The Safety Transformation in the Future Internet Domain

Roberto Gimenez[1], Diego Fuentes[1], Emilio Martin[1], Diego Gimenez[2], Judith Pertejo[2], Sofia Tsekeridou[3], Roberto Gavazzi[4], Mario Carabaño[5], and Sofia Virgos[5]

[1] HI-Iberia Ingeniería y Proyectos
{rgimenez,dfuentes,emartin}@hi-iberia.es
[2] ISDEFE
{dgimenez,jpertejo}@isdefe.es
[3] Athens Information Technology - AIT
sots@ait.gr
[4] Telecom Italia
roberto.gavazzi@telecomitalia.it
[5] Everis
{mario.carabano.mari,sofia.virgos.casal}@everis.com

Abstract. Public Safety is nowadays a priority, cornerstone and major concern for governments, majors and policy makers in current (and future) smart cities. Notwithstanding the foregoing, large advances in ICT technologies are foretold to revolutionize our society and enhance our feeling of safety (and hopefully, wellbeing). This chapter presents an introduction to three of the most promising technological pillars considered to be spearheads in this transformation: Internet of things, understood as the data capillarity through billions of sensors, Intelligent Video Analytics and Data Mining Intelligence, the latter two enabling smarter contextual awareness and prediction of potential threats leading to proactive prevention of them. The associated horizontal economic implications of this evolution and its impact into the societal and economic fabric are also tackled. Part of the results and analysis produced in this chapter are the outcome of the work carried out in the FP7 EU project SafeCity, one of the eight Use Cases of the FI Programme.

1 The Undergoing Safety Evolution in the Future Internet

A large urban growth has been recorded throughout the world within the last decade. Such population increase in cities has implied an equally pressing demand for vital public services such as transport, health, education or city security and citizens' protection. Protecting citizens is one of the key factors for a government and also a priority for the normal functioning of businesses, communities and civil society at large. Safety in the cities is becoming more and more complex due to the constant increase of city population and of city infrastructures complexity. In this sense, cities and countries' authorities have made a great effort in applying innovative approaches and new technologies in the Public Safety domain in recent years, especially in order

F. Álvarez et al. (Eds.): FIA 2012, LNCS 7281, pp. 190–200, 2012.

to reduce emergency response time and urban crime: for example, digital surveillance cameras have been placed in many critical areas and buildings throughout cities and call dispatchers have been created to distribute the emergency calls. Moreover, advanced technological capabilities facilitate urban public safety systems to become not just more interconnected and efficient, but also smarter and self-adaptive. Instead of merely responding to crimes and emergencies *after* a critical situation, novel smart systems emerge to analyse, anticipate and, actually, contribute to *preventing* them before occurring. After the terrorist attacks of March 2004 in Madrid, the city developed a new fully *integrated Emergency Response Centre* which, after an incoming emergency call, simultaneously alerts the required emergency agency (police, ambulance and/or fire brigade). The system can recognize if alerts relate to a single or multiple incidents, and assign the right resources based on the requirements coming from the ground. Furthermore, specialized video analytics systems are successfully installed for traffic surveillance purposes. These are CCTV-based systems capable of automatically detect illegal vehicles behaviour (e.g. cars stopped in forbidden areas, going in the opposite direction), restricted entries behaviour (e.g. bike entering in a forbidden road), stolen vehicles, etc. In addition, *M2M communications*, that is, intelligent communications by enabled devices *without* human intervention, are nowadays present in home and industrial security monitoring systems and alarms. Several Public Safety organizations and Public Administrations are using sensor networks to monitor environmental conditions or to be temporally deployed driven by an emergency situation. Other advanced technologies are focused on enhancing emergency notification mechanisms, fire and enforcement records management, surveillance, etc.

As presented, outstanding capabilities offered by advanced technologies are currently in use for safety purposes. However, there is still a wide list of non-satisfied safety capabilities requested by Public Safety agencies. Several on-going initiatives research upon how *Future Internet* can assist these entities in their daily work and during emergency response phases. That is the case of **SafeCity** (Future Internet Applied to Public Safety in Smart Cities) [1], an EU-funded project under the FP7 FI-PPP programme which proposes to enhance the role of Future Internet by developing smart Public Safety applications of high value. SafeCity aims at significantly improving the implementation and up-taking of Future Internet services in this safety field by 2015, leveraging the internet infrastructure as the bases of Public Safety centred open innovation schemes. It is focused in situational awareness (i.e. surveillance of public facilities, transport stations, energy facilities, roads, citizens in the streets; environmental monitoring), decision-making tools in C2 centres, seamless usage of ad-hoc communication networks temporarily deployed to support additional demand communication capacity (e.g. due to a major plan event) and alerting population mechanisms.

This paper presents the state-of-the-art and on going advances in these three vital technological fields (*Internet of things, Intelligent Video Analytics* and *Data Mining intelligence*) that are envisaged as fundamental pillars of the FI infrastructure in the Public Safety domain. It further continues discussing and concluding on what the economic implications of such technological advances for Safety purposes are.

2 Internet of Things, the Billion of Billions Connected Devices When Applied to Safety

The evolution from the City of today to the future "Smart and Safe" City will be highly driven by the introduction of advanced digital and ICT technologies. The city will be submerged by millions of simple and sometime tiny devices: sensors, meters, actuators that will represent the city's organs of sensing. All these millions devices shall be connected through a capillary network reaching all the peripheral devices. Like in the human body, there will be peripheral sensing organs connected through a peripheral nervous system to transmit the collected data to the central nervous system i.e. the brain. The brain is the set of command and control centers of the city; there, a diverse set of applications resides, a part of which are dedicated to citizens' protection and city infrastructure safety. The theoretical model for IoT services in the Smart City is the sensing – actuating infinite loop.

To realize and put in place such a complex command and control system, it is necessary to be based on a standardized ICT reference architecture tackling data networks connectivity and diverse IT application platforms interoperability. Such reference architecture is shown in Figure 1.

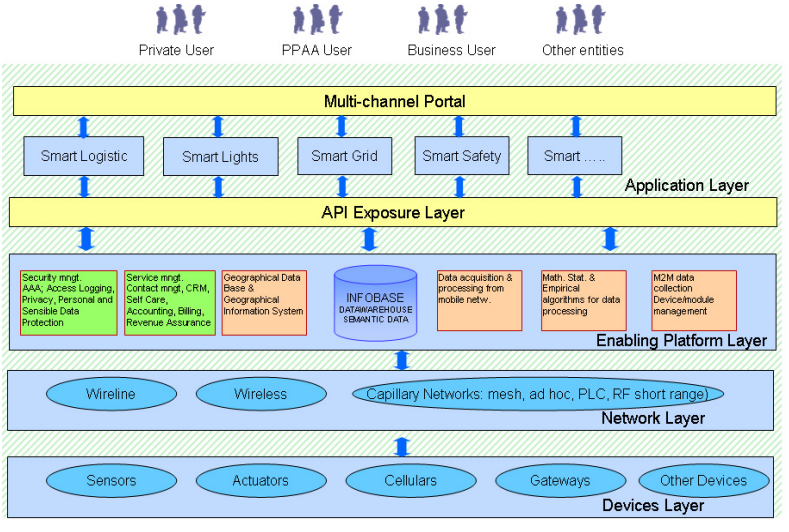

Fig. 1. Architecture and infrastructure model for IoT services in a Smart City

The reference architecture consists of different layers: Devices Layer, Networks Layer, Enabling Platform Layer and Applications Layer. The Devices Layer is composed by many types of smart devices (meters, actuators, sensors, etc.) that have both computation and data transmission capabilities. Many theoretical studies are considering which can be the best frequency in the spectrum to be allocated for short range RF devices. The GHZ frequency range seems not so suitable due to the very short geographical coverage and to the high sensitivity to electromagnetic noise.

So the bands of frequency currently under consideration in Europe are: 169 MHZ and 868 MHZ. All the devices need to be managed by a M2M (Machine To Machine) Platform with the following main features: open and standard interface with devices, open and standard interface with applications, legacy, non standard, adapters, devices and applications self discovery and identity management (access controls), connectivity management (session, mobility), content management (QoS), security, privacy and trust, service management (auto provisioning, auto configuration, self healing, SW and FW upgrade, ...) for applications and devices, asset management (SIMs Card for example), etc.

The Enabling platform layer besides M2M platform shall host also databases to manage big quantity of data and data mining capability to extract "Meaning" from the huge amount of data (see chapter 4). Capabilities of video analytics can also be part of the enabling platforms as enabling capabilities for many application based on image recognition (see chapter 3). Geographical localization of devices is also important to intervene in the geographical area impacted.

Finally, the application layer is where the various applications reside. The applications use web services APIs provided by the enabling platform layers. The architecture is based on state of the art of web 2.0 techniques like [2]: Service-Oriented Architecture (SOA), Software as a Service (SaaS), Mashups or Structured Information. The SOA (OASIS Reference Model for SOA#) is an architectural paradigm for integrated services available on the Net and owned and managed by different entities. With SaaS, the software for implementing services is not locally installed and self contained (an example of SaaS is world editor not installed on the computer where the editing is done, but available in the Net). Mashup techniques are based on SOA and enable to integrate different services to create a new and original service that can be as well available in the Net for future mashups. Last but not least, XML family languages have enabled the exchange of structured information between applications in the Net without any previous design phase in the databases. Regarding data connectivity the debate is open and research is on going to assess if public networks can be reusable for safe city applications. The main consideration in favor of a re-use of current commercial IP networks is that they are already in place while to build a specific network infrastructure for the smart city case would require efforts, time and money that cannot be spared (not to mention network planning and management).

Safety applications will leverage the IoT platforms described previously; in particular the capillary network hot spots will be very important points for installation on the territory of safety oriented sensors and actuators. First of all the IP Cameras sending video streaming in Real Time can be managed as "Smart Things" both in terms of data collection and in terms of operation management (maintenance in case of faults). The capillary networks hot spots can also be the points of installation of tools for alerting citizens. The alerting phase in safety services is very important. When there is some emergency situation, citizens shall be informed as soon as possible especially citizens close to the emergency areas. To alert citizens, Digital Signage panels or totem can be installed in the capillary networks points. Moreover through broadband connections it shall be possible to send alerting messages directly to the mobile devices of the citizens in the Area or close to the area using for example WiFi short range connections. To summarize the IoT is important for the safety smart services and eventually safety smart services can defined as IoT services.

3 The Radical Change That Intelligent Video Analytics Is Bringing to Safety in Smart Cities

A common problem in the operation of video surveillance systems is the sheer volume of information: there may be thousands of cameras installed, and it is simply impossible to physically monitor all of them on 24/7 basis. Furthermore, it is relatively easy to "fool" an operator by innocuous-seeming appearance or behavior. The wide deployment of digital video surveillance has led to computers replacing human operators and security personnel in order to efficiently monitor and analyze video footage in real-time and trigger alerts not affected by human fatigue and distraction as in the case of human operators. Video Analytics (VA) is about the use of dedicated software and hardware to analyze captured video and automatically identify specific objects, events, behavior or attitudes in video footage in real-time. Video analytics enables video surveillance to become a proactive monitoring tool that signals the need for immediate intervention by guards, police, or other security personnel. Video surveillance systems become thus more efficient being able to automatically recognize situations and trigger alarms or other actions (such as door locking). With video analytics acting as a remote observer (as shown in Figure 2), security personnel may receive notifications of an intruder or other suspicious event, and potentially act before a crime takes place – this added value brought around is crucial for crime prevention and safer cities.

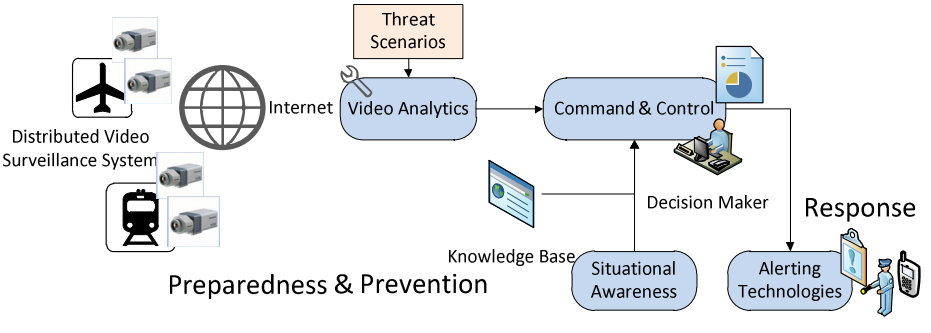

Fig. 2. Video Analytics in the landscape of a Smart and SafeCity

Given the explosion in the amount of video footage captured by security forces, the need to develop automatic intelligent methods for detecting suspicious people, objects or activities in video to trigger immediate alerts or further analysis has been widely recognized. Intelligent video analytics tools have been emerging for that purpose, deployed in the safety domain. However, recognizing objects and people in loaded scenes, identifying a person based on gait, recognizing complex behaviors and conducting analytics in multi-camera systems are still among the main challenges of research in this field. In video analysis, a monitored scene is visually analyzed to extract foreground, eliminating all irrelevant background information to the understanding of the problem at hand. A large number of methods exist, including adaptive Gaussian mixtures [3], which can be used together with shadow filters [4].

When medium or close field video streams are available (depth info), then more sophisticated scene analysis can be provided, e.g. body shapes and regions can be extracted. The dynamics of the evolving scene are interpreted and, according to the density and clutter in the scene, it may be possible to track single persons or moving objects, even in complex scenes. Multiple cameras with overlapping fields of view allow for 3D tracking. Such methods are heavily based on the quality of features detected (appearance, shapes etc.) and fail if image primitives are not reliably detected. There are approaches that attempt to infer events without construction of models. The detection of complex motion using motion models based on HMMs (Hidden Markov Models) targets to detect abnormal events in complex scenes. Apart from building models, the extracted information is used to recognize the event, usually under assumptions/rules. Other methods achieve event recognition by relying on both low-level motion detection and tracking, and high level recognition of predefined (threat) scenarios corresponding to specific behaviors.

Advancements in video analytics technology have increased recognition abilities, dramatically reducing false alerts due to weather, sun positions, and other environmental factors. Some of today's video analytics capabilities, along with safety example cases that these may handle, include:

- Character (e.g., alphanumeric) and inscription recognition for reading license plates, name tags, and containers; for e.g. suspicious parked cars detection.
- Facial recognition; for criminal/terrorist identification in public places (metro, airport, large public squares, etc.)
- Density of people, people counts, behavior (such as loitering, fighting, reading, sampling), slip-and-fall detection, gang activity, tailgating (vehicle or human) in restricted areas, a person coming over a fence;
- Object removal and tracking; for e.g. theft detection cases
- Smoke detection; for potential fire detection
- Pattern recognition and directional motion;
- Tampering (such as with ATMs or other devices);
- Illegally parked cars, unattended bags, spills; for citizens' protection
- Camera sabotage or malfunction, etc.; for crime intention detection

Intelligence and detection accuracy increases when one combines many of the above capabilities together, or fuses detection results from the analysis of diverse data/sensor inputs in an IoT infrastructure. For example, it is now possible to allow entrance to a secure building by linking a fingerprint with a face and a person's voice, as well as personal handwriting, requiring all to match before granting access. Today's intelligent video analytics systems can even spot potential problems by analyzing how people move in multi-camera crowded scenes – many video streams are analyzed simultaneously flagging suspicious people or objects, directing security personnel to focus on particular activities. Artificial intelligence combined with video analytics adds an intelligence layer, allowing learning of patterns while analyzing and dropping false alarm rates. Finally, the use of both server-based (up to now the prevailing architecture) and embedded, on-camera video analytics has led to even better performance and lower energy and bandwidth consumption.

Nowadays, there is another great challenge to be faced due to the great demand for respect for citizen's privacy in order to retain public trust. The Anonymous Video

Analytics (AVA) technology has emerged for that purpose [5], which uses pattern detection algorithms to scan real time video feeds, looking for patterns that match the software's understanding of faces. The data is logged and the video destroyed on the fly – with nothing in the process recognizing the persons who passed in front of the sensors. In safety applications, only the identity of suspicious people, logged in a database, is found and revealed. The advantages of intelligent video analytics for enabling safe cities as Future Internet applications in combination with other technologies, such as sensor networks or data mining, fusion and decision support, are thus numerous.

4 The Data Mining Intelligence in Smart Cities for Safety

Data mining has become the third key feature of many safety initiatives in smart cities. Often used as a means for detecting fraud, assessing risk and product retailing, public safety agencies can use predictive modelling and data mining techniques to look for previously unknown valid patterns, relationships in large data sets and process improvements in situational awareness and command centres. These smart public safety systems can collect data from different processes, systems, and devices and can apply intelligence to this mass of data. The intelligence applied to this data can detect patterns of incidents and generate new insights, so that officials can make well-informed decisions and take action in near real time. Also, using data mining saves time for field personnel, reduces costs, and avoids the need for travel. Instead of just reacting to crimes and emergencies, with these new technologies and capabilities, public safety officials can perform analysis so that they can anticipate and work to prevent incidents.

Specifically, public safety agencies like Richmond, Memphis and Edmonton Police Departments apply data mining intelligence to tactical crime analysis in order to review extremely large datasets and incorporate a vast array of variables, far beyond what a single analyst, or even an analytical team or task force, can accurately review. Also, data mining can be used to identify a crime or series of crimes associated with an increased risk of escalation or violence; thereby, it is facilitated the apprehension of the suspect and increased the possibilities of interrupting a crime series before serious escalation occurs. Besides, data mining is considered as an essential technique for analyzing Internet and Web log data since monitoring and characterizing "normal" activity can help to rapidly identify unusual or suspicious activities in large datasets, providing actionable patterns for use in subsequent analysis and surveillance. So, public safety agencies can use it to identify and characterize extremely rare events, anomalies, and patterns in relatively large datasets.

However, the continuous increase in data volumes causes great and challenging difficulties in processing, analyzing and extracting valuable, new and useful information for decision support tools. Therefore, methods for efficient computer-based analysis are indispensable. In particular, support decision making can greatly benefit from methodological techniques developed in the new interdisciplinary field of Knowledge Discovery in Databases (KDD) [6] encompassing statistical, pattern recognition, machine learning (ML), and visualization tools to support automatic data analysis and discovery of regularities (*patterns*) that are implicitly encoded and hidden within the data.

Besides *mining* knowledge from large amounts of data, annotation and correlation of data from numerous and diverse digital evidence sources are essential in the context of public safety. Annotation and correlation of data across multiple devices in order to highlight an activity matching a scenario of interest are considered as a promising technique to support the public safety agencies activities using a large volume of information derived from heterogeneous environments. Therefore, there is a need for normalization in the representation of data from multiple sources of digital evidence in order to support such pattern recognition [8].

By providing a normalised view of all the data available, generating scenarios of interest, mining of behavioural patterns and correlation between events can be established. The needs for new architectures that incorporate techniques to analyse data from multiple sets of digital evidence used by police and other investigation entities and to represent such data in a normalized manner are presented in [7].

Currently, techniques based on semantics are applied for annotation and correlation of data in the Safety and Security Knowledge Domain. Semantic data modelling techniques provide the definition and format of manipulated data. They define standardized general relation types, together with the kinds of things that may be related by such a relation type. In addition, semantic data modelling techniques define the meaning of data within the context of its interrelationships with other data. At this point, it is where ontologies fit into, which are actually the semantic data models. Ontology [9] is a formal representation of knowledge as a set of concepts within a domain, and the relationships between those concepts. It is used to reason about the entities within that domain, and may be used to describe the domain. Data models, metadata and annotations, classification schemes and taxonomies, and ontology are greatly used in a variety of applications and domains. In the security and safety application (knowledge) domain, effective data modelling and knowledge representation facilitate automated semantic-based analysis of large volumes of data and identification of suspicious or alert situations and behaviours. Their added value remains in sharing and extending such models and representations with other stakeholders and similar applications to facilitate data interoperability and unified reasoning within the same knowledge domain.

Finally, data management during disaster/crisis situations also requires facing the same, mentioned above problems, due to the fact that disaster data are extremely heterogeneous, both structurally and semantically. This creates a need for data integration and ingestion in order to assist the emergency management officials in rapid disaster recovery. Since the data in disaster management could come from various sources and different users might be interested in different kinds of knowledge, data mining typically involve a wide range of tasks and algorithms such as pattern mining for discovering interesting associations and correlations; clustering and trend analysis to classify events in order to prevent future reoccurrences of undesirable phenomena. Due to the fact that real-world data in disaster management tend to be incomplete, noisy, inconsistent, high dimensional and multi-sensory etc., development of missing / incomplete data correlation approaches in order to increase the situational awareness can be especially beneficial in this context [10].

5 The Related Economic Impact in This Transformation

As is shown in Figure 3, one of the sectors where Future Internet stands out in a Smart City is *Security*. As has been mentioned at the beginning of this report; '*protecting citizens is one of the key factors for a government and also a priority for the normal functioning of businesses, communities and civil society at large'*. If for instance, any facility in charge of providing day-to-day essential services suffers a disaster (e.g. terrorist attack); the service interruption should cause huge damage to society in the form of socio-economic losses, socio-political adverse effects, environmental consequences or even substantial human casualties, each being accompanied by related costs. Anticipating and preventing those potential threats has been widely analysed as an essential aspect in order not only to keep the wellbeing of modern societies but also as a cost-effective solution for any organization (public or private) in charge of those infrastructures.

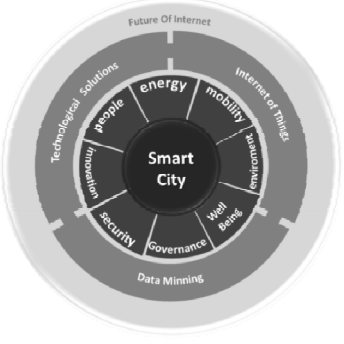

Fig. 3. The Smart City Framework

Moving security towards a most effective system will involve improvements in most of the other indicators such as productivity, flexibility, labour market or budgetary savings. For example, introducing a new security architecture framework based on pre-processing sensors will enable clearer data arriving to first responders, shortening times in their actuations. This reduction shall provoke optimizations in times and resources, which will reduce costs, rising higher productivity of security personnel, increasing job satisfaction and increasing efficiency and effectiveness process. It is also worth mentioning that public savings and situation can also been extrapolated to business and companies features, provoking similar conditions, being the impact in accordance with the business size and previous situation.

In the Internet of Things domain, 'SmartCities' will be submerged by millions of devices: sensors, meters, actuators, connected through a capillary network reaching all the peripheral devices. This process shall register several factors in real time, allowing for instance a smart management of potential threats or real emergencies allocated in different places of the city. In relation to video analytics and data mining domain, it is also worth it to stand out several examples of cities where cameras and sensors deployed are already managed in a smart way (together with M2M technologies and

data mining) contributing to reduce possible emergencies as well as its response time. For example, New York City for their City Control uses an innovative four dimensional, integrated visualization technology that provides automated situational awareness for anyone responsible for Securing and Protecting Infrastructure and/or Human Assets. These technologies contribute on an essential way to optimize capacity and first responders' response time, both to beat to a potential risk, and to response to an emergency. This phenomenon also brings an outstanding saving for responsible organizations in charge of economic management of cities.

To conclude, it is worth to highlight that most of the benefits for the end users do not create direct revenues, but significant operational savings and increased efficiency. Also it is expected that transformation will produce significant economic benefits for the society and business at large.

6 Conclusions

Smart Cities of tomorrow will provide a larger number of innovative services and new capabilities that will highly contribute to reinforce the feeling of safeness in citizens. **Enhanced M2M communications** will allow the massive usage of heterogeneous sensors (smart meters) around the city and its surroundings, internet-connected and self-configured devices that enable web-sensors access and surveillance-information sharing among diverse safety agencies involved. **Robust intelligent video analytics** that enable smarter contextual awareness will be applied not only for traffic purposes but also for other aspects as suspicious objects/behaviors early detection, and will represent the required answer to the existing explosion of video footage captured by security forces who want to enlarge the automated detection capabilities of their video surveillance systems. **Predictive modeling and data mining** techniques applied to surveillance data enable the early detection of incidents and the generation of new insights that efficiently support decision-makers. Depicted expected technological advances within these three pillar areas clearly benefit Public Safety services with intelligent real-time surveillance capabilities, efficient early detection mechanisms, enhanced information visualization and sharing, and semi-automatic decision support systems at Command and Control centers. Public Authorities will extremely reduce the response time to emergencies (see that Madrid Emergency Response Centre helped to reduce it to 25%) since innovative internet-based capabilities are expected soon, for instance, an efficient monitorization for road safety purposes detecting drastic weather changes, road condition, foreign objects, or the early detection mechanisms based on video analytics of suspicious/missing people, suspicious behaviors, illegal entries, suspicious objects, etc., which can be even more efficient with alerting capabilities to specific geo-graphically based population.

All these new techniques will have an important impact and fostering of economic sustainability within a Smart City while offering high quality Public Safety services.

References

1. SafeCity Project: FI-PPP (Future Internet Public Partners Partnership) Programme (2011-2013), http://www.safecity-project.eu/
2. Nuckull, D., Hinchcliffe, D., Governor, J.: Web 2.0 Architectures. O'Reilly (2009)
3. Stauffer, C., Grimson, W.E. L.: Learning patterns of activity using real-time tracking. IEEE Trans. Pattern Analysis and Machine Intelligence 22(8), 747–757 (2000)
4. Cucchiara, R., Grana, C., Neri, G., Piccardi, M., Prati, A.: Sakbot system for moving object detection and tracking. In: Video-Based Surveillance Systems-Computer Vision and Distributed Processing, pp. 145–157 (2001)
5. Cavoukian, A.: Anonymous Video Analytics (AVA) technology and privacy. White Paper, Information and Privacy Commisioner, Ontario, Canada (April 2011)
6. Han, J., Kamber, M.: Data Mining: Concepts and Techniques. The Morgan Kaufmann Series in Data Management Systems, Jim Gray Series Editor. Morgan Kaufmann Publishers (2000)
7. Osborne, G., Turnbull, B.: Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation. In: International Conference on Availability, Reliability and Security, ARES 2009 (2009)
8. Mohay, G.: Technical Challenges and Directions for Digital Forensics. In: SADFE 2005: Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, p. 155. IEEE Computer Society, Washington, DC (2005)
9. Guarino, N.: Formal Ontology and Information Systems. In: 1st International Conference on Formal Ontology in Information Systems (FOIS 1998), Trento, pp. 3–15 (June 1998)
10. Hristidis, V., Chen, S.C., Li, T., Luis, S., Deng, Y.: Survey of Data Management and Analysis in Disaster Situations. Journal of Systems and Software 83(10) (October 2010)