

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

5,800

Open access books available

142,000

International authors and editors

180M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



# Risk Assessment and Automated Anomaly Detection Using a Deep Learning Architecture

*Stelios C.A. Thomopoulos*

## Abstract

Risk-based security is a concept introduced in order to provide security checks without inconveniencing travelers that are being checked with unqualified scrutiny checks while maintaining the same level of security with current check point practices without compromising security standards. Furthermore, risk-based security, as a means of improving travelers' experience at check points is expected to reduce queueing and waiting times while improving at the same travelers' experience during checks. A number of projects have been funded by the European Commission to investigate the concept of risk-based security and develop the means and technology required to implement it. The author is the Coordinator of two of the flagship projects funded by EC on risk-based security: FLYSEC and TRESSPASS. This chapter discusses and analyses the concept of risk-based security, the inherent competing mechanism between risk assessment, screening time and level of security, and means to implement risk-based security based on anomaly detection using deep learning and artificial intelligence (AI) methods.

**Keywords:** risk assessment, security, anomaly detection, deep learning, neural networks, crowd simulation, control and command, surveillance, risk-based security

## 1. Introduction

Risk-based security is built around the premise that information obtained from observable aspects of human identity and possession and knowledge acquired about hidden aspects of human capability and intent can be intelligently combined to assess to some great extent of accuracy the threat a given individual poses to a security system, be it an airport or a border crossing point (BCP). Then, in turn, associating the estimated level of threat with a measure of risk by factoring in the cost that the assessed threat can represent to the system that is being secured by taking into account the impact and cost a given threat can have on a security system, a risk-based security approach can be designed and implemented, whereby security checks are tailored to be commensurate to the estimated risk each individual may pose, instead of being uniform irrespectively of the risk posed by each individual, as is the case today. Taking into account that less than 5% of all individuals can be a potential security risk, the savings in terms of time required to go through risk-based security systems with speedier tests for the 95% of low to no risk individuals can be significant, waiting times in security lines can be reduced and thus the level of comfort and customer satisfaction be drastically improved.

The concept of *risk-based security* is founded on the premise that less than 5% of travelers represent a threat to the security of a border crossing point (BCP), it is conceivable that by somehow identifying the risk-free travelers, the security checks for those “trusted” travelers can be relaxed and sped up, leading into lower delays in the security screening systems. By easing off the security checks on the “trusted” 95% of travelers, the security screening process can focus on the potentially “suspicious” 5% of travelers, thus increasing the odds of identifying them more efficiently.

The concept of risk-based security is indeed promising in terms of improving travelers’ experience by easing off security screening and reducing the overall time required to spend at a security check-point. However, the difficulty in implementing a risk-based security systems lies on: (a) developing and implementing non-intrusive, GDPR<sup>1</sup> compliant technology and systems that can estimate the risk level of each traveler without inducing additional and cumulative delays; (b) testing such systems before rolling them out in operational environments; and (c) estimate their performance and efficacy under ideal conditions for obtaining performance bounds, calculating the cost of the required investment for implementing risk-based technologies; and (d) calculate the degradation in performance when moving away from the “ideal” operational conditions into realistic operational conditions.

The European Union (EU) and other international organizations promote this approach through various initiatives. The European Commission (EC) issued the “Smart Borders package” which aims to modernize the Schengen area’s external border management by improving the quality and efficiency of border crossing processes through the establishment of ‘Stronger and Smarter Information Systems for Borders and Security’ [1]. The International Air Transport Association (IATA) proposed a Checkpoint of the Future, designed to enhance security while reducing queues and intrusive searches at airports by using intelligence-driven risk-based measures [2]. Along these lines the EC funded the Research and Innovation project FLYSEC [3] has developed and demonstrated an innovative, integrated, and end-to-end airport security system facilitating risk-based screening with the introduction of novel intelligent technologies.

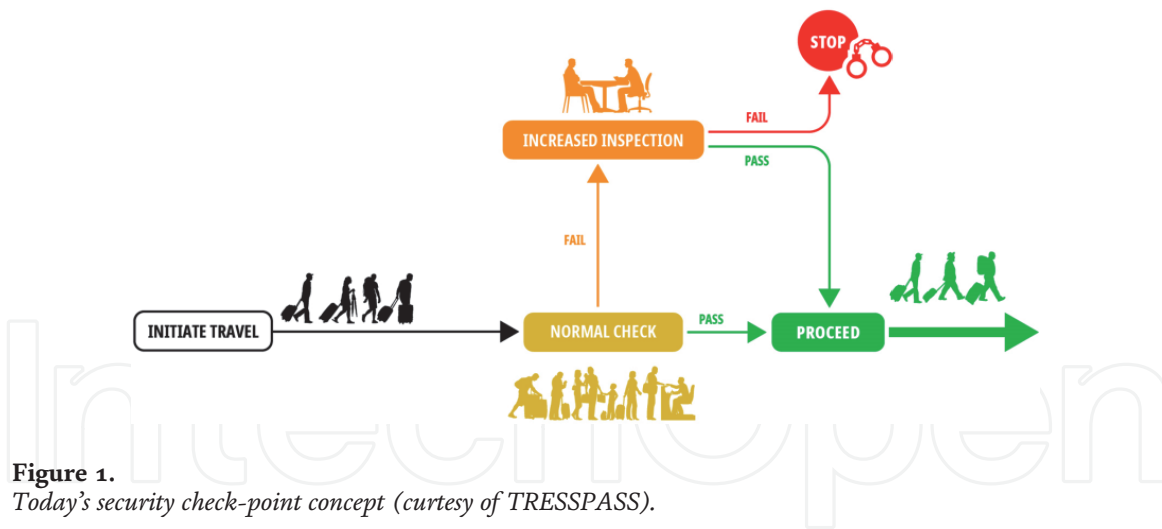
This chapter *discusses* a model of risk-based security developed over a number of EU funded projects, *highlights* the need to using simulation in assessing the efficacy of risk-based security technologies and protocols, and *elaborates* on the use of AI and deep learning algorithms for assessing the perceived risk for each traveler based on observable behavioral indicators (parameters), while *factoring in* information acquired from various sources about hidden behavioral parameters.

## 2. Conventional versus risk-based security

**Figure 1** shows a today’s conventional security check point whereby we distinguish two types of checks: (a) the “normal” check where all individuals in the security check area are treated uniformly by applying the same level of security for all; and (b) the “increased” security check point where travelers are channeled if they fail at normal security check point. It should be pointed out that in this security system of check points, currently implemented almost worldwide, the “increase inspection” is usually the outcome of randomized selection of travelers to be subjected to an increased level of inspection and is usually based on the principle of “importance sampling<sup>2</sup>” methods. These methods try to detect a probabilistic event, such as the existence of a suspect among travelers, with a certain degree of confidence by taking

<sup>1</sup> GDPR compliance: Complete guide to GDPR compliance: <https://gdpr.eu/>

<sup>2</sup> Importance sampling definition: [https://en.wikipedia.org/wiki/Importance\\_sampling](https://en.wikipedia.org/wiki/Importance_sampling)



**Figure 1.** Today's security check-point concept (courtesy of TRESSPASS).

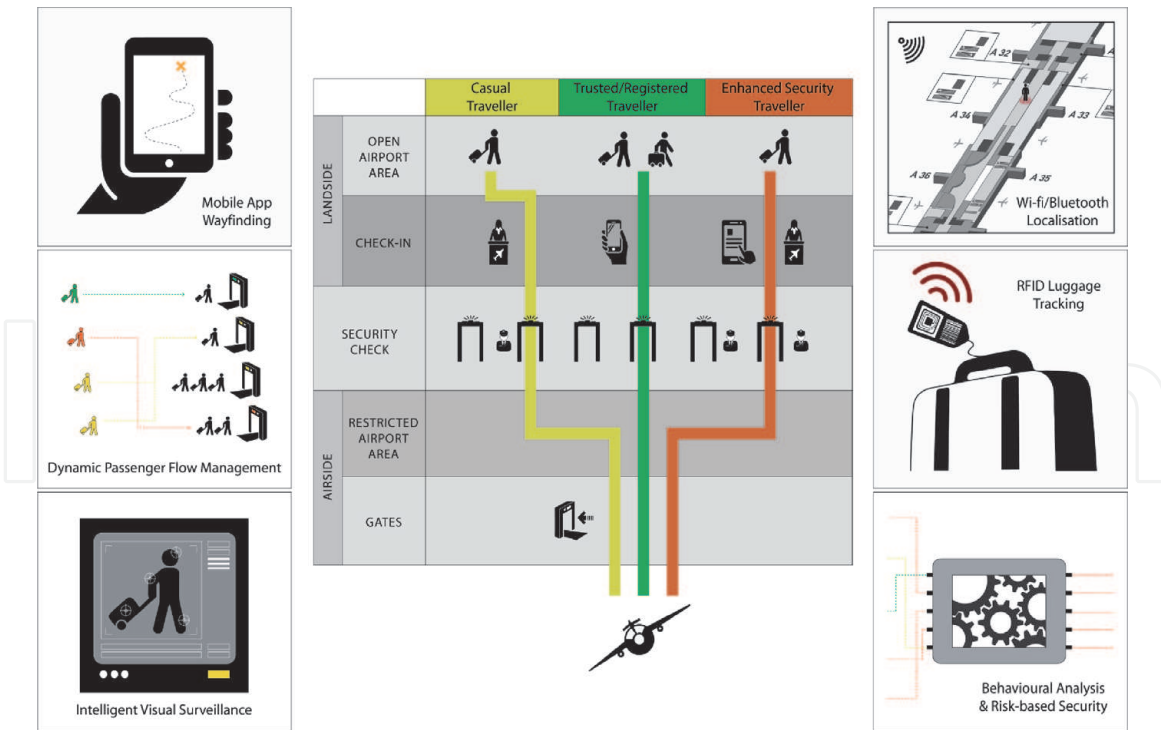
into account the probability of existence of such an event and possibly the range of values the event can assume. These methods are “blind,” that is they draw samples from the distribution indiscriminately and without taking into account any specific attributes of the samples, and thus, they are also GDPR compliant. As it will be pointed out further down in the chapter, risk-based methods need to pay special attention to comply with GDPR as they gather and use information and knowledge about individuals' private data such as identity, possession, capability, and intent.

Risk-based security associates the estimated risk for each traveler with a commensurate level of security scrutiny. Using prior information about each traveler and sensory data obtained while the traveler is within the security perimeter of a monitored area, a risk-based security system assigns a risk factor to each traveler and depending on the value of the risk factor, the traveler is mapped to a level of security scrutiny commensurate with the perceived risk. Although different number of levels can be associated with the estimated risk, for practical reasons, it is sufficient to associate the entire range of risk values into three different levels of security, Trusted/Registered (Green), Casual (Yellow) and Enhanced Security (Red), as shown in **Figure 2** [5].

In **Figure 2**,<sup>3,4</sup> a number of GDPR-compliant technologies that can be used for and contribute to the risk assessment are shown and include: mobile app way

<sup>3</sup> FLYSEC ... Complementing the ACI/IATA efforts, the FLYSEC European H2020 Research and Innovation project (<http://www.fly-sec.eu/>) has developed and demonstrated an innovative, integrated and end-to-end airport security process for travelers, enabling a guided and streamlined procedure from the landside to airside and into the boarding gates, and offering for an operationally validated innovative concept for end-to-end aviation security. FLYSEC has contributed towards: (i) innovative processes facilitating risk-based screening; (ii) deployment and integration of new technologies and repurposing existing solutions towards a risk-based Security paradigm shift; (iii) improvement of traveler facilitation and customer service, bringing security as a real service in the airport of tomorrow; (iv) achievement of measurable throughput improvement and a whole new level of Quality of Service; and (v) validation of technologies, devices and applications that can be used to assess risk while the travelers move around in the security perimeter.

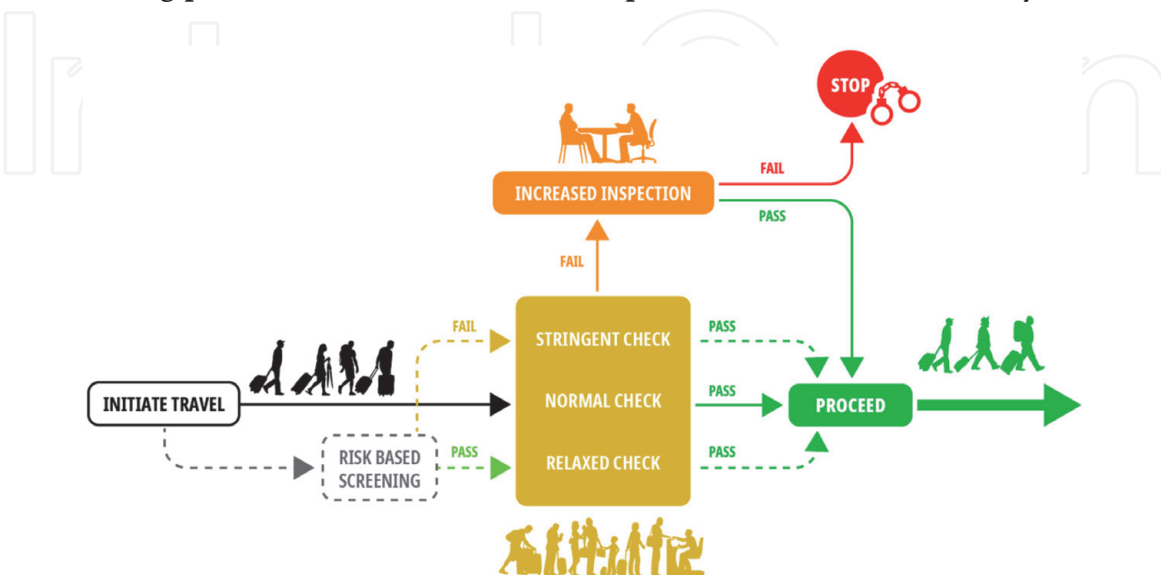
<sup>4</sup> TRESSPASS ... TRESSPASS focusses on risks emerging from people that use the BCP such as travelers and staff, including people that act as such. This includes their luggage, both checked in and hand-held. A typical DBT for a BCP is based on a subset of a typical set of attributes regarding such persons and their travel group. In a DBT, threats are described using as building blocks in terms of **Observable aspects**: (a) *identity*: specific people of which we know that they cause, or will not cause, a threat; and (b) *possession*: assets that we know that can be used to generate a threat, e.g. explosives; whereas in terms of **Hidden aspects**: (c) *capability*: people with specific skills with which they can, generate a threat; and (d) *intent*: people that have an intent from which a threat can be derived.



**Figure 2.** Association of three security scrutiny levels, namely “enhanced security,” “casual traveler,” and “trusted/registered” with the estimated level of risk for each traveler. These three levels have been introduced in the FLYSEC project [3] and carried over to the TRESSPASS project [4].

finding; dynamic travelers flow management; intelligent visual surveillance; Wi-Fi/Bluetooth localization; RFID mobile tracking; and behavioral analysis & risk-based security personnel mobile app.

**Figure 3** represents a risk-based security check point that results from combining the three-level risk-based security screening of **Figure 2** with the conventional security screening of **Figure 1**. As it can be seen from **Figure 3**, the need for assessing each traveler’s risk factor from various observable parameters requires measuring somehow these parameters, of course in a GDPR compliant way, and thus additional processing steps and capabilities that may induce additional delays in screening process. Thus, the fundamental premise of risk-based security as a



**Figure 3.** Risk-based security check point: The standard (randomized scrutiny checks) security check point of **Figure 2**, has been modified by introducing a three-level risk assessment process prior to the security scrutiny resulting in three different security scrutiny levels at the security screening check point (reference).



means of providing the same, at least, level of security as conventional check points without inducing additional delays, seems to be in conflict with the additional delay induced by additional screening tests required for estimating each traveler's risk index, unless the risk assessment process is done transparently while the travelers move from the entry to exit points in a BCP (Border Crossing Point).

Figures 4 and 5 depict two block diagrams implementing the conventional security screening process of Figure 1 and the risk-based security screening process of Figure 3 respectively. From the two diagrams it is clear that additional screening stages are required for assessing the risk for each traveler in risk-based security. Each one of these additional risk assessing stages induce additional delays in the security screening process, that add up to an overall additional time required for risk-based security screening compared to the time required for security screening through a conventional security check point.

Thus, it appears that risk-based security may require additional processing time for estimating risk that may offset the benefits from faster security screening for those travelers whose estimated risk classifies them in either the "trusted/registered traveler" or "casual travelers" categories for whom security screening is relaxed and thus faster than the time would be required to screen them in today's conventional

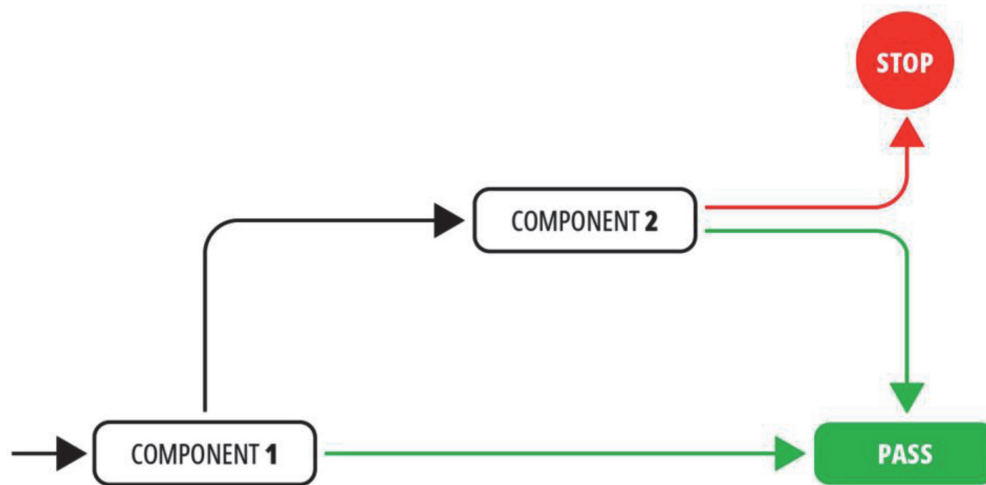


Figure 4.  
Configuration 1 (current BCP implementation).

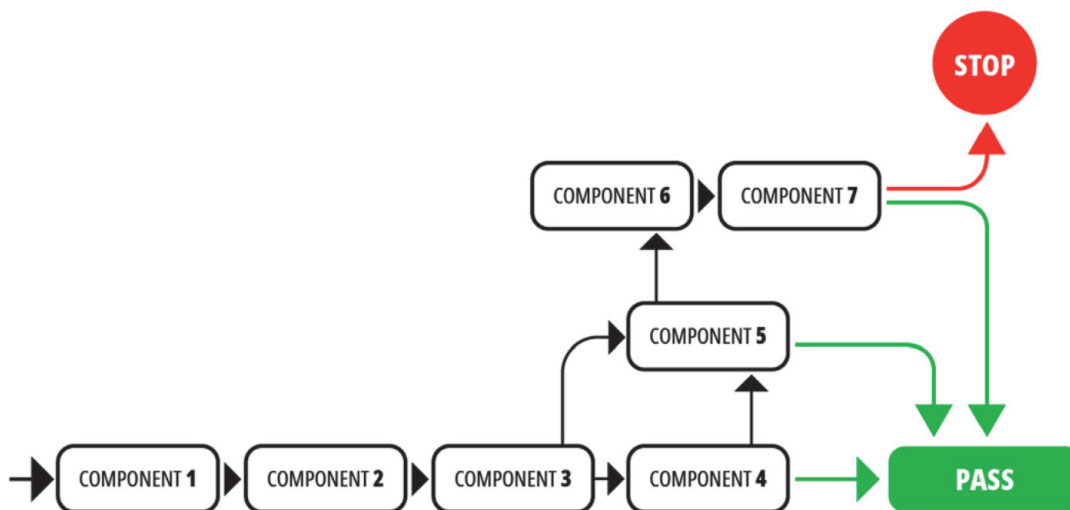


Figure 5.  
Configuration 2 (risk-based BCP implementation).

check points of **Figure 1**. Granted that over 90% of travelers fall within these two categories and will experience reduced delays at security screening, it remains to determine if the aggregate benefits from the reduced security screening at check points will trade off positively against the additional delays induced by the additional screening points for determining each traveler’s risk as in **Figure 5**.

In order to quantify the cost–benefit trade-offs between the efficiency of a risk-based security BCP and the delay induced by additional checks required for assessing risk, the following experiment was conducted using Fraunhofer’s FhG BCP Monte-Carlo agent-based simulator of a BCP configuration (courtesy of Fraunhofer Institute) [4].

For the simulation, we assumed a BCP with 1000 travelers, some exhibiting normal (no risky) behavior, whereas the rest exhibit suspicious behavior, with the following parameters:

- Distribution of traveler types: [Normal, Suspicious]: [0.9,0.1]
- Alarm threshold for each component: 0.5
- Risk calculation: According to the script below:

```
for all agents:
    risk = 0
    alarm = 0
    number_of_components_passed = 0
    current_component = component_1
    while current_component != Pass or Stop:
        #alarm is 0 or 1
        alarm = alarm + perform interaction between agent and component to get alarm
        number_of_components_passed += 1
        #risk is in the range [0,1] with risk threshold of 0.5
        risk = alarm / number_of_components_passed
        # if risk < 0.5 perform the same level of check otherwise more strict checks
        current_component = risk based next component
```

- Effectiveness calculation:

$$\text{diff\_1} = (\text{mean of total suspicious people} - \text{total people stopped})$$

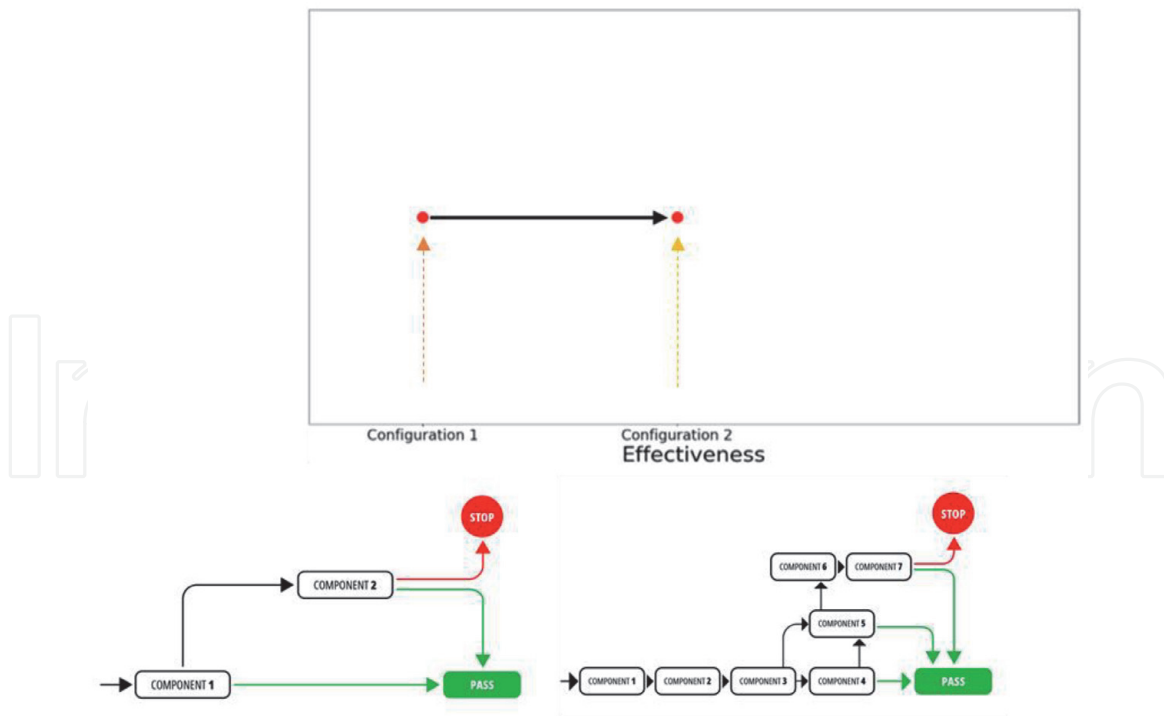
$$\text{effectiveness} = 1/\text{absolute}(\text{diff\_1})$$

- Ran over 10000 iteration with 100 travelers each time for both the configurations.

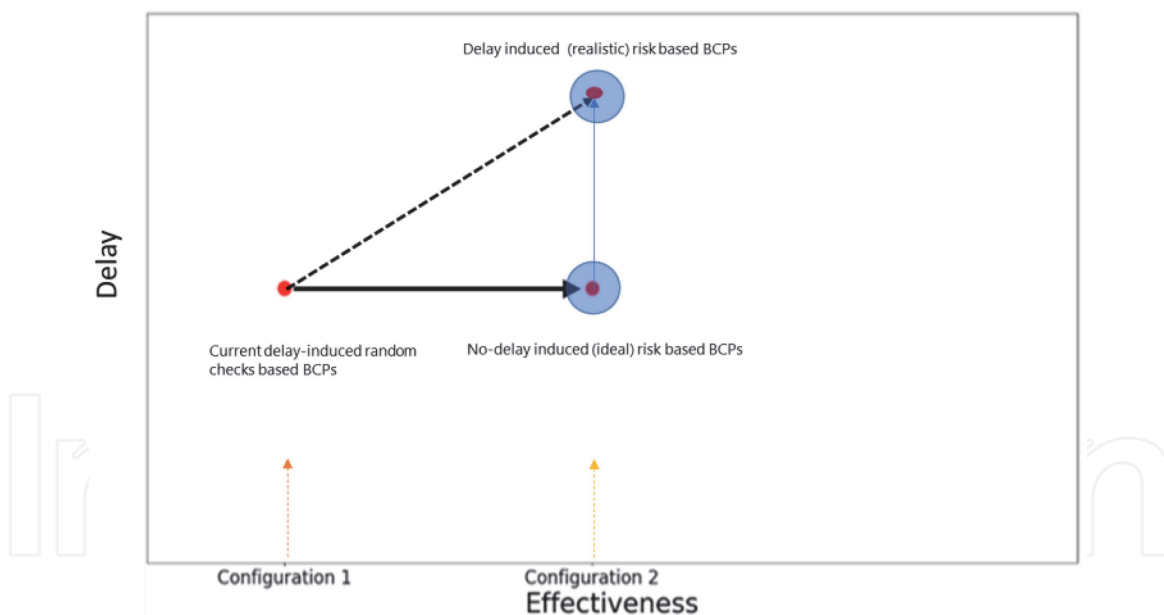
Using the above script for generating travelers with the above choice of parameters, 10.000 iterations with 100 travelers each time were run for each one of the two configurations of **Figures 4** and **5**, and the effectiveness (as defined above) of each configuration was calculated. The results regarding the effectiveness (as defined above) of each configuration are qualitatively summarized schematically in the graph of **Figure 6**.

**Figure 6** demonstrates the increase in effectiveness achieved by risk-based security in a BCP using the FhG simulator. The effectiveness of the BCR risk-based configuration 2 clearly surpasses that of the conventional BCT configuration 1. However, the diagram in **Figures 6** and **7** does not include the delays induced by the additional security check stages of the risk-based BSP configuration in **Figure 5**. If we consider these delays, then the operating point of the risk-based BCP not only does it move to higher efficiency but also to higher delays, as **Figure 7** clearly demonstrates.

From **Figure 7** it is clear that there is a competing mechanism between effectiveness (another way of stating “comfort”) and delay induced by a risk-based



**Figure 6.** Effectiveness calculation of a conventional BCP with random security checks determined by importance sampling versus risk-based BCP configuration: Effectiveness increases with the use of risk-based security in a BCP.



**Figure 7.** Effectiveness calculation of a conventional BCP with random security checks determined by importance sampling versus risk-based BCP configuration taking into consideration the additional delays induced by the additional risk assessment stages in configuration 2: Effectiveness increases with the use of risk-based security in a BCP, while induced delays increase as well.

security BCP versus a conventional BCP with randomized tests based on the theory of importance sampling<sup>5</sup>. The aim of the two EU-funded projects FLYSEC and TRESSPASS, coordinated by the author, is for FLYSEC to: (a) demonstrate that there is technology available or can be developed to implement risk-based security in a GDPR compliant way; (b) provide solid evidence of the risk-based security

<sup>5</sup> <https://www.safeopedia.com/definition/784/safety-sampling>



screening as an effective and non-instructive means of providing security with convenience to travelers; and for TRESSPASS to: (c) provide a comprehensive risk-assessment framework for calculating risk systematically in accordance with the TRESSPASS multi threat, multimodal that includes all **four tiers** of the access model, i.e.

1. measures undertaken with third countries or service providers;
2. cooperation with neighboring countries;
3. border control and counter-smuggling measures;
4. control measures within the area of free move,

by taking into account estimates and information about.

*Observable aspects of travelers' behaviors, i.e.:*

**Identity:** specific people of which we know that they cause, or will not cause, a threat;

**Possession:** assets that we know that can be used to generate a threat, e.g. explosives; and.

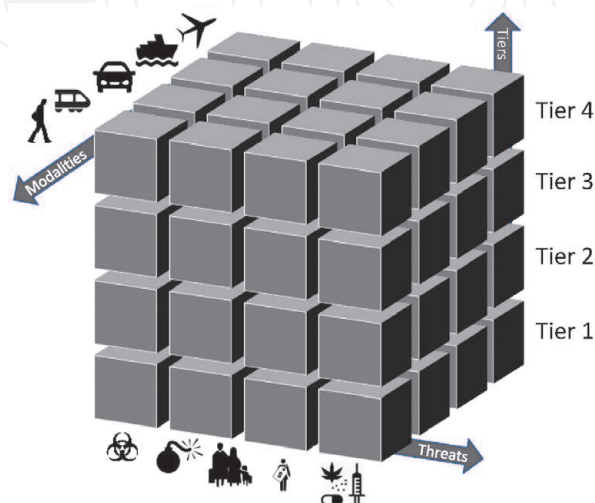
*Hidden aspects of travelers' behaviors, such as:*

**Capability:** people with specific skills with which they can, generate a threat;

**Intent:** people that have an intent from which a threat can be derived as depicted in **Figures 8** and **9**.

Thus, the aim of the two funded projects, namely FLYSEC and TRESSPASS, is to provide solid evidence and the means for moving the operating point (OP) of a risk-based BCP from the delay induced OP to the no-delay induced OP, or as close to it as possible without inconveniencing travelers and in a GDPR compliant way, as shown in **Figure 10**.

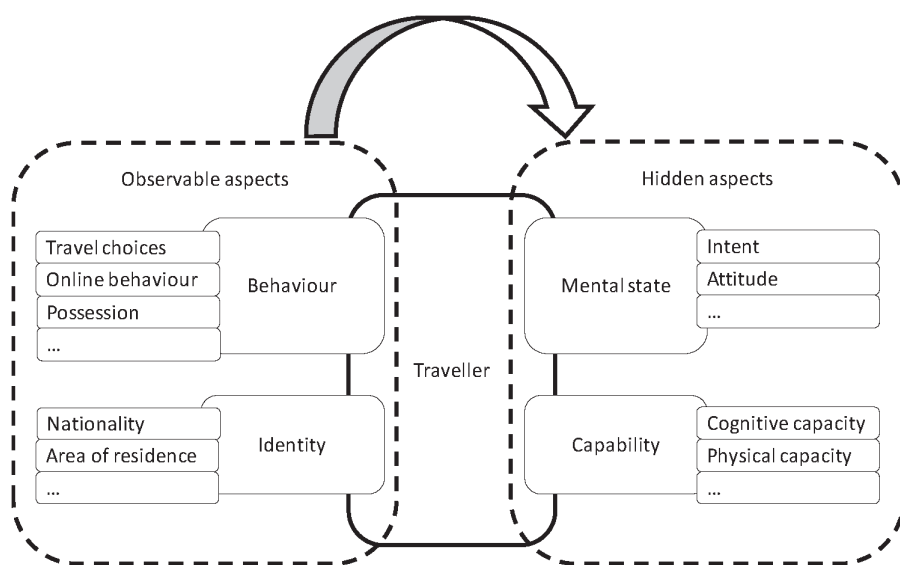
The greatest challenge in risk-based border management is the estimation of the risk for each individual traveler. In TRESSPASS, a framework for modeling risk and a systematic approach of quantifying risk are proposed as follows:



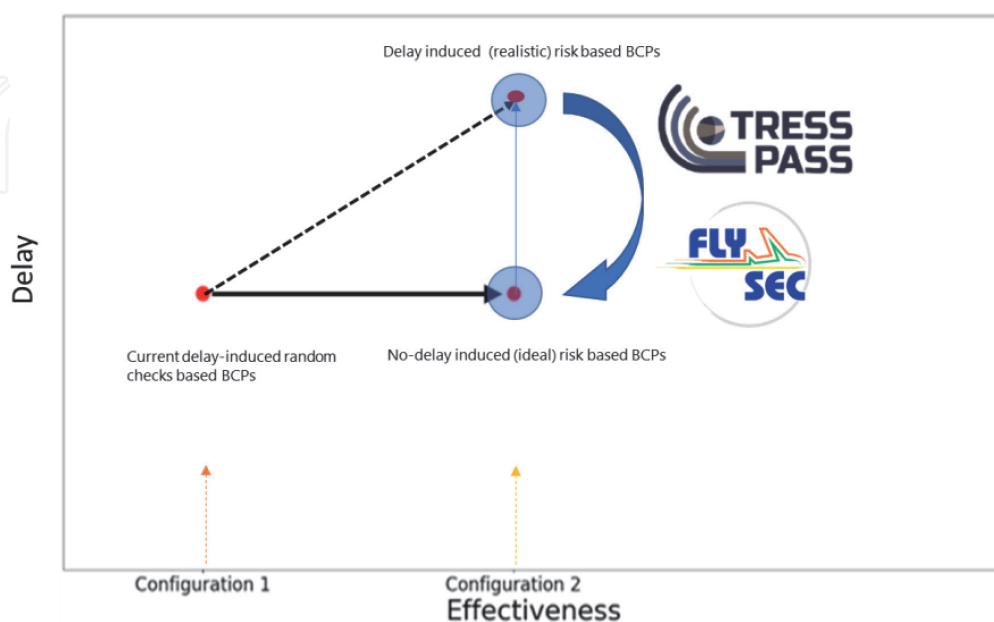
**Figure 8.**  
*Multi-modal, multi-tier TRESSPASS risk-assessment model.*

- Risk indicators are accurately estimated from available data collected from background information.
- The risk for each traveler is calculated.
- Based on risk, the system adjusts the number and types of security checks required for each traveler, in order to maintain a desired security level while optimizing the security system performance in terms of efficiency, traveler satisfaction and operational cost reduction.

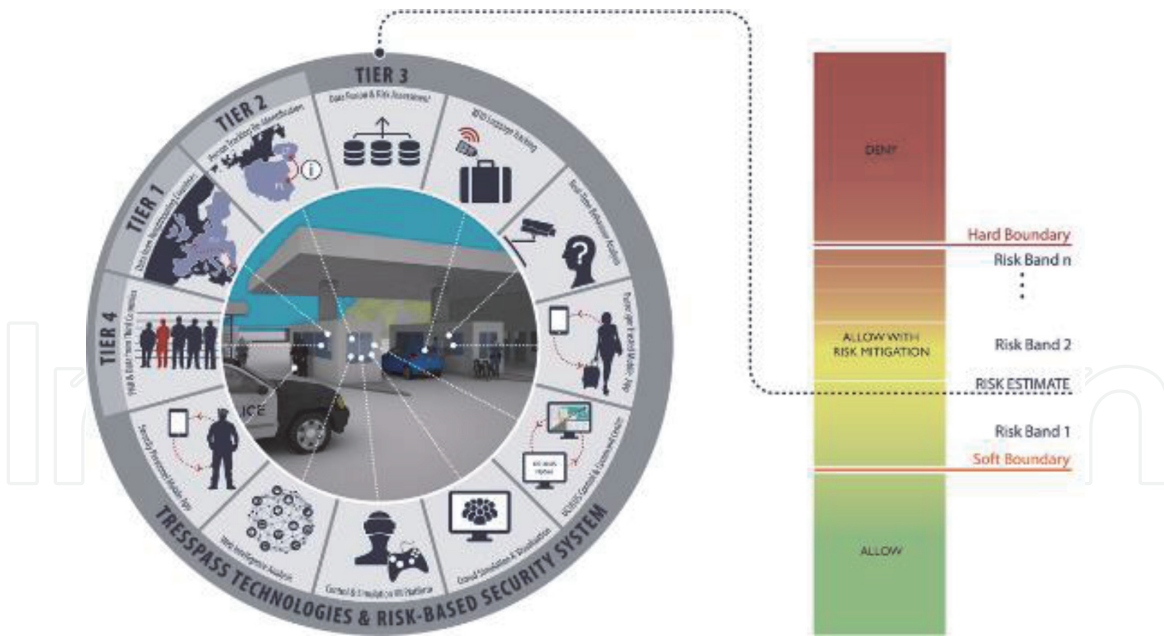
**Figure 11** summarizes in a comprehensive visual depiction the risk-based framework used in TRESSPASS [4], and previously introduced in FLYSEC [3]. The framework for risk-based security consists of an extensive use of technologies to



**Figure 9.**  
 Observable and hidden risk factors.



**Figure 10.**  
 Moving the operating point of a risk-based BCP to minimizing security check delays is the objective of both FLYSEC and TRESSPASS EU-funded projects.



**Figure 11.**  
TRESSPASS comprehensive risk-based security framework.

estimate risk from both Observable and Hidden risk indicators across all four security tiers and heavily tested, both in vivo and in vitro through simulation, in carefully designed pilots across all three BCP modalities: air, land and sea.

**Use of simulation in designing, testing, and assessing risk-based security**

Paramount to the design and testing alternative designs of risk-based security concepts, technologies and protocols, in order to achieve the increase in effectiveness of BCPs with the parallel reduction of delays, is the use of simulation. iCrowd is an agent-based simulator that can be used to implement and test different risk-based concepts and technologies in a flexible and realistic simulation environment [6]. **Figures 12 and 13** show a photo-realistic virtual reconstruction of an airport used extensively in simulating security scenarios and policies for a variety of projects and pilot use-cases.



**Figure 12.**  
Photo-realistic, agent-based simulation using iCrowd.

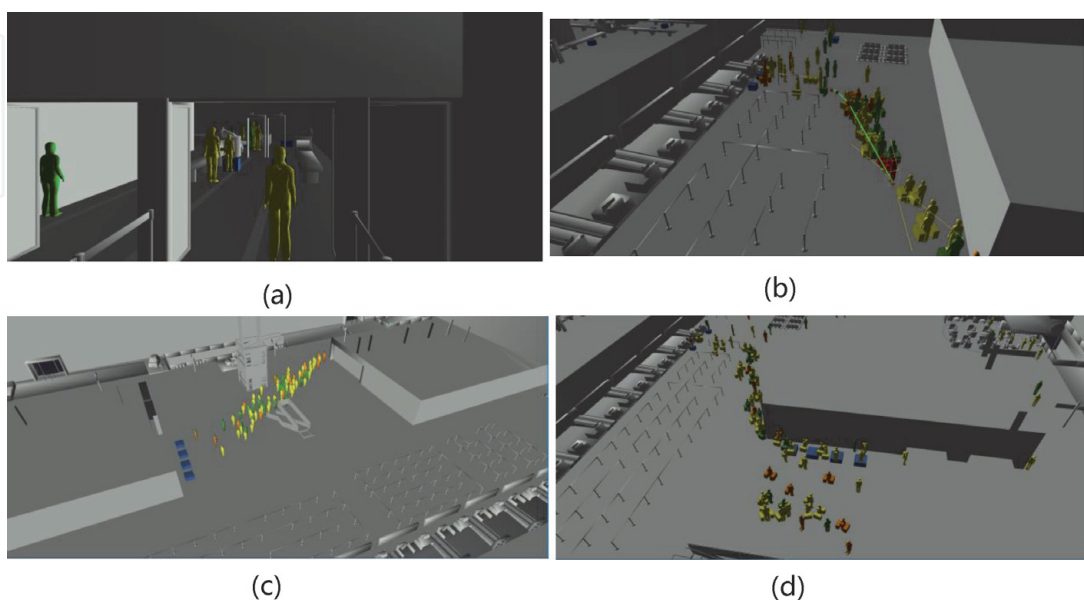




**Figure 13.**  
*Queue lanes in a risk-based security checking system: Photo-realistic simulation provided by iCrowd.*

## 2.1 The iCrowd simulator

The iCrowd Simulator is an agent-based simulation platform capable of handling small-scale to large-scale crowds and calculating the change of the status of each participating component depending on dynamic interactions with other entities or the environment during simulation time [7, 8]. It can be utilized in any bounded area, i.e. building interiors and exteriors, stadiums, or any exterior area e.g. public places like squares, open-air festival etc. Currently, it is being used to simulate crowd movement and crowd interactions in general, with the graphical display being optional. As an agent-based simulation platform, different parameters for each agent can be considered, such as physical, emotional, vital characteristics regarding the crowd that will be observed (i.e. stress levels, health status), object/obstacle parameters and also environmental parameters that can affect the final solution of each simulated scenario performed.



**Figure 14.**  
*(a): Aspect of third-person camera. (b): Path planning example: The green line indicates the path the selected agent (displayed are red) is following (c): Travelers enter the airport. The display of hold and hand luggage is turned on. (d): Travelers go through the check-ins. The display of hold and hand luggage is turned on.*

iCrowd offers a fully operational flow simulation for travelers and personnel inside an airport, as displayed in **Figures 12** and **13**. It enables the user to define simulation scenarios, it is implementing a sophisticated crowd engine with collision avoidance<sup>6</sup> with multiple, different behaviors that can co-exist inside the same simulation. It also supports distributed simulations, operating as an orchestrator. It has been integrated with the C2 Web Portal OCULUS Air to communicate data, such as displaying the position and the movement of simulated entities in real time, and the Fusion and Ingestion Server to update travelers' status accordingly depending on their interactions with the airport's hardware and other security technologies (i.e. Beacons, RFID scanners and RFID tags for carry-on luggage tracking), **Figure 14(a)–(d)**.

### **3. Means for estimating risk that induce no further delays in the security screening process**

This section of the chapter presents and discusses implementable means for assessing risk without inducing additional delays beyond what passengers experience with today's screening process, but instead reduce the time it takes to go through the security screening process by adjusting the level scrutiny in accordance to the perceived risk.

#### **3.1 Anomaly detection from passenger trajectories**

If passenger trajectories at an airport, or any BCP by the same token, could be tracked from the moment they enter the airport or the BCP in general, one could conceivably be able to differentiate suspicious looking trajectories from trajectories that would be expected for a passenger and thus classified as normal. Differentiating, however, between normal and abnormal behaviors may be a difficult proposition by itself, let alone that it should be done in accordance with privacy and GDPR regulations.

In the work presented in [9, 10], those two issues were addressed as follows. To develop a privacy and GDPR compliant tracking method, we assumed that passengers are tracked using overhead cameras that identify passengers as point targets from their top-down footprints (silhouettes); the footprints are reduced to a point for each passenger and are tracked across the entire airport area or BCP. In the initial phase of the study in [9, 10], it was assumed that passengers tracking was perfect, i.e. that all passengers' traces as they moved around the airport or BCP area are (anonymously) identifiable and traceable. i.e. that the tracking system has perfect knowledge of the position of each passenger at any time. Although the assumption of perfect knowledge is idealistic, it allows us to get upper bounds on the performance of the tracking system that can be used to make trade off calculations between cost of investment on cameras infrastructure versus the (theoretically) achievable accuracy of the risk calculation.

The difficulty in risk assessment based on trajectories stems from the difficulty in defining what constitutes an abnormal behavior and how it can analytically be described. In the approach in [9, 10] this has been overcome by defining what constitutes a normal (expected) behavior, training the AI (Artificial Intelligence) system to recognize normal behavior and test it with abnormal behaviors to reflect loitering, jittering, and other deviations from expected "normal" behaviors.

**Figure 14(a)** through **(d)** are snap shots from the native visualizer of the iCrowd simulator simulating an anomaly detection mechanism based on travelers' tracking AI algorithm based on a Recursive Neural Network (RNN) [9, 10]. As



discussed above, we assumed that travelers can be tracked anonymously using top-down view cameras in compliance with GDPR and ethics regulations. Based on a model of what constitutes a normal traveler route (trajectory) in an airport (or similarly any other BCP), a convolutional recursive neural network was trained with “normal trajectories” generated by the iCrowd simulator. Once the RNN is trained with “normal trajectories,” travelers with “suspicious behaviors” are generated among travelers with “normal behaviors” and the algorithm is tested if it could detect the “suspicious trajectories.” In **Figure 14(b)**, the traveler with suspicious behavior is color-coded red. The risk assessment algorithm detects and identifies the suspicious traveler in **Figure 14(d)**.

A complete technical description of the anomaly detection algorithm is given in the references [9, 10]. Next, we summarize the results in [9, 10] in order to demonstrate the possibility of implementing a risk-based security system that monitors traveler risk continually without additional delays that can offset the benefits of the risk-based approach.

### 3.1.1 Evaluation results

The evaluation of the risk assessment system of [9, 10] is done using the Precision-Recall (PR) diagram, the Receiver Operating Characteristic (ROC) curve, the Confusion Matrix, the F1-score and the Total Accuracy, as defined next:

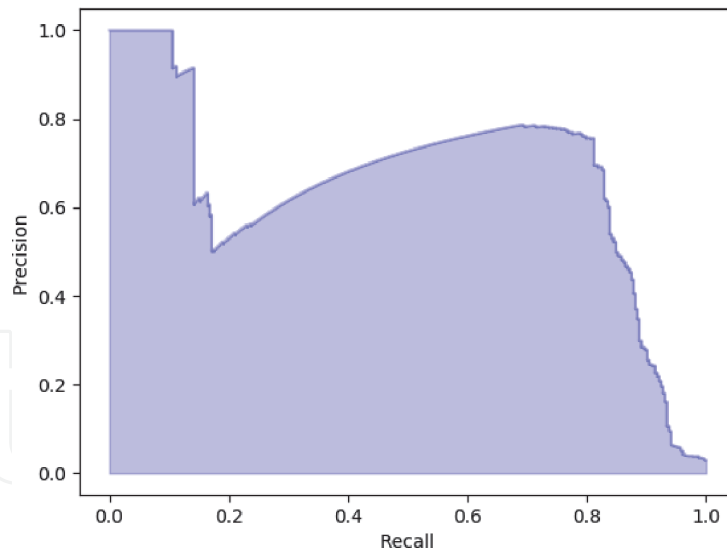
- Precision = (# of true suspicious behaviors detected)/(# of total labeled suspicious behaviors)
- Recall = (# of true suspicious behaviors detected)/(# of total suspicious behaviors)
- Receiver Operating Characteristic (ROC) curve = Probability of detection versus false alarm probability diagram
- Confusion Matrix = Normal versus abnormal confusion matrix
- F1-score =  $2 \cdot [(\text{Precision} \cdot \text{Recall}) / (\text{Precision} + \text{Recall})]$  which is the harmonic average of Precision and Recall.
- Total Accuracy = (# of Total Assessments)/(# of Total Cases)

**Figures 15–17** illustrate the PR diagram, the ROC curve and the Confusion Matrix respectively. Eqs. 6 and 7 calculate F1-score and Total Accuracy respectively. It should be reminded that the values of all evaluation metrics are defined within the interval [0, 1]. The closer to 1 a value lies, the better the achieved performance. **Table 1** summarizes the values of the recruited evaluation measures. The threshold score derived by the RNN architecture, by maximizing F1-score, is 3.7.

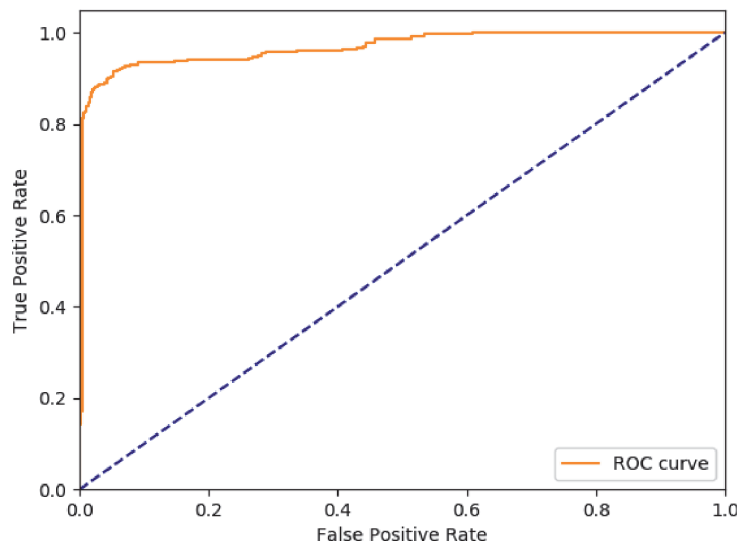
Furthermore, the F1 score (i.e. the harmonic average between Precision and Recall, Eq. (1)), along with the Total Accuracy, Eq. (2), the ROC AUC (Area Under Curve), and Average PR score, are calculated in **Table 1**,

$$F1 - score = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (1)$$

$$\text{Total Accuracy} = (\# \text{ of Successful Assessments}) / (\# \text{ of Total Cases}) \quad (2)$$



**Figure 15.**  
*Precision-recall diagram.*



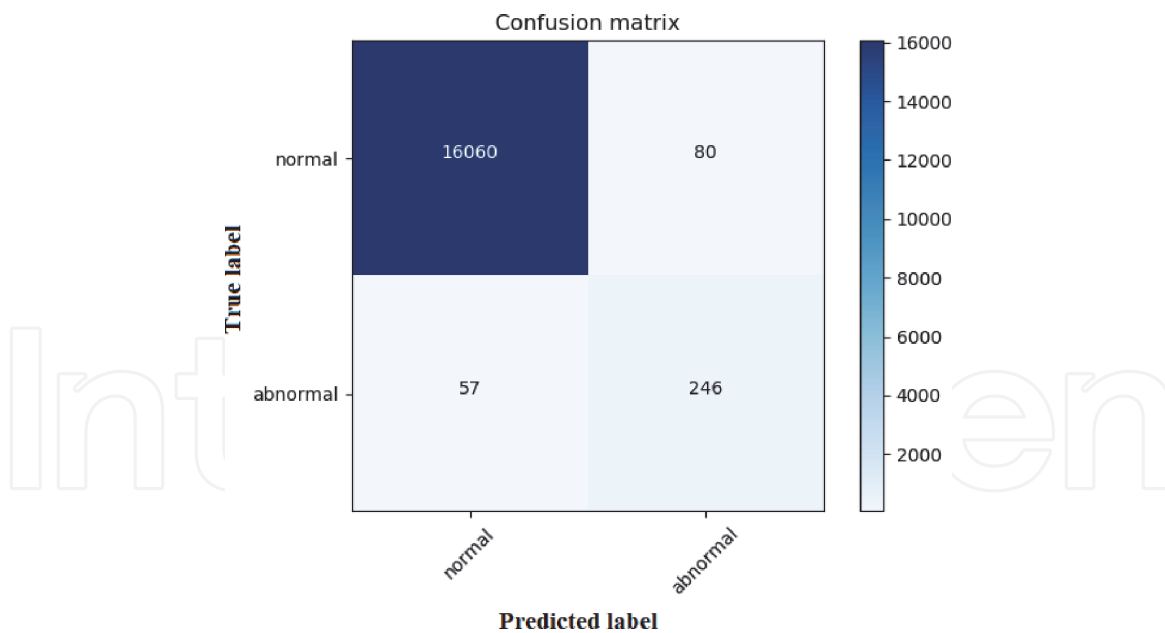
**Figure 16.**  
*ROC curve.*

### 3.1.2 Analysis and relaxation of ideal tracking assumptions - experimentation with noisy data

Most of the *false negatives* are abnormal trajectories that cannot easily be discriminated from the normal even by a human operator. Soft thresholding could be used in order to raise alerts for a human supervisor. On the other hand, the main reason for the *false positives* is the fact that airport travelers chose to move in ways that may not necessarily be similar to the normal trajectories. Large airport congestions make the aforementioned phenomenon even more intense.

Although the conditions the risk assessment algorithm was evaluated under assumed perfect knowledge of the traveler trajectories, relaxation of the assumption of perfect knowledge of the traveler trajectories by injecting noise in the position accuracy and/or assuming missing position data, did not have a considerable negative effect on the detection of abnormal trajectories as discussed next.

In order to assess the performance of the anomaly detection algorithm in realistic conditions we introduce noise in the data to emulate the uncertainty in passengers' positions reports. The "noisy data" emulate the inaccuracy in the reports of the



**Figure 17.**  
 Confusion matrix.

Measure	Value
Average PR score	0.66
ROC AUC (Area Under Curve)	0.97
F1-Score	0.78
Total Accuracy	0.99

**Table 1.**  
 Values of the recruited evaluation measures.

positions of the people in the space. Under realistic conditions, the tracking and risk assessment system will receive data from inaccurate sources, such as cameras, sensors, etc. used to estimate distances, mobile signal strength, etc.

In stark contrast, the iCrowd emulator produces people and their movements, and periodically reports the exact ones (so without noise) their positions in the risk assessment system. During the preprocessing of this data the possibility of the system to add Gaussian noise, the “volume” of which (parameter  $\sigma^2$  of Gaussian noise) is given by the user. This is obviously not intended to never be used in real application, and exists only for experimentation. For examining the behavior of the system under realistic conditions is required noisily data of different intensity.

Noise can enter the system in 2 cases: during training and during testing or actual application. It is known that when training any neural network, it is good to have variety in the data in which the network is exposed so that it is not over-trained. So, it is expected that training with Noisy data can improve the overall performance of the system. During testing or the actual implementation of the system would definitely be better to have perfect data, but unfortunately this is often impossible. In the context of the internship training and validation data were performed with Gaussian noise with  $\sigma^2$  from 0 to 1.9 with step 0.1, testing data with corresponding noise levels, and for each combination they were trained and evaluation of the neural network, and metrics were calculated for each of them. The metrics used were the Receiver Operating Characteristic curve (ROC curve), the Precision-Recall curve (PR curve), and the corresponding Area Under Curve (AUC) scores. These metrics give similar results, in the sense that they are defined

in  $[0,1]$  with value range  $[0,1]$ , so the minimum AUC value is 0 and the maximum is 1. Higher value means better true positive and true negative to false positive and false negative ratio. The two metrics generally return similar results, but in our case more weight is given in metric PR, as it offers a better estimate in cases that interest us more the positive class of results, or the results consist of significantly more elements of one of the two classes. Both features apply in the case of this risk assessment system.

During the experiment, networks emerged that failed to find an acceptable solution to why either they were trapped in a local minimum or they encountered the phenomenon of exploding gradient. These cases appeared to be random and independent of the parameters noise, so the network was initialized differently and the training started from the beginning. The experiments were performed using 3 levels of congestion in space, low, moderate, and high, and for each of them 40 neural networks were created, one for each training/testing noise combination mentioned above. For every desired network, 4 independent trainings were conducted and the averages of metrics of interest were kept. The same test data, corresponding to low-to-medium congestion, were used for testing all tested models. The final results are presented below (**Figures 18–20**):

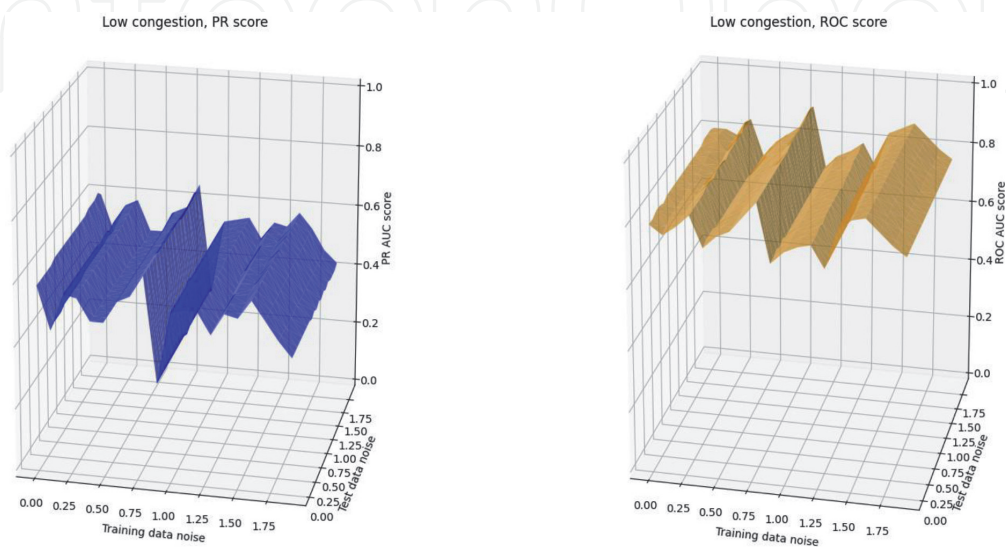
From the ROC AUC score graphs above, it is seen that the models that result in the highest performance correspond to the following noise level in the training data:

For low noise data, the best performing data with AUC = 0.91 corresponds to noise level  $\sigma^2 = 0.8$  in the training data.

For medium noise data, the best performing data with AUC = 0.96 corresponds to noise level  $\sigma^2 = 1.6$  in the training data.

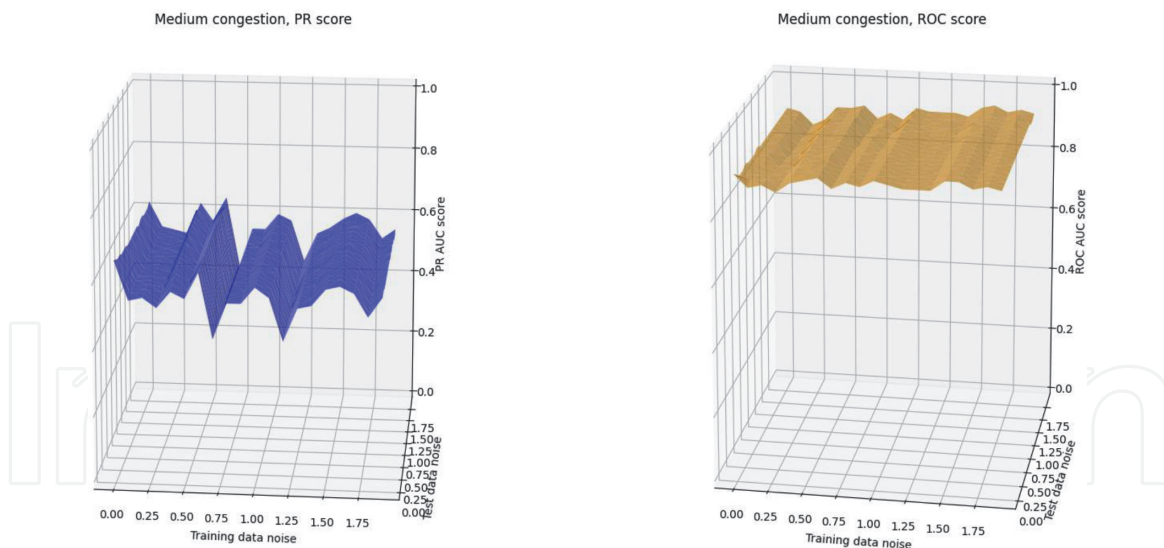
For high noise data, the best performing data with AUC = 0.95 corresponds to noise level  $\sigma^2 = 1.4$  in the training data.

From the above results it is clear that the performance of the networks remains constant when we apply noise to the test data. This implies that, since training completed, the network remains robust and is not affected by data noise, so it can to be used in a real application. Of particular interest are variations that occur when present noise in education data. As mentioned above, training a neuron network usually benefits from the difference in training data, as it helps learn the patterns that appear in the data instead of the data itself. This obviously does not mean that the more noise the better. In every network and for every application there is some optimal noise level that offers the best performance. At cases with low and

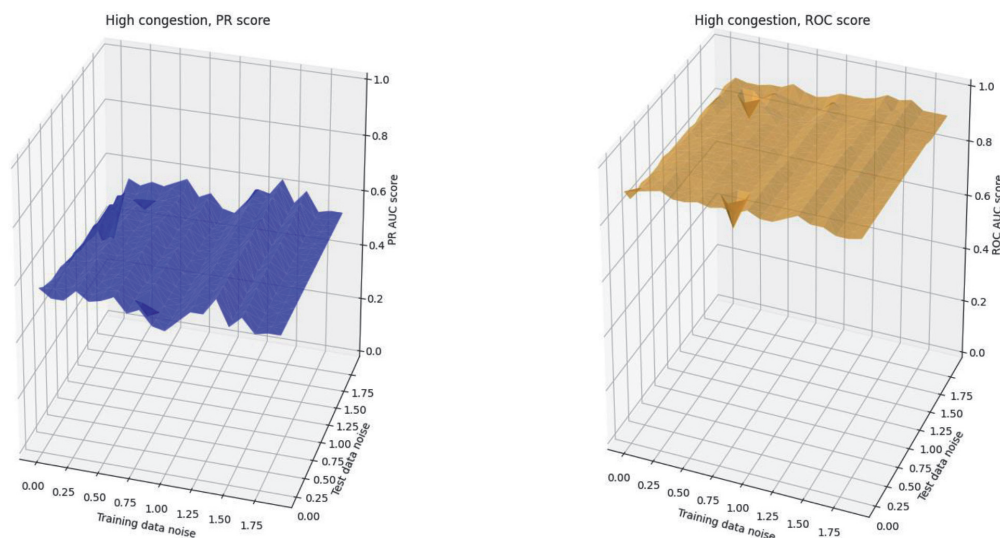


**Figure 18.** Training with low congestions data with different noise levels. Testing with low-to-medium congestion data.





**Figure 19.**  
 Training with medium congestions data with different noise levels. Testing with low-to-medium congestion data.



**Figure 20.**  
 Training with high congestions data with different noise levels. Testing with low-to-medium congestion data.

moderate congestion it seems that the Gaussian noise with  $\sigma^2 \sim 0.5\text{--}0.8$  has the best performance, while for high congestion the training with noise performs better with  $\sigma^2 \sim 1.4$ . The variance has not yet been attributed to any of its specific features network, model, training method, or data.

The evaluation results from the performance of the risk assessment algorithm with the iCrowd simulator demonstrates that risk assessment can be done accurately and without necessarily inducing additional delays in the security screening process since the trajectory classification in normal or suspicious is done by overhead cameras while the travelers go about their normal check-in routine at the airport. To that extent, the proposed risk assessment method based on anomaly detection on traveler trajectories can be used to improve the security screening effectiveness while keeping the delay low (or moving the operating point in **Figure 10** from high delay to low.).

Furthermore, the proposed method can be used as a financial investment tool for estimating the cost of acquiring the necessary equipment (in this case overhead cameras) for a certain level (probability of accuracy) before purchasing it, and for performing a trade-off analysis between the cost of acquisition of the necessary



equipment and the expected performance improvement in risk assessment. This way, the risk assessment simulator allows to be used as a cost–benefit tool for the analysis of performance of a risk-based security system.

### *3.1.3 Analysis, relaxation of ideal tracking assumptions and conclusions*

In its current form, the work in [9, 10] uses the time series of the coordinates of the trajectories of airport travelers for deep learning. In the future, additional features could be exploited. Such features are the velocity, acceleration and heading of the traveler. Moreover, alternative deep learning architectures could be tested such as the ones that account for contextual anomalies [11]. Furthermore, experiments on real-world data of human trajectories should be conducted. Such data are expected to contain more subtle and sophisticated anomalies. Finally, procedures that degrade data quality and emulate more realistic operational conditions are being implemented in order to test our system in the artificial presence of missing data, noisy data, data association issues, as is the case with data capturing devices operating under realistic operational conditions. Nevertheless, the present work and framework allow security investment decisions on tracking devices and infrastructure to be made by assessing the effectiveness of such an investment through the proposed risk assessment method that envelops the performance of any such system from above by considering ideal tracking conditions through perfect knowledge of all agents' location. The proposed method and framework is currently being extended to cover other border security modalities, such as sea, land as well as multimodal crossing points in the context of the EU-funded TRESSPASS project [4].

In conclusion, a deep learning architecture for real-time risk assessment based on the trajectories of airport travelers as proposed in [9, 10] can be used for assessing risk without interrupting or delaying the flow of passengers at an airport or BCP at large. The architecture implements a deep RNN network and is fully automated. Thus, it is expected to be of great use to the human operators monitoring airport surveillance footages, reducing the potential errors and misjudges. The proposed risk assessment system is tested on a realistic, synthetic data set generated with the iCrowd simulator tailored to data sets representing traveler movements at the Luxembourg airport; however, any airport or BCP could have been modeled and used instead. The experimental results are very promising and they indicate that further security improvements at airport control points are achievable through risk assessment without inducing additional delays. This is due to the fact that the suspicious behavior threshold, derived by the deep learning procedure in [9, 10], lies at such a level so as to capture the malicious behavior while, at the same time, reducing false-positive alerts.

## **3.2 Risk assessment using a security personnel application and IoT for behavior and event detection through suspicious signs reporting**

In [3] a GDPR compliant, mobile application was developed to allow security personnel on the floor of an airport, or any BCP, report in real time and with full respect to passengers' anonymity, suspicious behaviors, such as nervousness, unjustifiable sweating, etc., while passengers stand in security check lines. The mobile app works in conjunction with Smart Queue, another enabler of risk-based security [5]. Smart Queue is system that works in conjunction with passengers' ID documents; the system scans the passengers' ID document upon their arrival at the airport, or entry in the BCP, and in any subsequent security queue. This way, Smart Queue not only does it count the number of passengers at a queue waiting to go through security screening, but knows in which position in the queue each

passenger stands. This way, the security personnel that uses the security mobile app, needs to identify passengers only by their indexing number in the line they stand when reporting to the risk assessment back office system any suspicious behaviors about them. This way, anonymity of passengers and their personal data protection are maintained by the security mobile app. The information sent this way by the security personnel on the floor is then fused along with all other risk assessment reports about each passenger and the risk estimate is updated. The risk is reported to the security screening system and the passenger is classified in one of the three risk categories, namely green, yellow or red, as mentioned earlier.

In FLYSEC [3], a novel system architecture for Security and Safety surveillance systems that aims to identify adverse events or behaviors which may endanger the safety of people or their well-being has been introduced [12]. Through proper adaptations the system is applicable to a variety of monitoring systems for various critical infrastructures, border crossing points, and other places of interest (e.g., malls, mass transport systems). The proposed architecture depicts an Internet of Things (IoT) platform which comprises a sensing tier, a back – end processing and intelligence tier and a front end for visualization and user feedback tier. In further monitor and surveillance is performed mainly on the back – end intelligence component which consists of two modules: (a) the event detection module combined with a data fusion component responsible for the fusion of the sensors inputs along with relevant high level metadata, which are pre-defined features that are correlated with a suspicious event, (b) an adaptive learning module which takes inputs from security personnel about the correctness of the detected events, and uses it in order to properly parameterize the event detection algorithm. Moreover, a statistical and stochastic analysis component is incorporated which is responsible for specifying the appropriate features to be used by the event detection module. Statistical analysis estimates the correlations between the features employed in the study, while stochastic analysis is used for the estimation of dependencies between the features and the achieved system performance.

### *3.2.1 System architecture and interfaces*

The system architecture is organized basically in three tiers: Sensing components, back–end components, and front – end devices. The sensing components are responsible for acquiring input which is either high or low level heterogeneous data coming from visual sensors (CCD, IR, etc.), biometric sensors (fingerprints, other), audio sensors (microphones), indoor localization equipment (Wi-Fi, beacons, RFID scanners, etc.), document scanners which provide information about visitors (for example travel documents in an airport, or purchase information recorded on personal discount electronic cards), or human reports via terminal devices (e.g. PDAs, mobile phones, tablets, etc.).

Front–end devices are responsible for visualizing information to end–users and assisting their operations (for example official authorities receiving information about detected incidents of great interest, or visitors getting navigation information inside an infrastructure, etc.). Front–end devices consist of official management terminal tools which manage the information collected and processed by the back–end and sensing components and assist personnel operations by providing alerts and notifications about significant events (**Figure 21**), visualizations of infrastructure’s layout along with real – time updates about essential points of interest (for example size of queues, sensors viability, crowd distribution, etc.) (**Figure 22**). Moreover, front – end devices include also mobile user devices which operate as a personal assistant to passengers at an airport or a BCP. These mobile devices may provide online and offline services regarding indoor navigation, recommendation

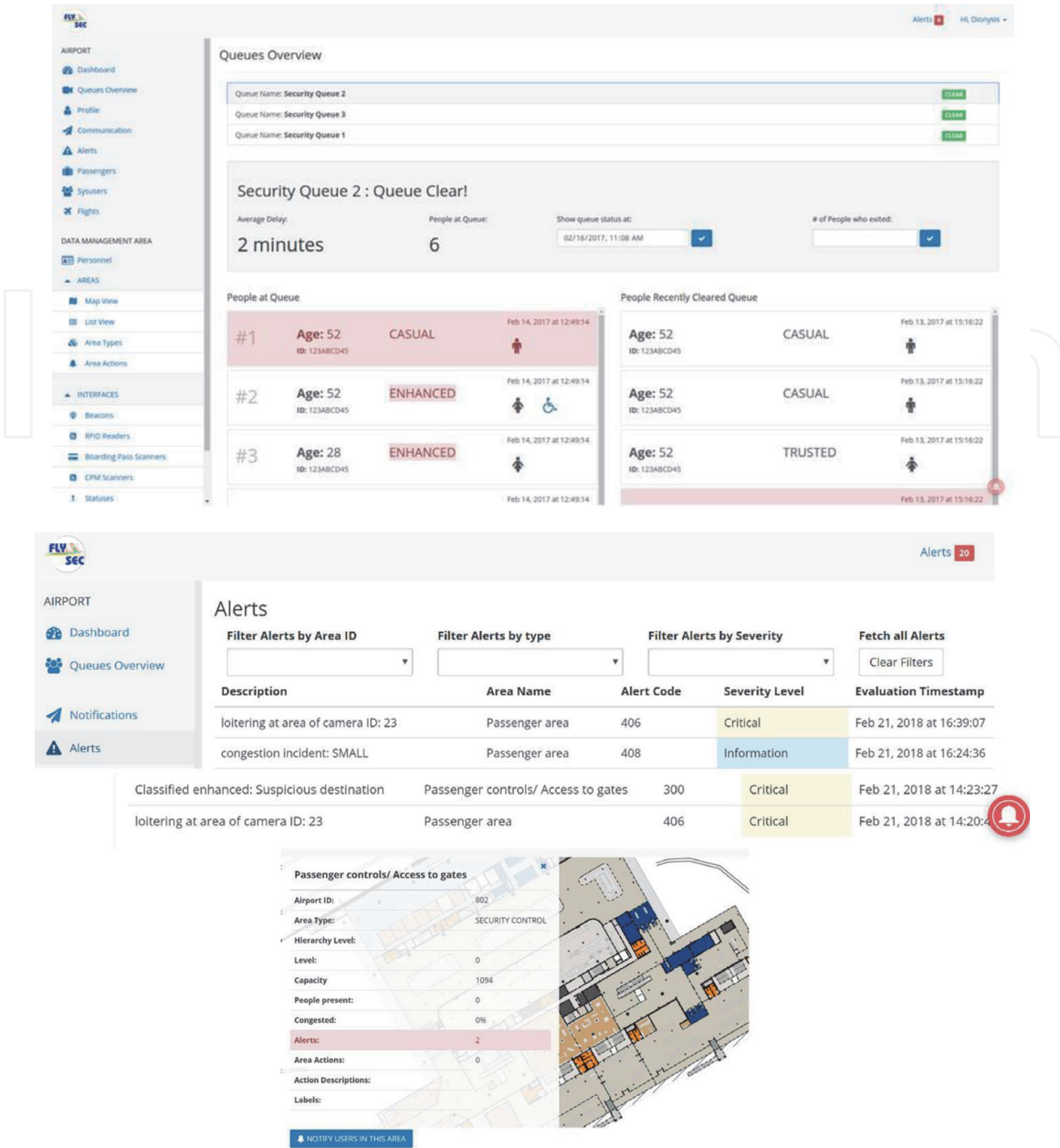


Figure 21. FlySec portal: - intelligent services visualization (upper); - automatic passenger classification (lower).



Figure 22. FlySec portal - layout visualization.



services (for products, point of interests, etc.), notifications and alerts. Finally, via these devices each user may provide a feedback to the system about requests or reports, about incidents that may concern their safety, or public security, or interactions with the system in the context of system automatic personal servicing.

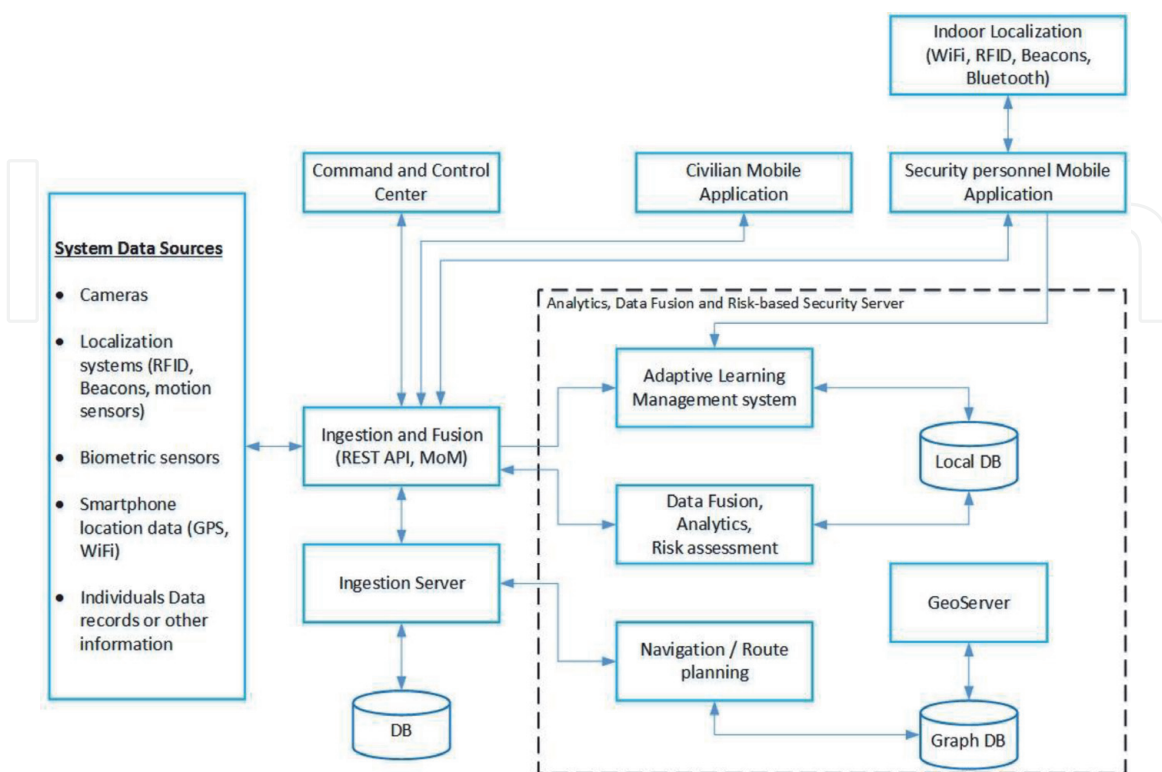
The back-end component contains the intelligence modules which process the input coming from sensing devices and produce high level intelligence and meta-data which assist operational personnel, enhance end-users' experience and content management services. These metadata are used either for further processing by fusion algorithms, or presented to end – devices via visualization methods on each end-device. Such metadata concerns directed paths for navigation services, fused high level visual information, or information regarding recommendations, detected incidents or notifications and alerts. Finally, the content management services enable efficient data storing and retrieving operations in a scalable way. The back – end component comprises a Message-oriented middleware in order to interconnect all the sensing and processing component, provides a REST API to front-end devices, supports web platforms interfaces (web – portal) and orchestrates the accurate functionality of the whole system, **Figure 23**.

The core intelligence residing in the “Analytics, Data Fusion and Risk-based Security Server” is presented in Section 3.3. The Data protection, Legal Compliance and Ethics are important aspects that should be taken into consideration in the system architecting process and are analyzed in Section 3.4.

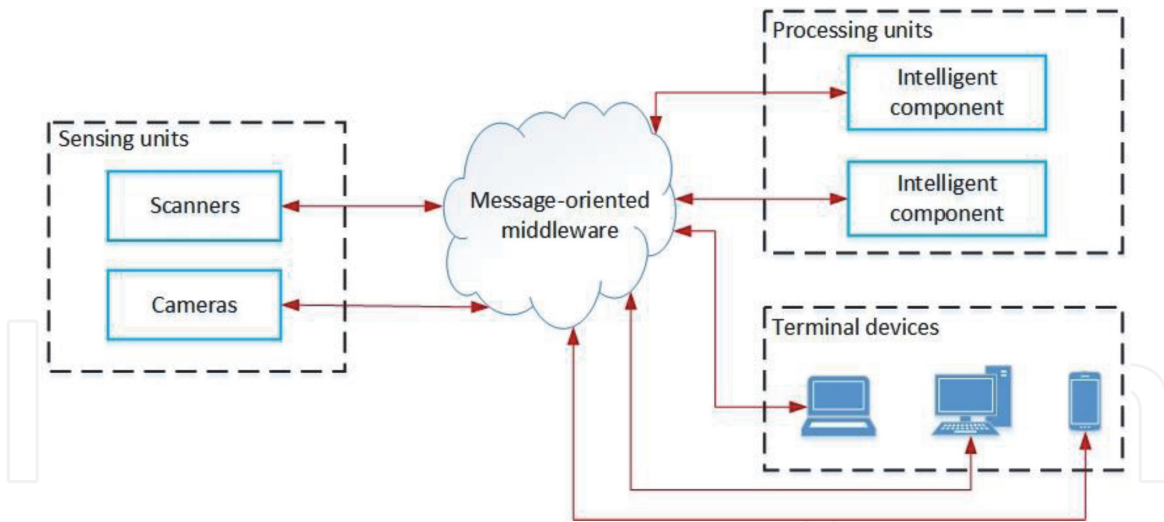
### 3.2.2 Analytics, data fusion and risk-based security server

#### Back-end Intelligence component

The proposed system is designed with the aim of enabling automated surveillance of large infrastructures such as airport, shopping malls, other. Such tasks incorporate massive monitoring of infrastructure visitors in real – time. Monitoring operation is based on an Internet of Things (IoT) installation architecture consisting of: (a)



**Figure 23.** Reference architecture of the FLYSEC security and safety risk-assessment surveillance system.



**Figure 24.**  
Back-end intelligence system architecture.

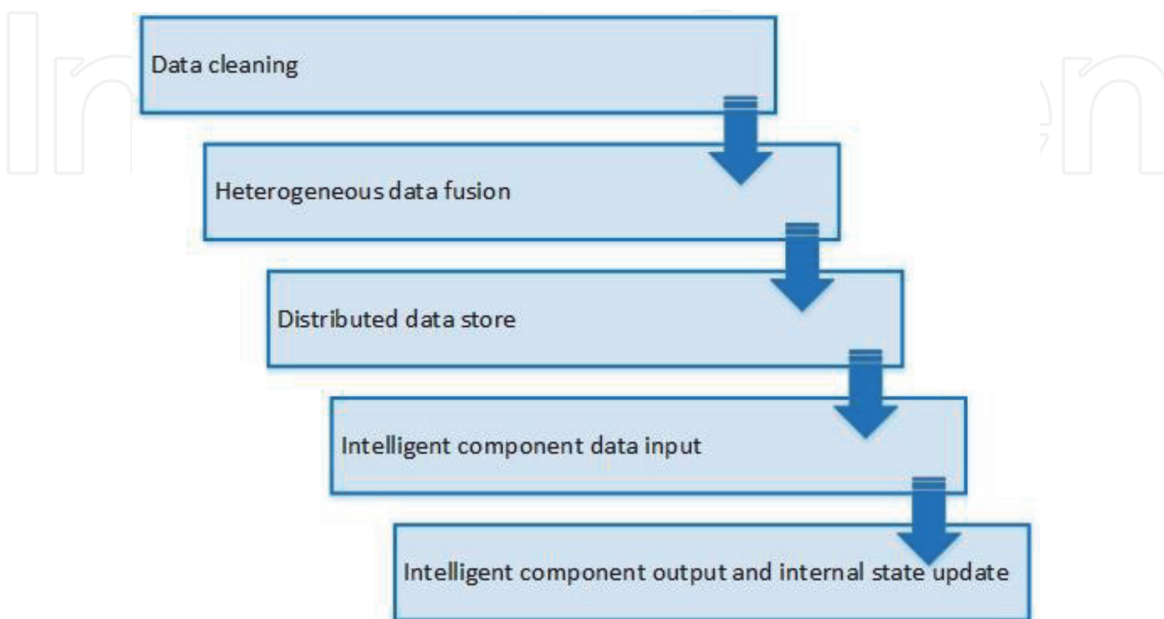
various types of sensing devices such as CCD surveillance cameras, QR/barcode scanners, localization equipment (NFC tags, WiFi beacons, etc), RFID scanners, etc., (b) processing units, both centralized and/or distributed, and (c) terminal devices such as mobile phones/tablets, computers, screens, electric signs, etc. (Figure 24).

Each sensor device may pre-process the acquired raw data (distributed processing) and the results are gathered on a central cloud-computing infrastructure consisting of independent but co-operative intelligent component each one dedicated for processing data and producing a specific intelligent response for the system. Moreover, the output is transferred to terminal devices. This processing procedure consists of the following steps (Figure 25).

The intelligent services are also responsible for automating the monitoring procedure and enhancing visitors' experience. Therefore, we propose two types of services: (a) *Assistance services* and (b) *Surveillance services*.

**Assistance services**

These services aim at monitoring visitors' behavior, profile, and interactions and provide information that could facilitate their purpose of visit and indicate services



**Figure 25.**  
Flow of data from sensors to the cloud or terminal devices.



that act as added value to visitors and simultaneously promote each infrastructure expectations. Indicatively two representative use cases are Navigation services and Recommendation engine.

- Navigation service corresponds to indoor localization and navigation of infrastructure visitors in order to assist them in reaching their desired points of interest (POI) not only as quickly as possible but also as efficient and desirable as possible by taking into account user requirements (e.g. disabilities, specific demands) and user location. Moreover, the service provide directions to each visitor via their mobile device to various POIs and informs the user in order to assist them reaching their goal of visit (for example provide information about location of various products in a supermarket, or shops in a mall, or provide information about flight departures or gates status in an airport)
- Recommendation engine aims at providing suggestion of POIs or services that take place inside the infrastructure. The engine takes into account the user profile (information that each user provides optionally during account registration), user feedback (comments, rates), user location and contextual information (time, season, POI status) and create recommendations that are estimated to be assistive to user visiting experience but also promoting infrastructure and POIs expectations and benefits.

### **Surveillance services**

These services aim at monitoring visitors' position and behavior and automatically detect incidents of significant interest such as malicious behavior, anomalous crowd trajectory flow etc. This solution is expected to enhance surveillance procedure for large-scale circumstances where it is demanded in real time, the accurate surveillance of a massive crowd. Indicatively we suggest two surveillance services: Suspicious unattended luggage incidents detection and suspicious visitor loitering detection.

- Unattended luggage incidents detection aims at monitoring in parallel both visitors and the luggage they carry. Such monitoring could be approached either using CCD cameras and approximately detect abandoned luggage for a long period of time, or by tagging luggage (for example using RFID tags) where using RFID scanners in co-operation with visual sensors (CCD cameras) and human reports (official surveillance personnel), estimate potential unattended luggage incidents. Moreover, in order to monitor visitors' position, we propose the use of indoor localization techniques using mobile devices in order to have an approximation of visitors' location that willingly allow it, and in addition visual sensors and human reports as well, in order to increase system's awareness of crowd location. Fusion of such information shall be exploited by machine learning algorithms, which result to a coarse grain estimation of visitors' luggage abandonment.
- Suspicious loitering detection aims at monitoring visitors' location and in real-time detect anomalous visitors' trajectories or positions that could be suspicious for malicious purposes. Such components may incorporate visual sensors (CCD cameras), human reports and mobile devices localization techniques (Wi-Fi beacons, NFC tags).

### **Data fusion and Risk-based assessment**

The Data Fusion unit inside the Analytics, Data Fusion and Risk-based Security Server aims to perform Hard and Soft fusion of heterogeneous data [13–15]

available from disparate sources of information such as physical sensors (“hard” data) and human resources (“soft” data). Hard data fusion refers to the combination of raw information from multiple sources so as to achieve more accurate estimations of the desired parameters (position, speed, other). To this end, a variety of theoretical tools, such as Signal processing techniques, Kalman filters, Sequential Monte Carlo methods, etc., can be used. On the other hand, soft data fusion usually applies on textual information (e.g., from humans’ reports, social networks, Internet, other) which has to be further processed using methods such as Information retrieval, Natural Language processing, and Semantic knowledge representation. Moreover, in this unit, Decision level fusion techniques could be applied using Evidence theory [14–16], Fuzzy Logic [17], 2-tuple Linguistic representation models [18, 19], and reinforcement learning methods [20, 21].

The Risk-based assessment unit is responsible for the classification of events and individuals into security classes according to their risk severity level. The unit exploits behavior and event indicators and their corresponding weights estimated in the ALMS system, intelligence generated in the Back-end Intelligence component, and any useful information from the system’s data sources in order to generate alerts and notifications to the Command-and-Control (C2) center if the risk severity level exceeds predefined thresholds.

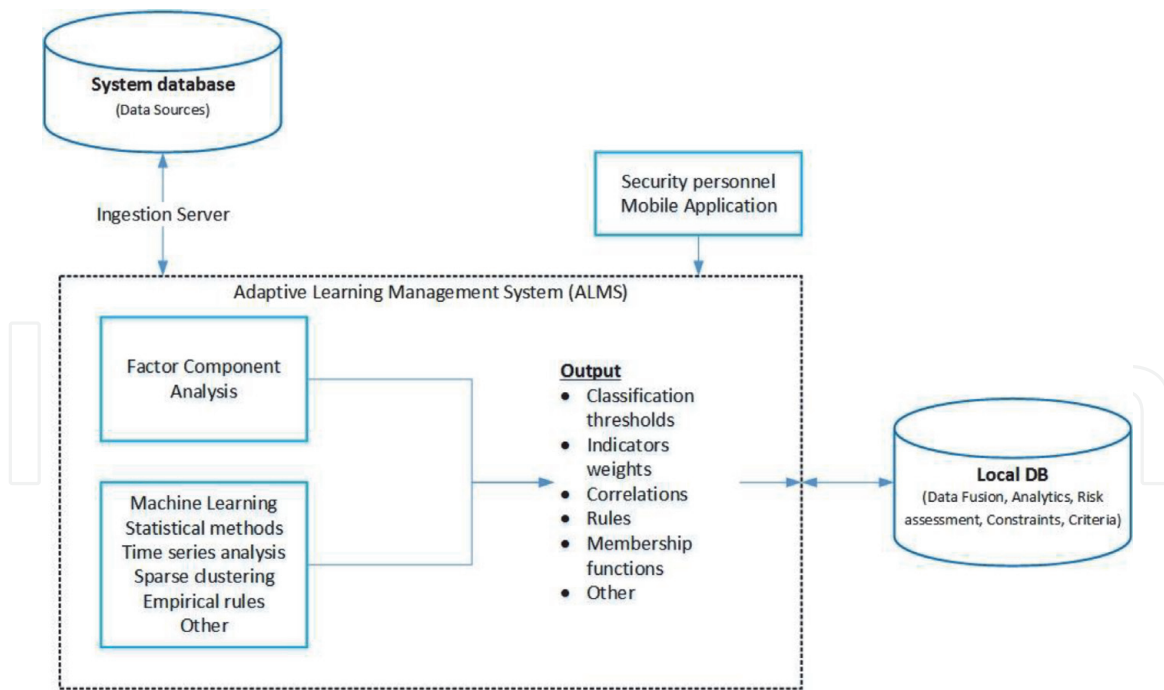
#### **Adaptive learning management system**

A security and safety monitoring system has to detect, evaluate, and classify, in an efficient and timely manner, behaviors and events of interest. To achieve this critical need, the algorithmic parameters used in the “Analytics, Data Fusion and Risk-based Security Server” have to be initialized and adaptively adjusted to handle changes in the monitoring environment. To this end, the use of an Adaptive Learning Management System (ALMS) which will exploit new and accumulated information is essential. An ALMS system can be applied for instance to iteratively adjust the Risk Assessment classification thresholds and the weights of the behavioral and event indicators or to recognize correlations between indicators, events, and behaviors in order to optimize the classification process and improve the efficiency of the system. An example of such an optimization approach could be the selection of a reduced number of indicators for event identification.

For the development of automated procedures able to estimate correlations, optimize selected parameters under certain criteria, and extract reduced dimensional feature vectors for Behavior and event detection the ALMS system demands efficient methodologies and algorithms. These methodologies and techniques can cover a wide area of theoretical tools including Machine Learning, Factor Component Analysis, Statistical methods, Time series analysis, Optimization theory, Sparse clustering, Fuzzy Logic, and other [18–21].

As shown in **Figures 23** and **26**, the ALMS unit receives input from i) the system’s database which includes data from system’s data sources, outputs of Data Fusion, Analytics, and Risk assessment unit, and optimization criteria and constraints and ii) the Security personnel Mobile App which is then used for the training of the applied algorithms. The ALMS stores its output in the system database, making it accessible to other units, and creating a continuous feedback loop of information gathering, learning, and adapting to security threats as they evolve.

The Factor Component Analysis component performs Factor Analysis on features/indicators denoting individual characteristics which affect the categorization of individuals in security-threat levels. Factor analysis is used to reduce the dimensionality of a correlation matrix that contains features/indicators describing a specific event or behavior. Factor Analysis does that by producing new general variables, called “factors”, incorporating inside them, the initial features/indicators according to a condition of high inter-correlation between the newly



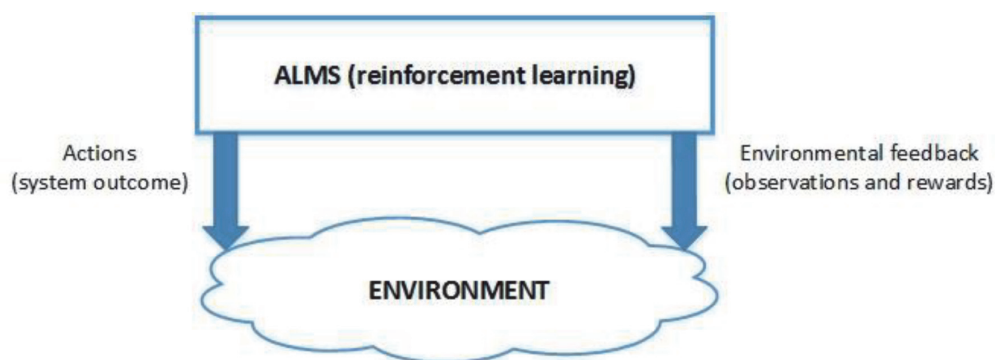
**Figure 26.**  
 The adaptive learning management system architecture.

emerged general variables (“factors”) and the initially presented specific variables [19, 22].

The system needs to analyze the input feed and result to its outcome, taking into account however, environmental factors regarding system’s efficiency, explicit policies that should be adopted or exceptions that should be applied, that are related to specific locations (e.g., restricted areas) or specific human profiles. Such information usually is returned to the system in the form of a generic asynchronous qualitative feedback (for example insisting user discards of system’s outcomes, or exception to system’s rules) that should be assimilated in real – time.

The system should be able to receive environmental feedback and adapt its operation to the current circumstances and requirements. Therefore, we propose a two-mode adaptation, an offline and an online. The offline adaptation regards a system initialization, responsible for translating human – understandable requirements to algorithms’ parameterization. The online adaptation should track environmental feedback for each action of set of actions (policies) produced by the system and adapt algorithms’ behavior in order to fulfill system’s requirements.

In this case we propose the implementation of reinforcement learning techniques where environmental feedback should be encoded to quantitative measures of rewards, **Figure 27**.



**Figure 27.**  
 Online ALMS.

### *3.2.3 Data protection, legal compliance and ethics*

Security and safety management systems and their data fusion and intelligent analytics capabilities require substantial data collection and processing in order to offer the best possible awareness and decision support to C&C operators, field personnel and first responders. Especially in the context of homeland security, privacy and data protection is often seen through the typical trade-off model perspective, requesting the public to give up –in the best case knowingly- on particular rights over the control of their personal data. However, such systems should not be based and developed on exceptions or operate only in extraordinary circumstances, the latter being very inefficient. With the latest guidelines of EU General Data Protection Regulation (GDPR), principles of data minimization and privacy by design will shift from best practices into a much more regulated form.

The proposed system is in line with these principles, following a “by design approach” in terms of data protection and ethics. Data collected are structurally separated from identifiable information, and identification occurs only upon the logged and explicit intervention of a human operator when truly needed. By assessing risks on real time, the system itself has the advantage of performing data minimization through early elimination of lower risk cases. On the front end and field, privacy enhancing technologies and smart sensors are also preferred and selected. E.g. smart visual sensors with on-board processing capabilities can filter out data before sending it over the wire and to the server for processing. Moreover, the system has been designed to include specific safeguards to protect individuals against discrimination, stigmatization and unduly prohibition of access to goods and services. Defined in [23], the system adopts these definitions and extends them to all protected grounds as defined in the Charter and the Treaty of Amsterdam, taking also into account the proposal for the horizontal directive that extends the context of EU non-discrimination law and prohibits discrimination “on grounds of sex, racial or ethnic origin, age, disability, sexual orientation, religion or belief”. In this context, Fairness and bias detection algorithms are applied to the adaptive learning management system while the human operator remains in control of the final enforcement following any automated decision making process. Intelligent behavior analytics can further support the case where security risks are based and calculated on how a person acts on the scene and not any discriminatory background information.

A subject of past and current research, assessing the societal acceptance of surveillance and security solutions comes with its own challenges. Acceptance is based on multiple parameters, individual perceptions and sometimes misconceptions and individual practices which may not be in line with the expressed concerns [24]. The proposed system and the overall risk-based security paradigm, is based on the positive fact that the vast majority of people have no malicious intent. The system focuses on the unknown and high-risk cases, intending to shift the current practices from annoying horizontal and disruptive processes to seamless and unobtrusive security. The combination of privacy and ethics by design along with the ethical and unobtrusive treatment set the parameters for a system with high acceptance, positive public perception and trust.

## **4. Conclusions**

In this chapter we discussed the concept of risk-based security, the possible trade-off between increased convenience for passengers from risk-based security and the delays induced by additional checks needed for establishing each



passenger's risk. We also presented a number of technologies, systems and applications that can be used for assessing risk at an airport or BCP without inducing additional delay as the discussed approaches estimate risk on-the-fly while passengers either walk around the airport or BCP from entrance to security check points or BCPs, or queue up in a security line awaiting to go through security checks. All methods discussed are GDPR and ethics compliant, thus they can be implemented in accordance to privacy and ethics regulations. Furthermore, the novel system architecture for Security and Safety monitoring systems introduced in [3] has been presented. The proposed system aims to identify adverse events or behaviors which may endanger the safety of people or their well-being having the ability to adapt in the surveillance environment changes. The dynamic adjustment of the algorithmic parameters adopted in various units of the system such as intelligence, and Risk assessment, makes it possible to monitor security threats as they evolve. Thus, the proposed scheme provides the potential of a high-performance system both in terms of the detection interval as well as in terms of the performance accuracy offering the capability of a timely and efficient response to abnormal events and behaviors.

## Acknowledgements

The research described in this paper has been supported by the following research contracts:

“FLYSEC: Optimizing time-to-FLY and enhancing airport SECurity,”  
Programme: Horizon 2020, European Union Grant Agreement No. 653879, Duration: 01/05/2015 - 31/07/2018, <http://www.fly-sec.eu>.

“TRESSPASS: Robust Risk Based Screening and Alert System for Travelers and luggage,” Grant Agreement No. 787120, Call: H2020-SEC-2016-2017-2, <https://www.tresspass.eu/The-project>.

The author would also like to acknowledge the use of some material from the Refs. [5–10, 12, 14]. He co-authored in collaboration with his colleagues whose names appear in these references.


IntechOpen

## Author details

Stelios C.A. Thomopoulos  
Integrated Systems Laboratory, Institute of Informatics and Telecommunications,  
National Center for Scientific Research “Demokritos”, Greece

\*Address all correspondence to: [scat@iit.demokritos.gr](mailto:scat@iit.demokritos.gr)

## IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 



## References

- [1] European Commission: “Smart Borders Package”: [https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en)
- [2] IATA Checkpoint of the Future: <http://www.iata.org/pressroom/pr/Pages/2011-06-07-01.aspx>
- [3] “FLYSEC: Optimizing time-to-FLY and enhancing airport SECURITY,” Programme: Horizon 2020, Contract No. 653879, 01/05/2015–31/07/2018, funding organization: European Union, <http://www.fly-sec.eu>.
- [4] “TRESSPASS: Robust Risk Based Screening and Alert System for Travelers and luggage,” Programme: Horizon 2020, Contract No. 787120, Call: H2020-SEC-2016–2017-2, funding organization: European Union, <https://www.tresspass.eu/The-project>.
- [5] Stelios C. A. Thomopoulos, Dimitris M Kyriazanos, Andreas Zalonis, ‘FLYSEC: A comprehensive control, command and Information (C2I) system for risk-based security’, Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII, v. 10646, International Society for Optics and Photonics, 25/6/2018.
- [6] V. Kountouriotis, S. C. A. Thomopoulos and Y. Pangelis, “An agent-based crowd behaviour model for real time crowd behaviour simulation.” Pattern Recognition Letters/Pattern Recognition and Crowd Analysis, vol. 44, pp. 30–38, (2014).
- [7] Kountouriotis V. I., Paterakis M., and Thomopoulos S. C. A., “iCrowd: agent-based behavior modeling and crowd simulator,” SPIE DSS 2016 - Defense, Security and Sensing, Convention Center Baltimore, Baltimore, Maryland, United States, 17–21 April, (2016).
- [8] Daveas S., and Thomopoulos S. C. A., “Embedding a Distributed Simulator in a Fully-Operational Control & Command Airport Security System,” in Proceedings Volume 10646: Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII, June (2018).
- [9] Stelios C. A. Thomopoulos, Stelios Daveas and Antonios Danelakis, “Automated real-time risk assessment for airport passengers using a deep learning architecture,” Proceedings Volume 11018, Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII; 110180O (2019) <https://doi.org/10.1117/12.2519857> Event: SPIE Defense + Commercial Sensing, 2019, Baltimore, Maryland, United States, 2019.
- [10] Giorgos Bouritsas, Stelios Daveas, Antonios Danelakis, Stelios CA Thomopoulos, “Automated Real-time Anomaly Detection in Human Trajectories using Sequence to Sequence Networks,” 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), p. 1–8, 2019/9/18.
- [11] Rikard Laxhammar, Göran Falkman, and Egils Sviestins, “Anomaly detection in sea traffic - a comparison of the Gaussian Mixture Model and the Kernel Density Estimator,” in [IEEE International Conference on Information Fusion], (2009).
- [12] Konstantinos Georgios Thanos, Constantinos Rizogiannis, John M. A. Bothos, Dimitris M. Kyriazanos, Andreas Zalonis, Stelios C. A. Thomopoulos, “A novel architecture for behavior/event detection in security and safety management systems”, Proc. SPIE 10200, Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI, 102000R (16–19 April

2018). Proceedings Volume 10646, Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII; 106460V (2018) <https://doi.org/10.1117/12.2307079>. Event: SPIE Defense + Security, 2018, Orlando, Florida, United States

[13] Klein, L. A., [Sensor and Data Fusion: A Tool for Information Assessment and Decision Making], SPIE press (2004).

[14] Thomopoulos, S. C. A., “Sensor Integration and Data Fusion,” Proc. SPIE 1198, Sensor Fusion II: Human and Machine Strategies, 178–191 (1990).

[15] Raol, J. R., [Multi-Sensor Data Fusion with MATLAB], CRC Press (2009).

[16] Shafer, G., [A Mathematical Theory of Evidence], Princeton University Press, Princeton, NJ (1976).

[17] Pedrycz, W. and Gomide, F., [An Introduction to Fuzzy Sets: Analysis and Design], MIT Press (1998).

[18] Martínez, L. and Herrera, F., “An overview on the 2-tuple linguistic model for computing with words in decision making: Extensions, applications and challenges,” *Information Sciences* 207 (1), 1–18 (2012).

[19] Rietveld, T. and van Hout, R., [Statistical Techniques for the Study of Language and Language Behaviour], (1993).

[20] Mnih, V., Badia, A. P., Mirza, M., Graves, A., Lillicrap, T. P., Harley, T., Silver, D. and Kavukcuoglu, K., “Asynchronous Methods for Deep Reinforcement Learning,” Proc. of the 33rd International Conference on Machine Learning, New York, NY, USA (2016).

[21] Sutton, R. and Barto, A., [Reinforcement Learning: An Introduction], MIT Press, (1998).

[22] Field, A. P., [Discovering Statistics Using SPSS for Windows], (2000).

[23] D. Potoglou et al, “Literature Review of Approaches for Measuring Preferences with Respect to Privacy, Security and Surveillance,” *The Privacy & Security – Research Paper Series*, (2014).

[24] FRA Handbook of EU non-discrimination law, available online (Accessed March 2018): [http://fra.europa.eu/sites/default/files/fra\\_uploads/1510-FRA-CASE-LAW-HANDBOOK\\_EN.pdf](http://fra.europa.eu/sites/default/files/fra_uploads/1510-FRA-CASE-LAW-HANDBOOK_EN.pdf).