop on Visual Surveillance and Performance Evaluation of Tracking and Surveillance* (pp. 113-120). IEEE. DOI: 10.1109/VSPETS.2005.1570905

Hassan, M. M., Hossain, M. A., Abdullah-Al-Wadud, M., Al-Mudaihesh, T., Alyahya, S., & Alghamdi, A. (2015). A scalable and elastic cloud-assisted publish/subscribe model for IPTV video surveillance system. *Cluster Computing*, 18(4), 1539–1548. DOI: 10.1007/s10586-015-0476-2

Husim Project (2012). Celtic Telecommunication Solutions. Husims-human situation monitoring system, 2012. Link =https://www.celticplus.eu/wp-content/uploads/2014/09/HuSIMS leaflet lq.pdf.

Ixmatlahua, S. D., Raygoza, R. O., Romero, O., Uribe, F., & Vargas, E. J. (2015). Metrópoli Digital: Una plataforma Web para la inclusión integral de las PyMES, Sociedad y Gobierno en el uso de las Tecnologías de la Información en la región de las Altas Montañas del estado de Veracruz, *México*. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informaçã*o, (SPE3), 43–54. DOI: 10.17013/risti.e3.43-54

Kessler G (2009). El sentimiento de inseguridad: sociología del temor al delito. Siglo Veintiuno Editores.

Kim, J. S., Yeom, D. H., & Joo, Y. H. (2011). Fast and robust algorithm of tracking multiple moving objects for intelligent video surveillance systems. *IEEE Transactions on Consumer Electronics*, 57(3), 1165–1170. DOI: 10.1109/TCE.2011.6018870

Kruegle, H. (2011). CCTV Surveillance: Video practices and technology. Butterworth-Heinemann.

Lin, C. F., Yuan, S. M., Leu, M. C., & Tsai, C. T. (2012, September). A framework for scalable cloud video recorder system in surveillance environment. In *Ubiquitous intelligence & computing and 9th international conference on autonomic & trusted computing (UIC/ATC), 2012 9th international conference on* (pp. 655-660). IEEE. DOI: 10.1109/UIC-ATC.2012.72

Ojha, S., & Sakhare, S. (2015, January). Image processing techniques for object tracking in video surveillance-a survey. In *Pervasive Computing (ICPC)*, 2015 International Conference on (pp. 1-6). IEEE. DOI: 10.1109/PERVASIVE.2015.7087180

Piccardi, M. (2004, October). Background subtraction techniques: a review. In Systems, man and cybernetics, 2004 IEEE international conference on (Vol. 4, pp. 3099-3104). IEEE. DOI: 10.1109/ICSMC.2004.1400815

Serby, D., Meier, E. K., & Van Gool, L. (2004, August). Probabilistic object tracking using multiple features. In *Pattern Recognition*, 2004. ICPR 2004. Proceedings of the 17th International Conference on (Vol. 2, pp. 184-187). IEEE. DOI: 10.1109/ICPR.2004.1334091

Shaikh, S. H., Saeed, K., & Chaki, N. (2014). Moving Object Detection Using Background Subtraction. In *Moving Object Detection Using Background Subtraction* (pp. 15-23). Springer International Publishing. DOI: 10.1007/978-3-319-07386-6_3

Vázquez, M. Y. G., Sexto, C. F., Rocha, Á., & Aguilera, A. (2016). Mobile Phones and Psychosocial Therapies with Vulnerable People: a First State of the Art. *Journal of Medical Systems*, 40(6), 1–12.