# A dynamic and scalable solution for improving daily life safety


Antonello Calabrò
Istituto di Scienza e Tecnologie dell'Informazione
Consiglio Nazionale delle Ricerche, ISTI-CNR
Pisa, Italy
antonello.calabro@isti.cnr.it

Eda Marchetti
Istituto di Scienza e Tecnologie dell'Informazione
Consiglio Nazionale delle Ricerche, ISTI-CNR
Pisa, Italy
eda.marchetti@isti.cnr.it

Davide Moroni
Istituto di Scienza e Tecnologie dell'Informazione
Consiglio Nazionale delle Ricerche, ISTI-CNR
Pisa, Italy
davide.moroni@isti.cnr.it

Gabriele Pieri
Istituto di Scienza e Tecnologie dell'Informazione
Consiglio Nazionale delle Ricerche, ISTI-CNR
Pisa, Italy
gabriele.pieri@isti.cnr.it



## ABSTRACT

The integration of computation, networking, and physical processes requires regular exchange of critical information in timely and reliable fashion and a secure modeling and control engine able to rule and to coordinate all different sources of information. In this paper we provide the description of a dynamic and flexible infrastructure to be installed and applied into daily realities, able to maximize safety and security with an extremely low impact on the maintenance and the updating effort. The proposal has been conceived in collaboration with an Italian kindergarten. Preliminary results collected during simulation and testing activity are encouraging.



## KEYWORDS

Smart sensors, Monitoring, Access Control, Safety, Indoor localization, RFID, Clustering

**ACM Reference format:**
Antonello Calabrò, Eda Marchetti, Davide Moroni, and Gabriele Pieri. 2019. A dynamic and scalable solution for improving daily life safety. In *Proceedings of Applications of Intelligent Systems, Las Palmas de Gran Canaria, Spain, January 2019 (APPIS2019),* 6 pages.
https://doi.org/10.1145/nnnnnnn.nnnnnnn


## 1 INTRODUCTION

Nowadays the use of different devices able to provide integrated computation, ubiquitous networking, and implementation of physical processes is speedily increasing. These provide the possibility to directly monitor and control physical objects so as to infer and apply rules and obligations also connected to specific personal behaviours with a visible improvement of the quality life of citizens.

The integration of computation, networking, and physical processes requires regular exchange of critical information in timely and reliable fashion and a secure modeling and control engine able to rule and to coordinate all different sources of information. As evident from the literature [32], usually it is possible to distinguish between three levels of rules: i) *Sensors rules* i.e., the rules for managing and correlating sensors data and technologies; ii) *Usage rules* i.e., the rules able to guide the Software Engineering (SE) process to define the users and the systems behaviour, and to protect against possible problems and inconveniences faults; iii) *Access control rules* i.e., the rules that manage the resources (sensors, technologies, data, and so on) and protect against possible malicious use or security flaws [26].

In this paper, based on the low cost, smart and flexible architecture provided in [1, 3] for the management and control of smart buildings, we propose a tailored solution for the daily reality of a kindergarten.

Specifically, the main goal of this paper is to provide a dynamic and flexible infrastructure to be installed and applied into daily realities, able to maximize safety and security with an extremely low impact on the maintenance and the updating effort. In the development and deployment of the proposed infrastructure, important requirements have been considered: i) privacy preservation; ii) the low cost of the proposed solutions; iii) the unobtrusiveness of the installations; iv) the possibility of integration with other possible existing equipment.

The paper is organized as follows. Section 2 provides a motivating example to better explain the idea of the paper. Background knowledge is provided in Section 3, while the infrastructure is described in Section Section 4. Finally, Section 5 gives a set of conclusions and the envisioned future work.

## 2 MOTIVATING EXAMPLE

To better explain the solution adopted, here we describe a very simple example of application considering an Italian kindergarten, where different kinds of people (educators, parents, children, janitors, guardians and so on) can access specific areas (or rooms) of the building, thus requiring different Sensors, Usage, and Access control rules. The proposed application is well in line with the recent regulatory trends promoted by the Tuscany Region in Italy [30] and might provide a set of services answering the precise safety needs of local stakeholders.

In the kindergarten, some of the rules that manage and coordinate the sensors (e.g., temperature, humidity, $CO_2$, and locks) and the actuators (e.g., door and windows locks, heating valves,



*APPIS2019, January 2019, Las Palmas de Gran Canaria, Spain*



ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

remote controlled plugs, air-conditioner) could be defined considering specific scenarios. For instance in the considered structure some elicited requirements are: i) the necessity to control the entrance times of each kid so as to promptly activate alarms for the parents and tutors in case of important deviations; ii) the necessity to control the entrances (doors and windows) and dangerous furniture/plugs of the building so as to assure that none of the kids could open/use it unless under the surveillance of adults; iii) notification in case some of the kids stay alone in some rooms longer than required; iv) localization of each kid in case of emergency situations.

These simple rules can be characterized for each specific kindergarten and can be directly embedded into the engine controlling the sensor behavior so as to reduce the maintenance effort. Other can be dynamically enacted to better satisfy the management of the school and the exigencies of the educators. For instance, the different activities executed in common rooms (physical exercises, rest period, drawing and so on) could involve different Sensors, Usage and Access rules depending on the day, time and person involved. The following are some examples of rules: (i) heating should be automatically increased during rest period or decreased in case of physical exercises; (ii) windows cannot be opened and lights must be set up to a dimmer profile during rest period; (iii) children access to garden is inhibited if a gardener is in the area.

These are just simple examples of rules, voluntarily ignoring complex, safe, and security aspects of the kindergarten management. Not all the mentioned rules have to be verified at the same time and in all situations. The peculiarity of the proposed system is to leave the freedom to the school to define each time the more suitable rules for their purposes. This can be done either by specifying the proper rules or selecting the most suitable ones from a pre-defined collection of frequently adopted rules.

Of course, the rules specifying the school management could have been implemented once for all, writing a standard usage control policy enforced by a standard usage control engine, as in many current available proposals. One of the challenges of the proposed infrastructure is the possibility of tailoring and customize different sets of rules. Specific internal features and tools are in charge of the management of possible errors and inconsistencies to promptly correct them.

# 3 BACKGROUND AND RELATED WORKS

## 3.1 Monitoring

Several proposals for monitoring are available, we can be mainly divide it into two groups: monitoring systems embedded in the core platform or the execution engine of the service, such as [10, 20], and those that can be integrated into the execution framework as an additional component, such for instance [8, 17, 18]. Both the solutions have specific advantages. For sure, an embedded solution reduces the performance delay of the execution framework, mainly in terms of interactions and communication time. Different indicators can be directly evaluated by the execution framework, which can also execute corrective actions in case of important deviations. The main disadvantage of these approaches is the lack of flexibility in the data collection, the rules definition and the language adopted. Usually, in these proposals, all the interested parameters have to be predefined and modeled directly into the platform engine, by means of specific editors, and are dependent on the notation used for the policy definition. In this paper we would like to overcome the above mentioned issue by proposing a monitoring framework on which rules are independent by components of the overall infrastructure and relative rules and parameters can be updated at runtime.

Among the additional monitor facilities, in this paper we refer to the framework called `Glimpse`[1], which is extremely flexible and adaptable to various scenarios and SOA architecture patterns.

## 3.2 Access control

*Access control systems* is a way to ensure that access to assets is authorized and restricted based on business and security requirements (ISO/IEC 27000, 2018[2]). Access Control ensures that only the intended people can access security-classified data and that these intended users are only given the level of access required to accomplish their tasks. Access control mechanisms usually rely on the eXtensible Access Control Markup Language (XACML) [28] for specifying Access Control Policies, which are specific statements of what is allowed and what is not. Briefly, an XACML policy has a tree structure whose main elements are: PolicySet, Policy, Rule, Target and Condition. The PolicySet includes one or more policies. A Policy contains a Target and one or more rules. The Target specifies a set of constraints on attributes of a given request. The Rule specifies a Target and a Condition containing one or more Boolean functions. If the Condition is evaluated to true, then the Rule's Effect (a value of Permit or Deny) is returned, otherwise a NotApplicable decision is formulated (Indeterminate is returned in case of errors). The PolicyCombiningAlgorithm and the RuleCombiningAlgorithm define how to combine the results from multiple policies and rules respectively in order to derive a single access result.

## 3.3 Positioning and activity recognition

The possibility of using sensory data to infer the location of persons and objects and to perform Human Activity Recognition (HAR) has received much attention in the last decade. A plethora of sensor technologies might be used for this purpose, also exploiting multimodal approaches for which reference datasets are available to the research community [33]. Radio-Frequency IDentification (RFID) technology has appeared as one of the most promising, since RFID tags are inexpensive and their reduced size allows to embed them in everyday objects including garments. Localization technologies can achieve millimetric accuracy using active RFID tags and phase differencing approaches [25, 27], but -for the use in daily realities as addressed in this paper- passive RFID tags appear to be more convenient since they do not require an internal power source and are more durable, hard-wearing and resistant to washing cycles. With particular configurations of RFID reader antennas, centimetric accuracy can be obtained even with the passive tag technology [22]. Since passive tags act as transponders and no direct active emission is involved, the total radio frequency power is extremely low, which poses less concerns in acceptance for use in wearable solutions. An RFID reader provides samples of the Received Signal Strength Indicator (RSSI) emitted by RFID tags in its range, that can converted

[1] http://glimpse.isti.cnr.it
[2] https://www.iso.org/standard/73906.html

through suitable temporal filtering into readings of the presence (or not) of the object or person to which the tag is attached. Using multiple antennas and bi- and tri-lateration techniques (see e.g. [13]), estimates of the position of the tag can be inferred. Such knowledge permits to enable spatio-temporal reasoning on the positions of the tags to perform HAR, either by studying the spatial relationships among the objects and subjects in the monitored environment at a given time or by performing trajectory analysis and clustering for activity classification [12]. Other sensor platforms ranging from binary presence sensors to sophisticated camera systems can be considered for collecting further data for performing HAR, which can then be fused together e.g. by using topological data analysis [5].

# 4 INFRASTRUCTURE

In Figure 1 the infrastructure proposed for the realization of the collected requirements is schematized. With reference to the picture, there are two kinds of roles: `Kids`, equipped with a passive RFID tag and `Power Users` (Teachers, Collaborators, Specialized personnel, etc) equipped with a digital bracelet able to receive notifications.

The kindergarten premises will be equipped with non-invasive technologies like: RFID lockers, Wi-Fi plugs and bulbs and RFID receivers for signal gathering. The infrastructure could be enriched also with additional low-cost COTS.

Considering the data flow, all the data, collected by the RFID antennas are sent through a Raspberry gateway to the `Position and Clustering Engine` components running on top of `tampe.isti.cnr.it`. These are in charge of processing the data in order to infer the position of tags in the kindergarten area and the spatial relationships among the kids and the personnel. The `Positioning Engine` uses an approach based on the RSSI of each RFID tags as measured by the receiving antennas in range. For each tag in the considered range, the output of the `Positioning Engine` is a soft location expressed as a probability density function. The `Clustering Engine` takes in input the soft locations and detects the presence of clusters of kids and the relative position of the personnel. Single kids isolated from clusters tutored by the personnel are automatically identified as well as other interactions and anomalous activities. The `Clustering Engine` and `Positioning and Clustering algorithms` components are running as docker component and can be deployed everywhere.

On top of `tampe.isti.cnr.it` there is also a small piece of software (a probe) in charge of packing up data relative to the position of the users and send it to the `Monitoring infrastructure` running on top of `glimpse-dev.isti.cnr.it`. The messages are sent through a message cloud by means of one or more brokers realized with ActiveMQ [2]. A rest interface for getting specific information about one or more users position is also provided by `tampe.isti.cnr.it`.

The node `glimpse-dev.isti.cnr.it`, is running on docker container. In case of emergency situations, the advantage gained by the combination of the two `Complex Event Processor` provide the possibility to override standard access control policies with emergency ones and enables the `Actuator` to execute suitable countermeasures [4]. More details in section4.1.

Finally, the `Actuator` component is in charge of communicating through REST interfaces with: (i) the kindergarten personnel digital bracelets for notifying violations or alarms; (ii) the non-invasive technologies of the building for enabling or inhibiting access/usage of the resources (doors, plugs..etc); (iii) the `Position and Clustering Engine` for getting `Personnel` position data in order to promptly alert the personnel also considering their proximity to the place where the violation occurred.

In the remaining of this section additional details about the monitoring infrastructure, the access control engine and the positioning and clustering algorithms are provided.

## 4.1 Monitoring infrastructure

The monitoring framework adopted in the proposed infrastructure is a extended customized version of the monitoring architecture presented in [9, 14–16, 24]. In our proposal the *glimpse-dev.isti.cnr.it* node (Figure 1) manages the complex event processing and the interactions with *Sensors*, *Actuators*, *Access Control Engine* and includes new features devoted to the usage and access control request generation.

The main monitoring components are:

- The *Rules Manager* component is in charge of orchestrating the rules generation starting from the templates stored within the component *Rule templates Repository* through the *Rules Generator* component.
- The *Rules Generator* is the component in charge of synthesizing the rules starting from the directives received by the *Rules Manager* by means of techniques based on generative programming approaches [6, 7, 19].
- The *Rules Templates Manager* is an additional internal repository storing the meta-rules enabling the run-time adaptation by means of generative procedures.
- The *CEP - Events* CEP (Complex Event Processing) Events is a rule engine realized by means of the Drools rule language [21]. It correlates the events, structured using JMS[29], flowing from *Sensors* and *Position and Clustering Engine* with the rules loaded by the *Rules Manager* component.
- The *CEP - Usage* is in charge of correlating complex events generated by the *CEP - Events* with the rules related to the usage of the resources, loaded by the *Rules Manager*.
- The *Rest Engine*, is the component in charge of communicating through REST [34] interfaces with the *Access Control Engine* in order to send/receive the *Access Control Engine* request/response.
- The *Response Dispatcher* through the *Message Broker (AMQ)*, realized by means of ActiveMQ [2], sends events to the actuators managed by the *Actuators gateway*.

The peculiarities of the proposed architecture is the use of a chain of two CEP entities, the *CEP - Events* and the *CEP - Usage*, for decoupling the activities concerning the management of the sensors from those more related to the administration of the resource usage and alarming situations. It lets a quick and high level updating of the general resource access and usage regulations and the planning of specific corrective actions in case of alarms or resource violations, leveraging from the specific sensor network on which they are

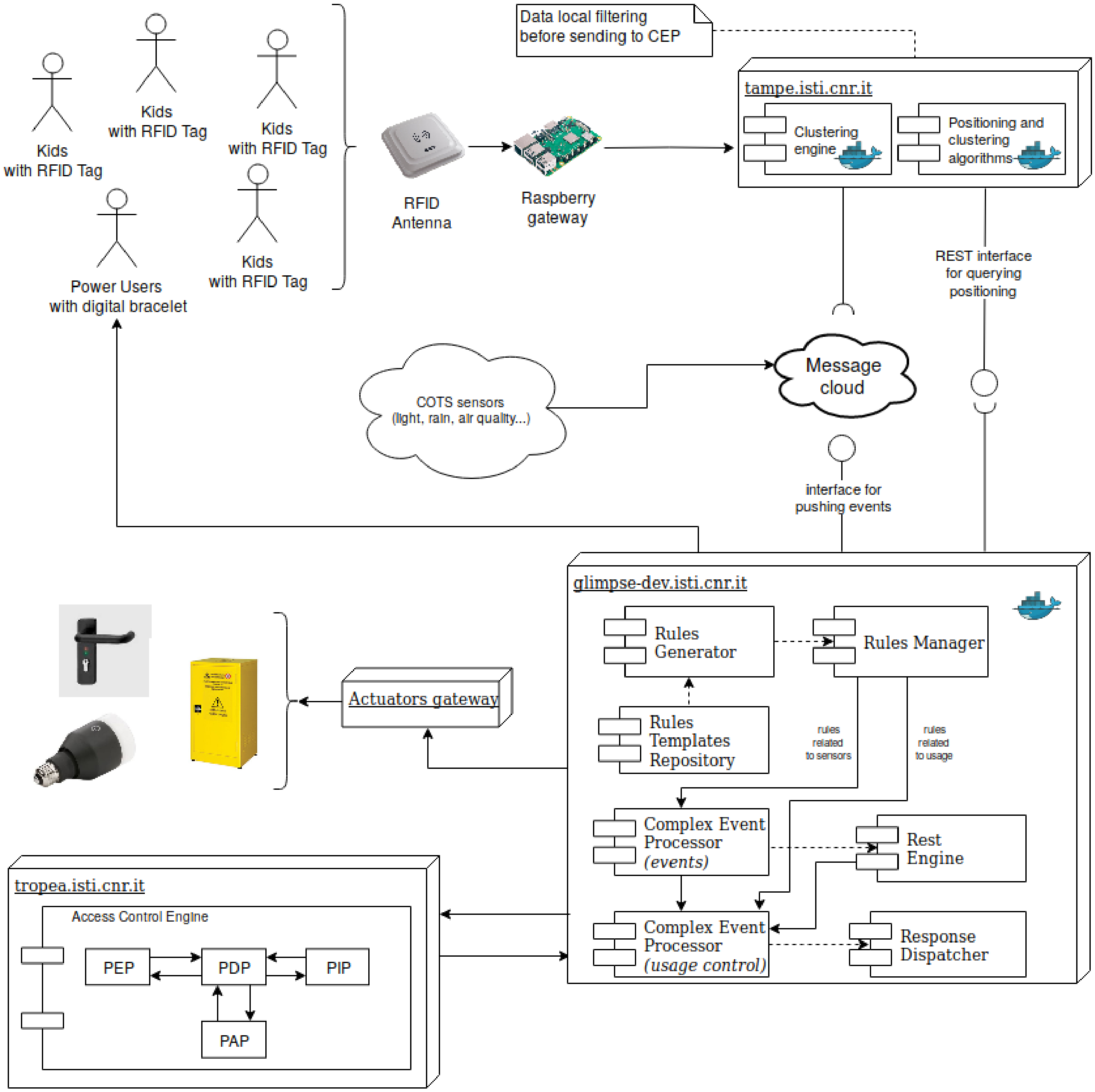


**Figure 1: Proposed infrastructure**

implemented. In order to improve the communication security, each component exposes a SSL certificate (self-signed certificates).

For space limitation, more details about the Monitoring Infrastructure, rules and meta-rules enactment can be found in [3, 4, 6].

## 4.2 Access Control Engine

This node manages the resource access by enforcing the XACML Policy defined by the Administrators. In particular, the *tropea.isti.cnr.it* (Figure 1) node contains *Access Control Engine* components that can be splitted in four modules that operates as follow: the *Policy Enforcement Point (PEP)*, usually embedded into an application system. It receives the access request in its native format from the *Glimpse: Monitoring Infrastructure*, constructs an XACML request and sends it to the *Policy Decision Point (PDP)*; it receives the PDP responses and forwards them to the *Glimpse: Monitoring Infrastructure* through its REST (REpresentational State Transfer) Interface called *REST Engine*. The *Policy Decision Point (PDP)* evaluates the policy with respect to the request and returns the response, including the authorization decision to the *PEP*. The *Policy Administration*

*Point (PAP)* is the component entity in charge of managing the policies and deploying them on the PDP; it receives the XACML access control policy by the *Management Interface*.

### 4.3 Positioning and clustering engines

This node processes the readings performed by RFID readers, detects the presence of targets in the monitored area, estimates their positions and performs spatial reasoning to identify cluster of persons. In particular, the *tampe.isti.cnr.it* (Figure 1) node contains the *Positioning and clustering algorithms* and the *Clustering engine*. The positioning algorithms are fed with the stream of readings performed by the available RFID antenna readers sent by Raspberry gateways. Each single reading consists of a quadruple (`TIMESTAMP, READER_ID, TAG_ID, RSSI`). A first module is regularly triggered at fixed time intervals to detect the presence of a tag within the range of a particular reader in a predefined detection time window $(T, T + \Delta T)$, in order to cut down the number of false positive and false negative readings. If a tag has been detected in the range of a particular reader in such detection time window, a robust estimate `RSSI_M` of the mean `RSSI` is computed averaging the received values for the quadruples having `TIMESTAMP` within $(T, T + \Delta T)$ weighted by their recency. The quadruple (`T, READER_ID, TAG_ID, RSSI_M`) is stored and used for further processing.

Tags that at a certain time were detected within the range of more than 2 readers are then positioned inside the environment by using elliptic trilateration [23]. For each of such tag, a soft positioning is produced by considering the intersection between the receiving ellipses of each reader where the tag has been detected with strenght `RSSI_M` as well as the structural boundaries of the premises (such as walls, doors and fences). For simplicity, every such region is approximated by its centroid and moment of inertia and converted into a Probability Density Function (PDF) using the corresponding Gaussian kernel.

Soft positioning is then used by performing spatial reasoning. The computed PDFs are used to estimate the density of occupation of each single point in the monitored area at every time. In such a way, tags that are distant from region occupied by others and that appears to be isulated can be promptly detected. Cluster analysis based on density estimation is also performed on the basis of the soft locations using a variant of Ordering Points To Identify the Clustering Structure (OPTICS) algorithm [31].

## 5 DISCUSSION AND CONCLUSION

In this paper we have presented a a dynamic and flexible infrastructure able to improve the safety and security of real world environments, with an extremely low impact on the maintenance and the updating effort. The proposal has been inspired by the collaboration with an Italian (Tuscany) kindergarten which provides a set of precise safety and security needs. In developing the infrastructure, important requirements have been considered such as privacy preservation and the unobtrusiveness of the installations.

Currently we are finalizing the verification and testing of the proposed solution, before to definitely installing it into the selected kindergartner school. In particular for assuring the feasibility and efficiency of the proposed solution, several lab simulations in a controlled environment are currently ongoing. These concern both functional and non-functional aspects such as the verification of the access and usage control policies and the components enforcing them through specific testing tools [11].

Attention has been also devoted to the assessment of the robustness of the monitoring infrastructure through a random generation of different kinds of events coming from different sources. More in detail, we simulated different stress peaks, transmitting 3 millions of events in 24h. A good quality of the service has been maintained, no information has been lost and the overall performance values have not been downgraded.

Density of the RFID readers for accurate positioning has appeared to be critical in order to support proper activity recognition. Indeed, while RFID technology is effective in providing binary presence information to be used by the monitoring infrastructure and acess control engine, a more global and uniform coverage is needed for pervasive activity analysis. For this reason, optimal antenna configurations are been sought, also considering the possibility to add other typologies of sensors.

Results collected during these simulations have provided encouraging results about the effectiveness of the approach in answering emerging safety needs of kindergarten. Further work will include a pilot experimentation in a kindergarten in Tuscany. On the basis of the pilot, it will be possible to design and evaluate more services for activity recognition based on positioning and clustering, so as to promptly identify not only events that might impact safety but also to collect more evidence that can help the personnel to gain more insight into the behaviour of kids.

## ACKNOWLEDGMENTS

This work has been partially funded by GAUSS, an Italian National Research project (MIUR, PRIN 2015) and by INTESA (FAR-FAS Regione Toscana 2014).

## REFERENCES

[1] Giuseppe Amato, Paolo Barsocchi, Fabrizio Falchi, Erina Ferro, Claudio Gennaro, Giuseppe Riccardo Leone, Davide Moroni, Ovidio Salvetti, and Claudio Vairo. 2018. Towards Multimodal Surveillance for Smart Building Security. *Proceedings* 2, 2 (2018). https://doi.org/10.3390/proceedings2020095

[2] Apache. 2018. Apache ActiveMQ. (2018). http://activemq.apache.org/.

[3] Paolo Barsocchi, Antonello Calabrò, Erina Ferro, Claudio Gennaro, Eda Marchetti, and Claudio Vairo. 2018. Boosting a Low-Cost Smart Home Environment with Usage and Access Control Rules. *Sensors* 18, 6 (2018), 1886.

[4] Paolo Barsocchi, Antonello Calabrò, Francesca Lonetti, Eda Marchetti, and Filippo Palumbo. 2018. Leveraging Smart Environments for Runtime Resources Management. In *Software Quality: Methods and Tools for Better Software and Systems - 10th International Conference, SWQD 2018, Vienna, Austria, January 16-19, 2018, Proceedings*. 171–190. https://doi.org/10.1007/978-3-319-71440-0_10

[5] Paolo Barsocchi, Pietro Cassará, Daniela Giorgi, Davide Moroni, and Maria Antonietta Pascali. 2018. Computational Topology to Monitor Human Occupancy. In *Multidisciplinary Digital Publishing Institute Proceedings*, Vol. 2. 99.

[6] Antonia Bertolino, Antonello Calabrò, and Guglielmo De Angelis. 2013. Adaptive SLA monitoring of service choreographies enacted on the Cloud. In *7th IEEE International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems, MESOCA 2013, Eindhoven, The Netherlands, September 23, 2013*. 92–101. https://doi.org/10.1109/MESOCA.2013.6632741

[7] Antonia Bertolino, Antonello Calabrò, and Guglielmo De Angelis. 2013. A Generative Approach for the Adaptive Monitoring of SLA in Service Choreographies. In *Web Engineering - 13th International Conference, ICWE 2013, Aalborg, Denmark, July 8-12, 2013. Proceedings*. 408–415.

[8] Antonia Bertolino, Antonello Calabrò, Francesca Lonetti, and Eda Marchetti. 2016. Towards Business Process Execution Adequacy Criteria. In *8th SWQD 2016, Vienna, Austria, January 18-21, 2016, Proceedings*. 37–48.

[9] Antonia Bertolino, Antonello Calabrò, Francesca Lonetti, Antinisca Di Marco, and Antonino Sabetta. 2011. Towards a Model-Driven Infrastructure for Runtime Monitoring. In *Software Engineering for Resilient Systems - Third International Workshop, SERENE 2011, Geneva, Switzerland, September 29-30, 2011. Proceedings.* 130–144.

[10] Antonia Bertolino, Said Daoudagh, Donia El Kateb, Christopher Henard, Yves Le Traon, Francesca Lonetti, Eda Marchetti, Tejeddine Mouelhi, and Mike Papadakis. 2015. Similarity testing for access control. *Information & Software Technology* 58 (2015), 355–372.

[11] Antonia Bertolino, Said Daoudagh, Francesca Lonetti, Eda Marchetti, Fabio Martinelli, and Paolo Mori. 2014. Testing of PolPA-based Usage Control Systems. *Software Quality Journal* 22, 2 (June 2014), 241–271. https://doi.org/10.1007/s11219-013-9216-0

[12] Jiang Bian, Dayong Tian, Yuanyan Tang, and Dacheng Tao. 2018. A survey on trajectory clustering analysis. *arXiv preprint arXiv:1802.06971* (2018).

[13] Jean-Sébastien Bilodeau, Abdenour Bouzouane, Bruno Bouchard, and Sebastien Gaboury. 2017. An experimental comparative study of RSSI-based positioning algorithms for passive RFID localization in smart environments. *Journal of Ambient Intelligence and Humanized Computing* (2017), 1–17.

[14] Antonello Calabrò, Francesca Lonetti, and Eda Marchetti. 2015. KPI Evaluation of the Business Process Execution through Event Monitoring Activity. In *ES 2015, Basel,Switzerland, October 14-15, 2015.* 169–176.

[15] Antonello Calabrò, Francesca Lonetti, and Eda Marchetti. 2015. Monitoring of Business Process Execution Based on Performance Indicators. In *41st,EUROMICRO-SEAA 2015, Madeira, Portugal, August 26-28, 2015.* 255–258.

[16] Antonello Calabrò, Francesca Lonetti, and Eda Marchetti. 2017. Access Control Policy Coverage Assessment Through Monitoring. In *Computer Safety, Reliability, and Security - SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings.* 373–383. https://doi.org/10.1007/978-3-319-66284-8_31

[17] Antonello Calabrò, Francesca Lonetti, Eda Marchetti, and Giorgio Oronzo Spagnolo. 2016. Enhancing Business Process Performance Analysis through Coverage-Based Monitoring. In *10th QUATIC 2016, Lisbon, Portugal, September 6-9, 2016.* 35–43.

[18] Pamela Carvallo, Ana R. Cavalli, Wissam Mallouli, and Erkuden Rios. 2017. Multi-cloud Applications Security Monitoring. In *12th GPC 2017, Cetara, Italy, May 11-14.* 748–758.

[19] Krzysztof Czarnecki and Ulrich W. Eisenecker. 2000. *Generative programming - methods, tools and applications.* Addison-Wesley. I–XXVI, 1–832 pages.

[20] Said Daoudagh, Francesca Lonetti, and Eda Marchetti. [n. d.]. Assessment of Access Control Systems Using Mutation Testing. In *TELERISE 2015, Florence, Italy, May 18, 2015.* 8–13.

[21] JBoss Drools. [n. d.]. Drools Fusion: Complex Event Processor. ([n. d.]). http://www.jboss.org/drools/drools-fusion.html.

[22] Dany Fortin-Simard, Jean-Sébastien Bilodeau, Kevin Bouchard, Sebastien Gaboury, Bruno Bouchard, and Abdenour Bouzouane. 2015. Exploiting passive RFID technology for activity recognition in smart homes. *IEEE Intelligent Systems* 30, 4 (2015), 7–15.

[23] Dany Fortin-Simard, Kevin Bouchard, Sebastien Gaboury, Bruno Bouchard, and Abdenour Bouzouane. 2012. Accurate passive RFID localization system for smart homes. In *Networked Embedded Systems for Every Application (NESEA), 2012 IEEE 3rd International Conference on.* IEEE, 1–8.

[24] Amira Ben Hamida, Antonia Bertolino, Antonello Calabrò, Guglielmo De Angelis, Nelson Lago, and Julien Lesbegueries. 2012. Monitoring Service Choreographies from Multiple Sources. In *Software Engineering for Resilient Systems - 4th International Workshop, SERENE 2012, Pisa, Italy, September 27-28, 2012. Proceedings.* 134–149. https://doi.org/10.1007/978-3-642-33176-3_10

[25] Cory Hekimian-Williams, Brandon Grant, Xiuwen Liu, Zhenghao Zhang, and Piyush Kumar. 2010. Accurate localization of RFID tags using phase difference. In *RFID, 2010 IEEE International Conference on.* IEEE, 89–96.

[26] Francesca Lonetti and Eda Marchetti. 2018. Issues and Challenges of Access Control in the Cloud. In *Proceedings of the 14th International Conference on Web Information Systems and Technologies, WEBIST 2018, Seville, Spain, September 18-20, 2018.* 261–268. https://doi.org/10.5220/0006948702610268

[27] Pavel V Nikitin, Rene Martinez, Shashi Ramamurthy, Hunter Leland, Gary Spiess, and KVS Rao. 2010. Phase based spatial identification of UHF RFID tags. In *RFID, 2010 IEEE International Conference on.* IEEE, 102–109.

[28] OASIS. 2013. eXtensible Access Control Markup Language (XACML) Version 3.0. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html. (January 2013).

[29] Oracle. 2016. *Java Message Service Documentation.* Technical Report. http://www.oracle.com/technetwork/java/docs-136352.html.

[30] Regione Toscana. 2018. Prima infanzia: un Protocollo per prevenire il rischio abbandono bambini in auto. (2018). http://www.consiglio.regione.toscana.it/ufficio-stampa/comunicati/comunicati_view?idc=0&id=26490 In Italian.

[31] Glory H Shah, CK Bhensdadia, and Amit P Ganatra. 2012. An empirical evaluation of density-based clustering techniques. *International Journal of Soft Computing and Engineering (IJSCE) ISSN* 22312307 (2012), 216–223.

[32] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production* 140 (2017), 1454 – 1464. https://doi.org/10.1016/j.jclepro.2016.10.006

[33] Moritz Tenorth, Jan Bandouch, and Michael Beetz. 2009. The TUM kitchen data set of everyday manipulation activities for motion tracking and action recognition. In *Computer Vision Workshops (ICCV Workshops), 2009 IEEE 12th International Conference on.* IEEE, 1089–1096.

[34] Erik Wilde and Cesare Pautasso (Eds.). 2011. *REST: From Research to Practice.* Springer. https://doi.org/10.1007/978-1-4419-8303-9