10

CARS-AD Project: Context-Aware Recommender System for Authentication Decision in Pervasive and Mobile Environments

João Carlos Damasceno Lima[1,2], Cristiano Cortez da Rocha[3], Iara Augustin[2] and Mário Antônio Ribeiro Dantas[1]
[1]*Federal University of Santa Catarina*
[2]*Federal University of Santa Maria*
[3]*MobilEasy Technologies Ltda*
Brazil

1. Introduction

Recommender Systems (RS) emerged as an independent research area in the mid 90s, and they have been proved in the recent years to be a valuable approach for coping with the information overload problem (Ricci, 2011). In general, recommendation systems manage the overload of information by helping a user to choose among an overwhelming number of possibilities. In another point of view, we argue that the underlying concepts of Context-Aware Recommendation Systems are also useful to build supporting software (infra-structure) for mobile, pervasive and ubiquitous environments, which have requirements such as invisibility of computing, follow-me semantics (Augustin et al., 2006), context-awareness, adaptation, user-centric personalization, everyday human activities.

A pervasive environment is characterized by a richness of contexts in which users, devices and agents are mobile in several places and with several entities, including services, applications and resources. These elements can be available or not in a particular time and space. In fact, information regarding this time-space scenario can be used to develop a behavioral pattern of an entity in several contexts (Munoz-Organero et al., 2010).

To achieve ubiquity, the support system, which runs the environment management, must be designed to find the right balance between the user individuality and the system proactivity. In mobile and pervasive computing, we consider that the user's tasks must be personalized, while functionalities associated with security must be designed proactively. In mobile environment, the user moves constantly and wants to maintain access and to continue with the activity that he was performing (follow-me semantics). While traveling, the user can be served by different context (networks, systems, resources), which require authentication services periodically. Thus, proactive support system must know when to perform the authentication so implicitly or explicitly, seeking to reduce the user interference. We propose adopting a Context-Aware Recommender System (CARS) to help in this decision making process.

On the other hand, it is known that mobile devices can be easily lost, stolen, or used by several users, enabling sensitive information to become inappropriately available and could be stolen or broadcasted without permission. To avoid this situation, there is the need to adopt an authentication process, given that standard security policies allow that a second form of user validation can be used to complement the traditional alphanumeric passwords.

In pervasive computing, in which the majority of mobile devices has a reduced size, users face difficulties on providing (safe) passwords with too many characters. Considering that the pervasive space is rich in additional information, captured by sensors such as location, time, temperature, security camera images, which compose the environmental context. Therefore, it is possible to use this information, associated with the user behavior as a component of the authentication process. The challenge of this solution lies on the complexity of modeling the individual behavior, as there is the need to develop models to deal with different user behavior.

To address this issue, we present a user behavioral model based on activities, environmental contexts, and user profile. These three elements form a tri-dimensional matrix of a CARS to the authentication in a pervasive system. We also will discuss the processes of (i) content-based filtering, (ii) collaborative filtering and (iii) hybrid filtering. A relevant factor of the behavioral model is the spatial-temporal modeling, which allows us to compute the conditional probability of the occurrence of a given activity. This factor allows to consolidate user implicit authentications in the pervasive space or to launch a challenge question to determine the user authenticity.

2. Implicit authentication

2.1 Motivation and proposal

With the popularization of mobile devices (smartphones and tablets), there is a gradual user migration to the use of pervasive computing environments. The most common use of such devices is the storage and the retrieval of information that is relevant to the users, such as financial services, social networks, electronic messages, and e-commerce.

However mobile devices add disadvantages regarding the safety and privacy of information that is stored. Now new security mechanisms should be concerned about the loss of the devices and where they are being used, since it can be easily lost, stolen or used by multiple users, allowing confidential information may be used inappropriately.

The standard security policies allow the use of a second alternative for user validation that can be used to complement the traditional alphanumeric passwords and minimize the disadvantages of loss of information in mobile devices. The password-based authentication has the advantage of being simple to implement and use few resources (no additional hardware is usually needed). However, usual password discovery methods (phishing, keyloggers, and social engineering) has been successfully applied in breaking many passwords.

The use of an additional validation as part of the authentication provides a more secure process. There are several services (e.g. google authenticator) that already implement it, but they still have problems regarding usability and cost. The choice of enterprises for the use of SecureID tokens that are displayed by auxiliary devices and have characteristics related

to desktop-based computing, where information is restricted to safe environments (business and home) are very different from the pervasive environment where mobile devices not have these limiting safety.

The implicit authentication is an approach that uses observations of user behavior for authentication. Since people are creatures of habits - a person goes to work in the morning, perhaps with a stop at the coffee shop, but almost always using the same route. Once at work, she might remain in the general vicinity of her office building until lunch time. In the afternoon, perhaps she calls home and picks up her child from school. In the evening, she goes home. Throughout the day, she checks her various email accounts. Perhaps she also uses online banking and sometimes relies on her smartphone for access away from home. Weekly visits to the grocery store, regular calls to family members, etc. are all rich information that could be gathered and recorded almost entirely using smartphones. (Shi et al., 2011).

With the migration of users to pervasive computing, mobile devices begin to collect the information produced by daily user activity: user schedule, calls users, messages, and add additional data (eg time and location) in the information produced. This set of data and information that is collected daily defines a profile that woks as a reliable criterion for authenticating users.

According to Shi et al. (2011) the implicit authentication is able to: i) act as a second factor for authentication passwords and supplements for greater assurance of a profitable and easy to use, ii) work as the primary authentication method to completely replace passwords, and iii) provide additional security for financial transactions such as credit card purchases, acting as an indicator of fraud. We note that in the latter scenario, the act of making the transaction does not require any user action on the device.

2.2 Research in authentication for pervasive environment

We present a set of related approaches for context-aware authentication with the goal of comparing this work with the state-of-art in this area:

1. **Implicit Authentication with User Behavior Learning** - Shi et al. (2011) propose an implicit authentication mechanism through user behavior learning. The mechanism focuses on the use of mobile devices (PDAs) and presents a technique to determine the computation of an authentication score based on the user recent activities. To compute such score, the positive (habitual) events are identified; the score increases whenever an habitual event is observed, as buying coffee always in the same store, in a similar period of time, daily. The score decreases when negative (sporadic) events are detected, such as the call to an unknown number or sudden changes of expected places (an event associated with the theft or the inappropriate use of the device). The passage of time is treated as a negative event in which the scores gradually decrease. When the score reaches a lower limit, the user must authenticate explicitly, inserting a code. The successfully authentication will boost the score. The limits can vary for different applications, depending on security needs.
2. **Transaction Level Authentication** - Sathish Babu & Venkataram (2009) present an authentication schema to mobile transactions, named TBAS (Transaction-Based Authentication Scheme), which aims to classify user-operated transactions in the application level in mobile computing environments. Through this classification, the

system (i) is able to interfere and to analyze user behavior using cognitive (intelligent) agents, and (ii) can determine the security level needed, predicting, thus, the cost associated with the authentication process delay, given the application of cryptography algorithms. TBAS uses two kinds of cognitive agents: a mobile cognitive agent (MCA) and a static cognitive agent (SCA). In this approach, the SCA creates the MCA and sends this mobile cognitive agent to the mobile device. This procedure is done while the user is being authenticated.

3. **Authentication based on Activity Recognition** - Hassan et al. (2008) propose an activity-based security mechanism that aims to help in the user activities in ubiquitous environments. Such mechanism is composed of an authentication system based on the human identification of images (Jameel et al., 2006) of an activity oriented access control module. The proposed model supports several kinds of devices, including mobile devices (PDAs), laptops, and desktops. In the mechanism, the activity recognition manager (ARM) provides information regarding user activity to the authorization system, through low level data collection related to the activity and the production of high-level contextual information. This way, the ARM can conduct the process of reasoning about user actions.
4. **Context-based Authentication** - Corradi et al. (2004) propose a security middleware, named UbiCOSM (Ubiquitous Context-Based Security Middleware). Such approach adopts the context as a basic concept to the specification and the execution of security policies. Therefore, the permissions are associated directly to the contexts, instead of being associated with the identities and with the user roles. The information about contexts and resources is provided by the CARMEN middleware (Bellavista et al., 2003). The UbiCOSM access control manager works with two context classifications: physical and logical context. Physical contexts identify physical spaces delimited by specific geographical coordinates. This way, a user operates in a given physical context, depending on his current location; thus, the user can only belong to a physical context. Additionally, the physical contexts define specific boundaries to the access control manager, as each physical context has references to the resources which must be protected.

2.2.1 Analysis of the approaches

In this section, we conduct an analysis of the previously presented approaches considering the essential requirements to the authentication on pervasive environments. As shown on Table 1, the majority of the approaches present a weak contextual modeling, as they consider only aspects regarding the characteristics of the devices used by the user and his spatial context. In this way, such systems have an incomplete vision of the scenario, hurting the decision making process. The proposal 1 works with a limited spatial-temporal model, because time is modeled though a simplification that does not allow the inference of weekly or biweekly activities (for example, on every Saturday the user plays tennis with new adversaries and needs to contact them to schedule the game).

A small part of these analyzed approaches presents some mechanism to dynamically analyze and model user behavior. The proposals presented on 3 and on 4 are static, i.e. they do not offer mechanisms that the system can use to dynamically aggregate the knowledge and the skills acquired by the user during his interactions with the system. In 3, despite the proposition of an activity recognition mechanism, the user must explicitly inform the activity that he is executing. In 4, although a proposal for using profiles to determine the user

Characteristics	Implicit AuthZ with User Behavior Learning	Transaction Level AuthZ	AuthZ based on Activity Recognition	Context-based AuthZ
Contextual Model	Spatial and Temporal	Spatial	Spatial	Spatial
Behavioral Model	Dynamic Profile through scores	Cognitive Agents	Explicit	Static Profile
Atomicity and Dinamicity	Yes	Yes	No	No
Flexibility	No	Yes	No	Yes
Privacy	Yes	No	No	Yes
Authentication control	Client	Client	Client	Server

Table 1. Approaches for Context-Aware Authentication (AuthZ)

permissions is presented, the user must explicitly determine which activities he intends to perform on the system.

As the battery life time is a major usability concern in mobile devices (Rahmati & Zhong, 2009), it is desirable that the authentication mechanisms take into account aspects related to the consumption of computational resources in an intelligent way, when they execute their security procedures. Thus, the validation of the proposal in 2 is based on the categorization of mobile transactions, considering the security level needed to perform such operations. Although there is this cost categorization associated with the authentication process, such categorization is only used to determine the impact of the delay associated to the cryptography algorithm used, and to define which will be the authentication methods (challenges) used. On the other hand, in 1 and in 3, despite the authors cite that the proposed architecture is lightweight, no experiments or additional details are presented to describe how such architecture deals with the mobile devices energy constraints. The architectures having the authentication control in the server do not interfere in the applications and in the mobile device operational system, making its dissemination easier and reducing battery consumption.

The possibility of managing the security policies by the users has become steadily more important in the design of security solutions that aim to align the usability to the capacity of maintaining acceptable levels of integrity, reliability and availability in mobile applications (Toninelli et al., 2009). However, security and usability have been rarely integrated in a satisfactory way in the design and in the development of mobile systems (Hong et al., 2007).

Therefore, we aimed to analyze the proposed approaches in terms of privacy and flexibility of authentication mechanisms and policies. In 2 and 4 it is presented another authentication mechanism. In 2, different challenges are provided to the user in order to ensure his identity, depending on the security level needed by the requested transaction and the user behavioral anomaly level. On the other hand, in 4, the user defines its preferences through profiles, which are used by the system in the user authentication and authorization processes. In 1 it is not presented a validation mechanism nor the generation of challenges, the authors inform that this can be performed by the applications, in different levels. In 3, the proposed architecture

provides only one authentication way for the user, which is the process of identifying images proposed before by the same authors in Jameel et al. (2006).

3. Context-aware recommendation systems

We adopt Burke's taxonomy (Burke, 2007) to provide an overview of the different types of RS, which has become a classical way of distinguishing between recommender systems and referring to them. He distinguishes six different classes of recommendation approaches:

- Content-based filtering: recommends items that are similar to the ones that the user liked in the past;
- Collaborative filtering: recommends to the active user the items that other users with similar tastes liked in the past;
- Demographic: recommends items based on the user demographic profile. The assumption is that different recommendations should be generated for different demographic niches;
- Knowledge-based: recommends items based on specific domain knowledge about how certain item features meet users needs and preferences and, ultimately, how the item is useful for the user. Notable knowledge-based recommender systems are case-based or constraint-based systems;
- Community-based: recommends items based on the preferences of the user's friends. This technique follows the epigram "Tell me who your friends are, and I will tell you who you are".
- Hybrid recommender systems: based on the combination of the above mentioned techniques. A hybrid system combining techniques A and B tries to use the advantages of A to fix the disadvantages of B.

Many resources in ubiquitous environments can be available and the users want to share them. However, the situations and the preferences of users are different, even if the users are in the same environment. Therefore, we want to have a proper RS for sharing the available resources. These and other possible models for recommendation systems may be adequate for current uses, but perhaps not for future ubiquitous computing.

Ubiquitous computing systems with knowledge of more than locations - say, the tools a person is using - could greatly benefit that person by recommending others who have expertise with those tools. Although it may be impossible to optimally anticipate the needs of each user at any place at any time, ubiquitous computing will enable such systems to help people to cope with an expanding array of choices (McDonald, 2003).

Therefore, the recommendation approach, which proved to be successful to PC users, cannot be straightforwardly applied for mobile users due to the obstacles that are typically present in mobile usage environments, such as: limitation of mobile devices and wireless networks, impact from external environment, and behavior characteristics of mobile users (Ricci et al., 2011).

3.1 Mobile recommender systems

Mobile recommendation systems are systems that provide assistance to the users as they face decisions "on the go", or, in other words, as they move into new, unknown environments.

Examples include consumers making purchasing decisions in retail stores, or students having ad hoc meetings to decide on assignment workload van der Heijden et al. (2005).

As mobile devices are popular and are becoming a primary platform for information access and business applications, recommendation techniques can increase the usability of mobile and pervasive applications, providing more focused content and tailoring the information to the needs of the user. Ricci et al. (2011) reviews the major techniques that have been proposed in the last years and illustrates the supported functions by Mobile Recommender Systems (MRS).

As we have observed, in the most mobile recommender systems, the recommendation target is Internet content, multimedia (videos, music, films, books), product promotions, tourist experiences and traffic information. The data sources are users and Internet transactions. For those MRS that add context-awareness, the more commonly context information is the user location (location-aware applications).

Context-based applications pro-actively retrieve content of interest based on the user current task or his profile. Roberts et al. (2008) describe the implementation of a mobile recommender system for leisure activities, named Magitti, which was built for commercial deployment under stringent scalability requirements. Ricci & Nguyen (2007) exploit the recommendation by proposal and critiquing techniques in the MobyRek system, that has been designed to run on a mobile phone with limited user input. It searches functionality, lets the user to formulate both must and wish conditions, and returns a ranked product list. The result of an empirical evaluation of the system shows that it can effectively support product selection processes in a user friendly manner.

Although the systems target different needs, they share a common design: the system collects different types of (contextual) information characterizing the user (such as preferences, activities, location, device) and uses it to filter and to rank relevant content items and trying to anticipate the needs or the products in which the user may be interested, while he is moving himself.

3.2 Pervasive security and recommender systems

Security problems in RSs are addressed with two goals in mind: (i) to control malicious users (Ray & Mahanti, 2009), and (ii) to ensure user privacy (Zhan et al., 2010). Thus, we are interested in recommender systems for security in mobile and pervasive environment.

The goal of research in Mobile, Pervasive and Ubiquitous Security is to understand and to analyze the new security and privacy issues arising from the high mobility, context-awareness and invisibility of these systems, that begin to be available, and to propose solutions to safely deploy applications, services and appliances anywhere, anytime, on any device, on any network, running on background.

According to Johnson (2009), pervasive environments need context-aware security mechanisms because the context changes allow these mechanisms to be adjusted on the basis of the current situation. Therefore, the mechanisms using this approach are able to effectively deal with traditional security systems limitations that are designed for static environments. Nevertheless, most of the research regarding the development of context-aware authentication systems is limited or vague (Ricci & Nguyen, 2007). Usually, these systems only consider traditional aspects, e.g. the user location. As a result, they provide an abstract and weak view

of a certain situation. Thus, the decisions made within these systems are poor, because they are based on an incomplete scenario.

Few works address issues about pervasive security and context-aware recommender systems. Kim et al. (2009) propose a new authenticated key management method, called 3DE_sec, to minimize the load of the authenticator, even with mobile nodes or the insertion or deletion of nodes. The proposed system generates personalized profiles (using inference of data captured from RFID systems) containing user preference and various lifestyles and uses of recommendation service, it updates based on past history and currently available services. The system architecture is composed by profile collector, profile aggregator, collector resolver, and service manager. The evaluation results indicate that the method can set a shared key faster and more securely using a multiple-key ring assigned to each node before deployment secure and efficient recommendation service in RFID.

Romero-Mariona et al. (2008) propose a recommendation system for helping developers to choose among security requirements approaches. As part of their ongoing research, they identified ten key characteristics (elicitation support, level of customer involvement, unambiguity level, completeness level, clarity level, traceability level, overall security level, update difficult of the security specifications, automation support level, scalability level) that are used to recommend which of the 12 approaches surveyed better suits a specific project. In a different direction of these approaches, we aim to recognize the suitable moment to renew the user authentication automatically or to ask the user for information to explicitly authenticate him.

4. CARS-AD architecture

The pervasive space exists in an environment where situations or contexts surround the user. In particular, these contexts are relevant for the adaptive process of services and information offered to the user through context-aware applications (Dey, 2001). Therefore, the situations that a user can experienced in a pervasive environment are personal, complicating the representation of the user's context and its parameters.

We analyzed the resources offered by mobile devices to identify contexts and properties relevant to the users and their behaviors in pervasive environments. Consequently, the following authentication-relevant contexts were identified (Uden, 2007):

- Operational context: describes the goals, tasks and activities of the user;
- Interpersonal context: describes the social aspects of the user, such as the relationships and communication channels between the user and his community;
- Spatial context: considers attributes regarding the use's location;
- Environmental context: captures the situations surrounding the user, such as services, people and information accessed by the user.

The temporal property was integrated with the context model to improve the decision-making process (Uden, 2007). Specifically, this model considers historical data, such as the user learning capacity, including the acquisition of skills and knowledge, and the evolution of activities and behaviors (see Figure 1).

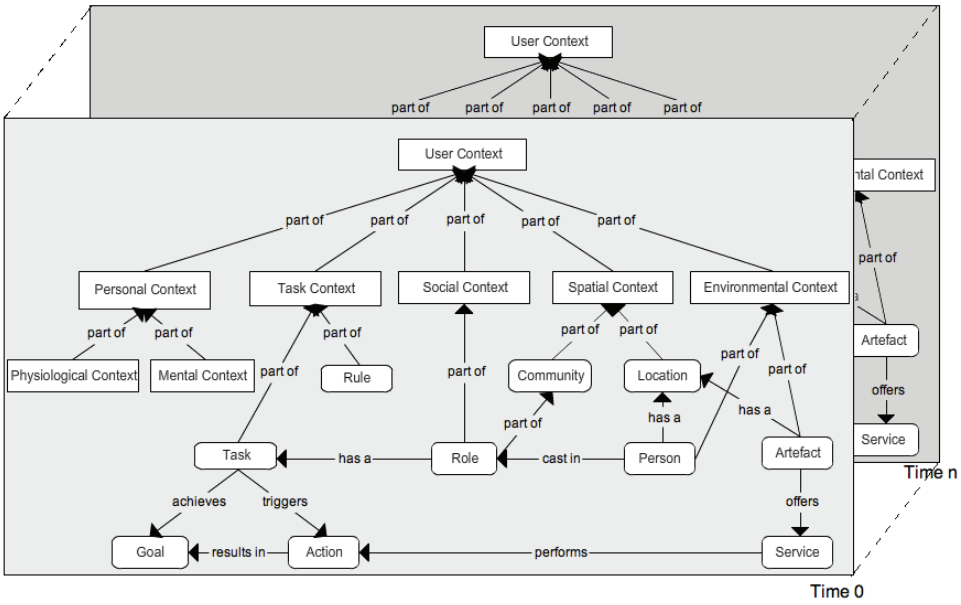

Fig. 1. Contextual Modeling adapted from Cassens & Kofod-Petersen (2006)

4.1 Context model

The proposed context-aware authentication architecture attempts to use resources that are commonly found in mobile devices, such as smartphones, to monitor the behavior of the user in different situations and events where the user is immersed in the pervasive space. These devices are considered as special artefacts that are commonly used by the users to perform tasks and activities, and consequently, to achieve their goals in mobile environments (Uden, 2007). Specifically, these devices offer access to resources such as (Lima et al., 2010):

- User calls: provide information considering the interpersonal context, which is comprised by the community in which the user is inserted and the environmental context, that is regarding the people surrounding the user;
- User schedule: one of the richest resources in terms of context, as it provides information about the relationship between the user and the members of his community. It can help to determine the user location, the people surrounding him and the activities that the user wants to execute in a given time frame;
- GPS: provides information regarding the user spatial situation;
- Device battery level: can indicate the interaction form between the user and the environment, as well as the intensity of such interaction;
- User applications: provide information related to the operational and the environmental context: in particular, such applications indicate which artifacts the user needs to achieve his goals through the performed activities;

- Sensors: can provide information regarding the environment, visual authentication and other information that define the environment in which the user is interacting with the authentication system.

The architecture has additional modules that allow the recommendation system implementation, described as follows:

- Group profile: a pre-defined profile which considers the standard characteristics of the agents (users, applications, use sessions and environment) which interact with the system.
- Explicit profile: created during the first interaction of the system with the user through an interactive interface; contains the events made explicit by the user and extracted from their contacts and the personal agenda stored in the mobile device. This profile can be customized and synchronized at any time;
- Implicit profile: created through the processing of user events and his explicit profile; it has the relevant information about frequent events, the actions taken by the users, and their spatial-temporal characteristics.
- Recommendation filter: an adaptive filter according to the approach (based in content, collaborative, or hybrid) which uses the vector space model to compute the information relevance, and uses a formal treatment through the vectors to compute the similarity between the profiles being analyzed.

The context-aware authentication architecture is illustrated in Figure 2. The context subsystem, or, user context, is responsible for capturing all the situations that determine the occurrence of a new event through the resources previously described. Thus, this subsystem sends the event description e_i to the belief analyzer subsystem.

Belief Analyzer: The Belief Analyzer is responsible for the definition of behaviors or beliefs, as well as for the classification of events and the inference of behaviors through the activities, the stored profiles, and the perceived and registered events. The behaviors are analyzed by similarity or probabilistically in order to define new occurrences and to determine the attitude to be adopted by the system, as well as the actions that must be taken in a new occurrence. The beliefs database works with a knowledge repository (storing beliefs and profiles).

Recommendation Filter: The Recommendation Filter aims to determine the new implicit profiles, i.e. for each combination of an event with the explicit profile, a new orthogonal vector is determined. This vector is used to compute the similarity: if the similarity degree is higher than a defined threshold, the profile is considered relevant and, then, it will be stored in the system as a new implicit profile, with a weight equals to the similarity degree.

Probability Analyzer: The subsystem which analyzes probabilities (Probability Analyzer) is responsible for the user categorization, based on the conditional probabilities of his behavior. This classification is divided in three categories: normal, suspect and abnormal.

Challenger: The subsystem determines how the user will be questioned in order to prove his identity on the system, based on the categorization made by the Probability Analyzer and on the authentication level needed for the desired operation. The response to the challenge proposed to the user is, then, stored for future queries.

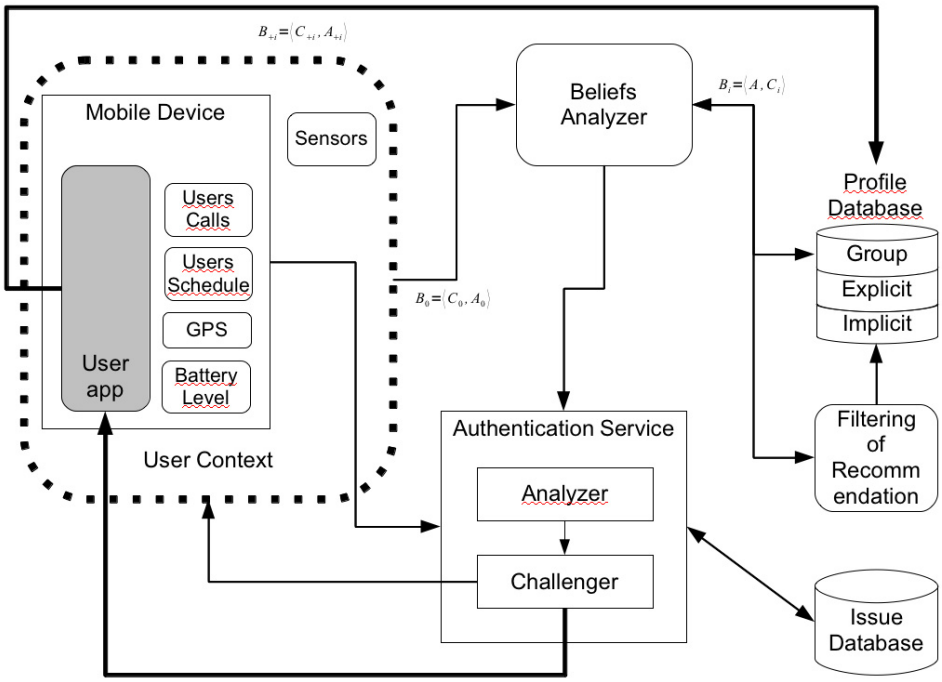

Fig. 2. Proposed Architecture

4.2 Behavioral model

Given the habitual tendencies of individuals, time correlations are important for the determination of successive events (Rocha, 2010). Hence, the prediction of events defines the actions and behaviors that the user will adopt. This work uses the following definitions to formally define the concepts of event and behavior:

- Event: situation of a given entity, in a given location, in a certain time space. An event can be determined as $E_i = \langle id_{entity}, situation_{entity} \rangle$
- Context: a set of events with relevant knowledge to the context definition of recommendation systems. Defined as $C_i = \langle time, location, E_1, E_2, E_3, E_4, .., E_n \rangle$
- Activity: set of actions for realization of a task, defined as $A_i = \langle a_1, a_2, a_3, a_4, ..., a_n \rangle$
- Behavior: the set of events or context related to an activity execution or set of actions (e.g. prescription for patients). It can be defined as $B_i = \langle A_i, C_i \rangle$

In the first moment we used the cosines of vectors to calculate the similarity between contexts and activities. However due to the diversity of domains that exist between the elements of each of these vectors was necessary normalization of values, similar case was reported in Su & Khoshgoftaar (2009). To solve this problem was adopted Pearson's correlation.

The similarity between two different contexts is established by the equivalence of events and it is determined by the possibility that activities in these contexts may occur again. The similarity between context is defined as

$$Sim(C_i, C_j) = \frac{C_i \times C_j}{|C_i| \times |C_j|} \tag{1}$$

When applying the normalization values through Pearson's Correlation Coefficient (PCC) in equation 1. The new similarity between contexts will be

$$PCCc_{i,j} = \frac{\sum_{u \in U} (c_{u,i} - \overline{c_i})(c_{u,j} - \overline{c_j})}{\sqrt{\sum_{u \in U} (c_{u,i} - \overline{c_i})^2} \sqrt{\sum_{u \in U} (c_{u,j} - \overline{c_j})^2}} \tag{2}$$

The equivalence between two activities can be determined by reusing actions or by the similarity between the activities. Can be defined as

$$Sim(A_i, A_j) = \frac{A_i \times A_j}{|A_i| \times |A_j|} \tag{3}$$

When applying the normalization values through Pearson's Correlation Coefficient in equation 3. The new similarity between activities will be

$$PCCa_{i,j} = \frac{\sum_{u \in U} (a_{u,i} - \overline{a_i})(a_{u,j} - \overline{a_j})}{\sqrt{\sum_{u \in U} (a_{u,i} - \overline{a_i})^2} \sqrt{\sum_{u \in U} (a_{u,j} - \overline{a_j})^2}} \tag{4}$$

The presented definitions represent the behavioral modeling and the way to compute the similarity between contexts and between activities. Using these definitions the processes of Recommendations System filtering are defined and characterized.

4.3 Spatio-temporal permutation model

The observed events in the execution of activities form a database for the process of detecting information clusters, which translates to the habits of users. These clusters can be classified into three broad categories: purely spatial, purely temporal or spatio-temporal. In purely spatial clusters, the occurrence is higher in some regions than it is in others, and purely temporal clusters feature the occurrence of events as being greater in a certain period than it is in others. Finally, spatio-temporal clusters occur when events are temporarily higher in certain regions than they are in others. Among the models used to predict events in a spatio-temporal context, we propose the use of spatio-temporal permutation, which allows the incorporation of covariate information found in other contexts within the pervasive space.

According to Kulldorff (2005), the spatio-temporal permutation model is based on three characteristics: i) detecting data clusters in space and time simultaneously; ii) working with only events or cases; and iii) applying the probabilistic model in a null hypothesis to conclude that the events follow a hypergeometric distribution.

Assuming the count of events e, in the timeline set in t, located in a region, z, with circular features according GPS coordinates, is defined as e_{zt}. The total number of observed events, E, and the total number of conditioned events, M_{zt}, are expressed by the following formulas:

$$E = \sum_{z}\sum_{t} e_{zt} \quad M_{zt} = \frac{1}{E}\Big(\sum_{z} E_{zt}\Big)\Big(\sum_{t} E_{zt}\Big)$$

The prediction of an event encompasses the following assumption: the conditional probability of an event $P(E_a)$, in the region z was observed at the time t_1 and t_2, defined in a particular cylinder a, which reflects a possible cluster; therefore, E_a has an average M_a and follows the hypergeometric distribution determined by the following function:

$$M_a = \sum_{(z,t)\,\in\, A} M_{zt} \tag{5}$$

$$P(E_a) = \begin{pmatrix} \sum\limits_{t\,\in\,(t_1 \vee t_2)}\ \sum\limits_{z\,\in\, A} E_{zt} \\ E_a \end{pmatrix} \frac{\begin{pmatrix} E & -\Big(\sum\limits_{t\,\in\,(t_1 \vee t_2)}\ \sum\limits_{z\,\in\, A} E_{zt}\Big) \\ \Big(\sum\limits_{t\,\in\,(t_1 \vee t_2)}\ \sum\limits_{z\,\in\, A} E_{zt}\Big) & -\ E_a \end{pmatrix}}{\begin{pmatrix} E \\ \sum\limits_{t\,\in\,(t_1 \vee t_2)}\ \sum\limits_{z\,\in\, A} E_{zt} \end{pmatrix}} \tag{6}$$

The SaTScan tool developed by Kulldorff (Kulldorff, 2005) is used to determine the regions of the clusters and the statistical significance is validated by the use of a Monte Carlo hypothesis test.

The conditional probability of the user $P(E_a)$ provides an estimation of the user's past and present activities. Thus, there are four cases that can occur: normal execution, abnormal execution, and two cases of suspicious execution. Normal execution entails the same activity in the same spatio-temporal context, and abnormal execution involves different activities in different spatio-temporal context.

The two cases of suspicious execution occur when the same activity is performed in a different spatio-temporal context or when different activities occur in the same spatio-temporal context. In the first case, the security-relevant context of the activity will define the authentication policies.

4.4 Filtering for recommendation system

In this project, we work with the development of 3 (three) recommendation filters:

Content-Based Filtering: The recommendation system uses the definitions of user behavior to establish their guidelines, if a particular activity in a temporal context was last conducted ($Time_0$ in Figure 1), there is a reasonable probability that this same activity can be executed again ($Time_{+1}$ in Figure 1). The temporal context that can be represented similarly to Oku et al. (2010):

$$\langle \underbrace{\ldots,(A_{-1},C_{-1})}_{B_{Past}}, \overbrace{(A_0,C_0)}^{B_{Present}}, \underbrace{(A_{+1},C_{+1}),\ldots}_{B_{Future}} \rangle \tag{7}$$

Collaborative Filtering: This filtering process uses the information from other behavior of users $\Big\langle \underbrace{(B_1 = (A_1, C_1))}_{User_1}, \overbrace{(B_2)}^{User_2}, \underbrace{(B_3)}_{User_3}, \dots \Big\rangle$ to predict the users being implicit authentication $\Big\langle \underbrace{(B_0 = (A_0, C_0))}_{User_{Predict}} \Big\rangle$. Therefore, the similarity can be applied to the user behavior. And can be defined as:

$$\begin{aligned} Sim(B_0, B_1) &= Sim\Big((A_0, C_0), (A_1, C_1)\Big) \\ &= Sim(A_0, A_1) \times Sim(C_0, C_1) \end{aligned} \tag{8}$$

$$\begin{aligned} Sim(B_0, B_2) &= Sim\Big((A_0, C_0), (A_2, C_2)\Big) \\ &= Sim(A_0, A_2) \times Sim(C_0, C_2) \end{aligned} \tag{9}$$

Hybrid Filtering: The proposed model uses a hybrid filtering which explores the space-time perspective to define clusters of events and user behaviors. It is performed to predict the need of authentication. Regarding the user knowledge base expansion, it uses a similarity vector to expand and to redefine the user profile.

5. Cases and results

5.1 Content-based filtering

The presented experimental results are related to the content-based filtering process. The data from testing and the content-based filtering process results are preliminary. They were collected using two mobile devices during two weeks, with a total of 96 events, which were contextualized through their location, device and the time of their occurrence. The case study will refer to the content based filtering as shown in Figure 3. The analysis was conducted through complete authentication cycles, as follows:

1. The behavior B_0 is captured in the mobile device producing the B_0 vector.
2. The event is analyzed through the content based filtering process, which uses a clustering algorithm similar to k-means, where the clusters are formed by devices and other information that compound the event. The average values of the events define the centroid of the cluster, shown in Figure 4. The centroids are calculated through a normal distribution and their values are updated every time the user needs to authenticate explicitly. Every new event is calculated the distance to the centroid, which will be called the rank of similarity.
3. The need to challenge the user is analyzed, based on the authentication level required by the application, rank of similarity and statistical information the centroid of clusters (represented by the Centroid $D1$ in Figure 4); and
4. if the authentication process is completed with success then the user behavior is stored in the profile database.

In content-based filtering, the clusters of devices are defined as parameters because:

- Mechanisms are used massively by the User to carry out their activities;

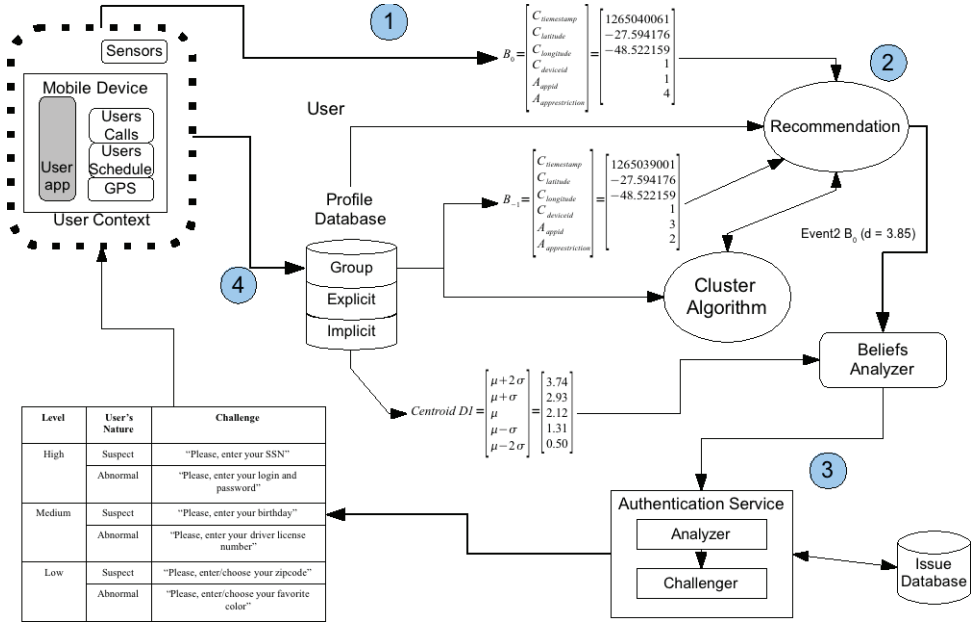

Fig. 3. Experimental Results to the Content Based Filtering

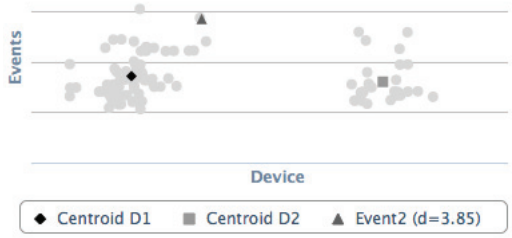

Fig. 4. Cluster of Devices

- Users work with a limited number of devices that enables the creation of statistical models for each user; and
- Filtering processes work with different parameters, which enables its completeness. The spatio-temporal parameters have already been evaluated in the hybrid filter, the focus in this filter is to study another parameter that incorporates the context of the user;

The authentication process begins with the first user interaction with the system. In this interaction, the user alphanumeric password is explicitly requested and the behavior vector B_0 is defined.

The authentication recommendation process starts being performed in the second user interaction. When the second interaction is requested, the behavior vector B_0 is redefined to B_{-1}, preserving previous user authentication information.

Level	User's Nature	Challenge
High	Suspect	"Please, enter your SSN"
	Abnormal	"Please, enter your login and password"
Medium	Suspect	"Please, enter your birthday"
	Abnormal	"Please, enter your driver license number"
Low	Suspect	"Please, enter/choose your zipcode"
	Abnormal	"Please, enter/choose your favorite color"

Table 2. Challenge for Authentication Level

In the second interaction, the request was done in the same mobile device, from the same location of the first interaction. However, such request was done to other application with different restrictions, represented by the B_0 vector in Figure 3.

The content based filtering does the execution of the cluster algorithm to determine the rank of similarity, which indicate if this application is being executed by the same user. In the case of *Event*2, shown in Figure 4, the rank of similarity is equal to 3.85, this value is calculated through the Euclidean distance between centroid $D1$ and the *Event*2. Thus, the user category is determined (normal, suspect, abnormal). We assumed the following definition:

- Normal user: the distance of the new event must be until one standard deviation from the centroid;
- Suspect user: the distance of the new event must be until two standard deviation from the centroid; and
- Abnormal user: values higher than the defined above.

Given the intervals defined above, there is the need of testing the user with the challenge corresponding to a abnormal user and to the authentication level required by the application (high level), as shown in the Table of Figure 3 and Table 2. When the user responds the challenge correctly, he is authenticated in the system, executes the desired operation and the requested event is inserted in the user profile, which contains the history of his interactions with the system.

5.2 Collaborative filtering

The presented experimental results are related to the collaborative filtering process. The data from testing and the collaborative filtering process results are preliminary. They were collected using three mobile devices during six weeks, with a total of 160 events, which were contextualized through their location, device and the time of their occurrence. The case study is related to the collaborative filtering as shown in Figure 5. The analysis was conducted through complete authentication cycles, as follows:

1. The behavior B_0 is captured in the mobile device producing the B_0 vector of the $User_0$.
2. The behavior B_0 is analyzed under the collaborative filtering process that uses Pearson's correlation coefficient to determine the rank of similarity between B_0 and the behaviors available in database of other users, represented generic by B_1 and B_2, shown in Figure 5.
3. The analysis of the need to challenge the user is based on the authentication level (defined on the Table 2) required by the application and rank of similarity (represented by the $PCC\ B_0$ in Figure 5); and

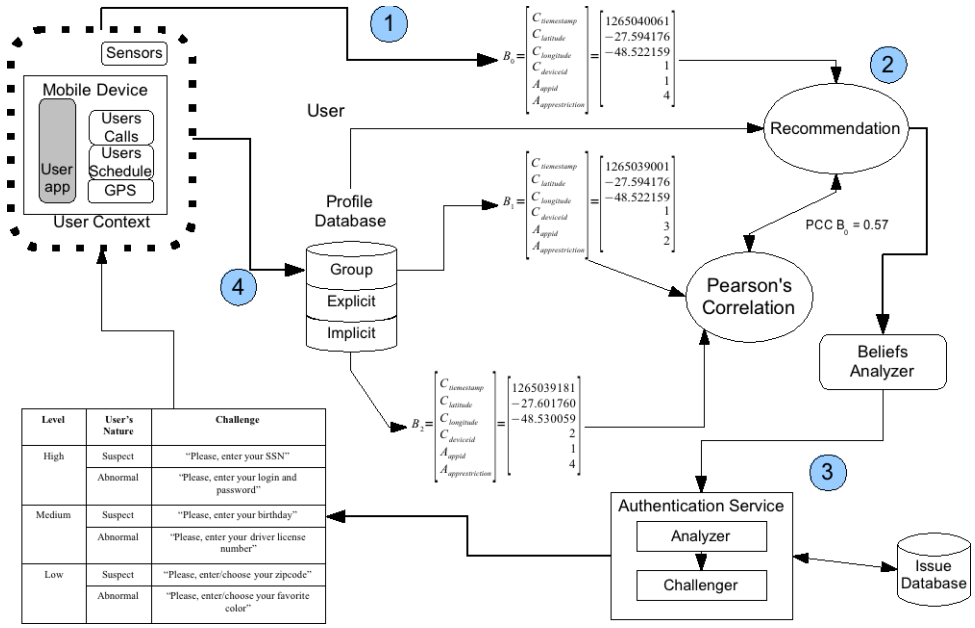

Fig. 5. Experimental Results related to the Collaborative Filtering

4. if the authentication process is accomplished with success then the new user behavior is stored in the profile database.

This filter aims to find other users who have a similar behavior (profile) to that of the User who is being authenticated. Thus, it is possible to determine that user behavior B_0 has similar behavior to that stored in database. The use of this filter requires that users decrease your privacy and allow their behaviors to serve as a basis for the definition of ranks of similarities (PCC).

The authentication process begins with the User performing the first authentication through an explicit process (typed password). The information collected in his first iteration are stored in the user profile. In the second interaction the system will try an implicit authentication using the Content-Based Filtering, in case the rank of similarity are below of the desirable level, the system performs Collaborative Filtering.

The Collaborative Filtering performs the search in a three dimensional matrix (*User x Context x Activities*) that formally is represented by: $R : U \; x \; C \; x \; A \rightarrow S$, where S is the value of evaluation in space result with expected value of $[0 \; , \; 1.00]$. In this project, the S was replaced by PCC aiming to standardize values and transform the relation between the behaviors in a linear relation which can be represented on a Cartesian plan, shown in Figure 6.

Those expect values to the PCC possess values between $[-1.00 \; , \; 1.00]$, and the nearest to 1 will be most similar behavior among users. If values are negative represent opposite behaviors among users. Thus, the user category is determined (normal, suspect, abnormal). We assumed the following definition:

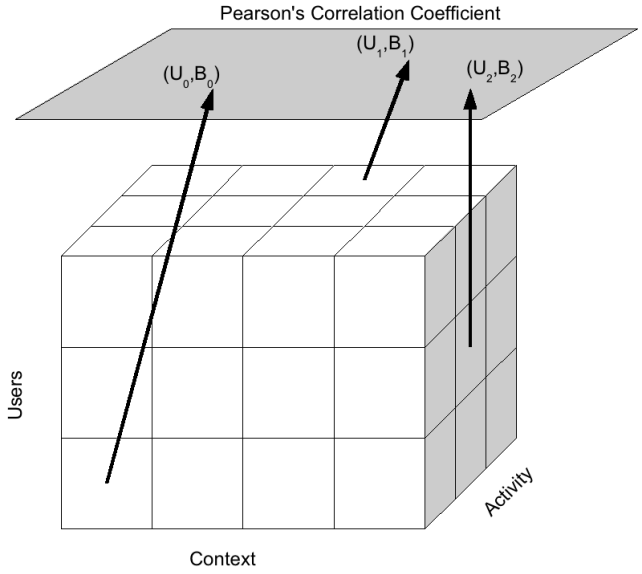

Fig. 6. Person's Correlation apply in Collaborative Filter

- Normal user: PCC above 0.85;
- Suspect user: PCC between 0.70 and 0.85;
- Abnormal user: PCC below 0.70.

Given the intervals defined previously, there is the need of testing the user with the challenge corresponding to a abnormal user and to the authentication level required by the application (high level), as shown in the Table of Figure 5 and Table 2. When the user responds to the challenge correctly, he is authenticated in the system, executes the desired operation and the requested event is inserted in the user profile, which contains the history of his interactions with the system.

5.3 Hybrid filtering

The experimental results presented in this section are related to the hybrid filtering. We conducted an analysis of the architectural core (Beliefs Analyzer) and its interaction with other modules, through complete authentication cycles (see Figure 7), as follows:

1. the behavior (B_0) is captured in the mobile device;
2. the event is analyzed under the spatio-temporal perspective;
3. the conditional probability determined by the spatio-temporal permutation model is used to verify the similarity degree of the event with the user behavioral profile;
4. the need to challenge the user is analyzed, based on the authentication level required by the application; and
5. if the authentication process is completed with success then the user behavior is stored in the profile database.

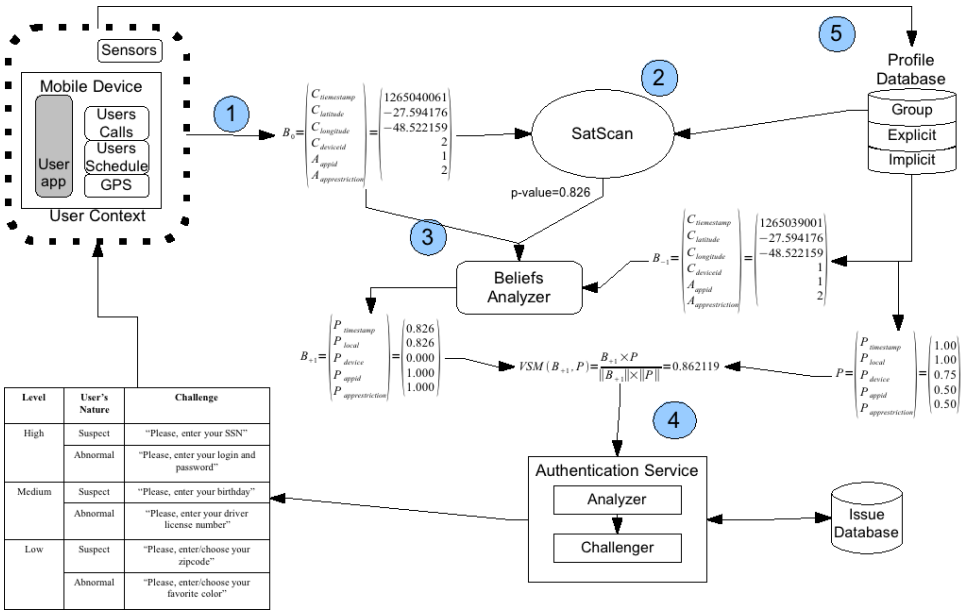

Fig. 7. Experimental Results of Hybrid Filtering

Based on this analysis, it is possible to determine the capacity of the context sensitive authentication system to aggregate new user knowledge and abilities, enabling system autonomicity. With this purpose, firstly, we defined which are the behavioral attributes to be considered according to the proposed target scenario.

We opted for the following parameters: the mobile device used, the location of the event occurrence, the timestamp of the event occurrence, the application being executed and the constraints of the executed application. Next, we defined the weights associated with each behavioral attribute, to set different priority levels to the analysis of the different comparative attributes. Therefore, the following weights were used: $P = (P_{timestamp} = 1.00, P_{location} = 1.00, P_{device} = 0.75, P_{appid} = 0.50, P_{apprestriction} = 0.50)$

When the user accesses the system for the first time, he enters personal information (e.g. authentication in the medical clinic). When he provides such information, he is authenticated on the system. After such information is provided, the system is able to extract the explicit profile and the user session profile, which in the first interaction are the same.

Therefore, the proposed authentication process is performed from the second user interaction. In the second interaction, the same application was requested, from the neighborhood location of the first interaction. However, such request was performed from another available mobile device. To determine the vectors used to compute the similarity degree, we need to use the weights previously defined to VectorP. On the other hand, to determine VectorE, the attribute values must be compared, which is performed comparing the captured behavior B_0 and the session profile (behavior B_{-1}). The attributes values that remained unchanged received one (1) as its value, and those that changed received zero (0) as its value. In the case of the

spatio-temporal attributes (location and timestamp) the value to be received is the minimum value of the spatio-temporal permutation model considering the spatio-temporal cluster used as reference, determined using the SaTScan tool (Kulldorff, 2005).

The base to the analysis, in the SaTScan tool, is composed of 280 previously collected events. Thus, when comparing the p-value of the two executions of the spatio-temporal permutation model (with co-variables and without co-variables), the system finds the minimum value between them to analyze the worst case (the case that represents a higher risk to the authentication process). Therefore, the system uses the p-value of 0.826, determined by the spatio-temporal analysis without co-variables, which is represented in Figure 8. Such value is used to compute the similarity degree between the captured event and the session profile, which represents the user execution context, and, therefore, exists only during the interaction of the user with the application being considered. The remaining models shown on Figure 8 are presented to demonstrate the efficiency of the spatio-temporal permutation in the detection of anomalies in pervasive systems.

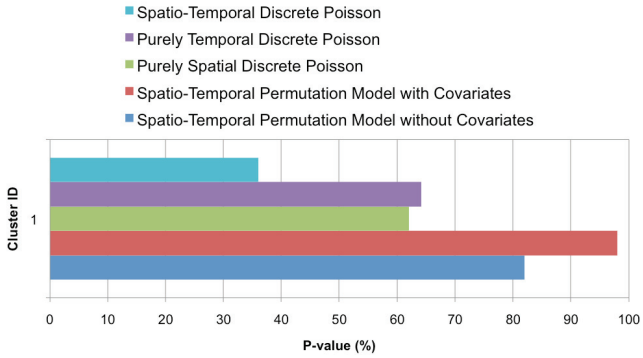

Fig. 8. Results of SaTScan analytical models

After the definition of these two vectors, it is possible to determine the similarity degree between the captured vector and the session profile. However, as there is the need to determine which are the intervals of values for similarity degree, which determine each user category (normal, suspect and abnormal). Thus, we assumed the following definition:

- Normal user: a similarity degree above 90%;
- Suspect user: a similarity degree between 70% and 90%;
- Abnormal user: a similarity degree below 70%.

According to the definition of these intervals, there is the need to test the user with the challenge regarding to a suspect user and regarding to the authentication level required by the application (medium level), according to table presented in the Figure 7 and Table 2. When the user responds the challenge correctly, he is authenticated in the system, executes the desired operation and the requested event is inserted in the user profile, which contains the history of its interactions with the system.

As Figure 9 illustrates, it is perceptible that the proposed context sensitive authentication architecture enables the evolution of its behavioral parameters, through the incorporation of

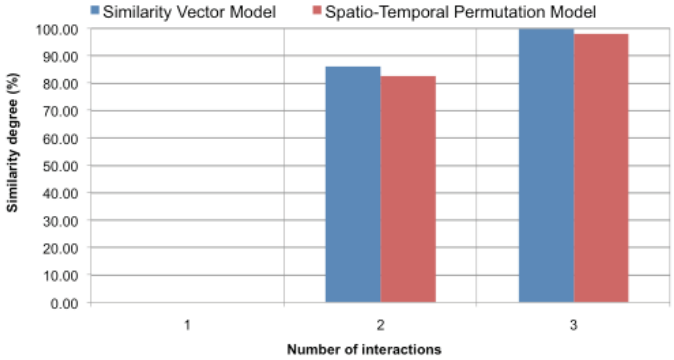

Fig. 9. System evolution according to the number of interactions

user events (activities) to the explicit profiles, implicit profiles and user session. Interactions of the system with the authentication module are represented in the X-axis, the first interaction is a traditional authentication, i.e., through password without graphical representation.

Consequently, the system is able to widen its knowledge base, and, thus, aggregate the user actions, which reflect its knowledge and abilities, refining the authentication process according to the number of interactions with the user. Through the dynamism offered by the proposed architecture, it is possible to provide a higher autonomicity to the user, i.e., the authentication system continually reduces the need for explicit data input to the system (response to challenges).

6. Conclusion and research agenda

Through this research, regarding the determination of user behavior in mobile computing environments, we confirmed the importance of considering two fundamental attributes in the user context: space and time. Such properties are relevant, as human beings have habits and the time correlations determine successive events that define a behavioral profile. Thus, in this work, an event is defined as the situation of an entity defined by one of more contexts that compose the user total context, in a given location and in a given time frame.

Therefore, a research was needed to analyze behavioral models considering both attributes (time and space) simultaneously, aiming to obtain a more precise evaluation of user behavior, identifying conformity in the behavior standard and possible behavior anomalies, which would characterize a suspicion attempt of automatic authentication.We proposed the use of a context-aware recommendation system model which allows the user of three filtering approaches: i) content based filtering, ii) collaborative filtering and iii) hybrid filtering. The experimental results comprising the content based filtering, and its respective analytical model, present a significant efficiency in the detection and analysis of anomalies in the authentication process.

Beyond that, the proposed architecture fulfills the autonomicity and dynamicity requirements, as through the behavioral profiles defined by the vector space model, the system is able to aggregate the skills and the knowledge acquired by the user during his interaction with the system. Additionally, our proposal provides flexibility as it allows different authentication

forms, according the security levels required by the executed applications. Thus, we consider that the proposed approach was able to circumvent the lack of existent alternatives in the literature to fulfill simultaneously the requirements of context-awareness, computational efficiency, flexibility, autonomicity and dynamicity.

Future work will focus on conducting the impact analysis of the number of users on the context-aware authentication mechanism, i.e. the system capacity to maintain an acceptable rate of success in the authentication process even in the presence of an increasing number of users registered in the system. Another future work is a case study for each recommendation filter, aiming to evaluate their performance in terms of knowledge acquisition and of portability of mobile devices in the authentication of information and of the device itself.

7. Acknowledgments

This work was partially supported by CNPq (National Counsel of Technological and Scientific Development) of MCT (Ministry of Science and Technology), Brazil.

8. References

Augustin, I., Yamin, A., da Silva, L., Real, R., Frainer, G. & Geyer, C. (2006). ISAMadapt: abstractions and tools for designing general-purpose pervasive applications, *Software: Practice and Experience* 36(11-12): 1231–1256.
URL: *http://onlinelibrary.wiley.com/doi/10.1002/spe.756/pdf*

Bellavista, P., Corradi, A., Montanari, R. & Stefanelli, C. (2003). Context-aware middleware for resource management in the wireless Internet, *IEEE Transactions on Software Engineering* 29: 1086–1099.
URL: *http://www.computer.org/portal/web/csdl/doi/10.1109/TSE.2003.1265523*

Burke, R. (2007). Hybrid web recommender systems, *in* P. Brusilovsky, A. Kobsa & W. Nejdl (eds), *The adaptive web*, Vol. 4321 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 377–408.
URL: *http://portal.acm.org/citation.cfm?id=1768211*

Cassens, J. & Kofod-Petersen, A. (2006). Using activity theory to model context awareness: a qualitative case study, *Proceedings of the 19th International Florida Artificial Intelligence Research Society Conference, Florida, USA, AAAI Press*, pp. 619–624.
URL: *http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Using+Activity+Theory+to+Model+Context+Awareness+:+a+Qualitative+Case+Study#0*

Corradi, A., Montanari, R. & Tibaldi, D. (2004). Context-based access control management in ubiquitous environments, *Network Computing and Applications, IEEE International Symposium on* 0: 253–260.
URL: *http://www.computer.org/portal/web/csdl/doi/10.1109/NCA.2004.1347784*

Dey, A. (2001). Understanding and using context, *Personal and ubiquitous computing* 5(1): 4–7.
URL: *http://portal.acm.org/citation.cfm?id=593572*

Hassan, J., Riaz, A. & Raazi, S. (2008). Activity-based Security Scheme for Ubiquitous Environments, *IPCCC 2008.* pp. 475–481.
URL: *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4745102*

Hong, J., Satyanarayanan, M. & Cybenko, G. (2007). Guest Editors' Introduction: Security & Privacy, *IEEE Pervasive Computing* 6(4): 15–17.

Jameel, H., Shaikh, R., Lee, H. & Lee, S. (2006). Human identification through image evaluation using secret predicates, *Topics in Cryptology–CT-RSA 2007* 4377: 67–84.
URL: *http://www.springerlink.com/index/EVL6JGT546674294.pdf*

Johnson, G. (2009). Towards shrink-wrapped security: A taxonomy of security-relevant context, *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, IEEE, Galveston, TX, pp. 1–2.
URL: *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4912819*

Kim, J., Song, C., Kim, T., Rim, K. & Lee, J. (2009). Secure and Efficient Recommendation Service of RFID System Using Authenticated Key Management, *Ubiquitous Information Technologies & Applications, 2009. ICUT'09. Proceedings of the 4th International Conference on*, IEEE, pp. 1–5.
URL: *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5405678*

Kulldorff, M. (2005). SaTScan: software for the spatial, temporal, and space-time scan statistics, version 5.1 [computer program], *Inf Manag Serv* .
URL: *http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:SaTScan:+Software+for+the+Spatial,+Temporal,+and+Space-Time+Scan+Statistics#0*

Lima, J., Rocha, C. & Dantas, M. (2010). An authentication approach based on behavioral profiles, *Information Systems and Technologies (CISTI), 2010 5th Iberian Conference on*, IEEE, Santiago de Compostela, Spain, pp. 1–4.
URL: *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5556601*

McDonald, D. (2003). Ubiquitous recommendation systems, *Computer* 36: 111.
URL: *http://www.computer.org/portal/web/csdl/doi/10.1109/MC.2003.1236478*

Munoz-Organero, M., Ram\'\iez-González, G., Munoz-Merino, P. & Kloos, C. (2010). A Collaborative Recommender System Based on Space-Time Similarities, *IEEE Pervasive Computing* pp. 81–87.
URL: *http://www.computer.org/portal/web/csdl/doi/10.1109/MPRV.2010.56*

Oku, K., Nakajima, S., Miyazaki, J., Uemura, S., Kato, H. & Hattori, F. (2010). A Recommendation System Considering Users' Past/Current/Future Contexts, *ids.csom.umn.edu* pp. 3–7.
URL: *http://ids.csom.umn.edu/faculty/gedas/cars2010/OkuEtAl-CARS-2010.pdf*

Rahmati, A. & Zhong, L. (2009). Human-battery interaction on mobile phones, *Pervasive and Mobile Computing* 5(5): 465–477.

Ray, S. & Mahanti, A. (2009). Strategies for effective shilling attacks against recommender systems, *Privacy, Security, and Trust in KDD* 5456: 111–125.
URL: *http://www.springerlink.com/index/d6v15h1276872265.pdf*

Ricci, F. (2011). Mobile recommender systems, *Information Technology and Tourism* 12(3): 205–231.
URL: *http://www.ingentaconnect.com/content/cog/itt/2011/00000012/00000003/art00002*

Ricci, F. & Nguyen, Q. (2007). Acquiring and revising preferences in a critique-based mobile recommender system, *IEEE Intelligent Systems* 22: 22–29.
URL: *http://doi.ieeecomputersociety.org/10.1109/10.1109/MIS.2007.43*

Ricci, F., Rokach, L. & Shapira, B. (2011). Introduction to Recommender Systems Handbook, *Recommender Systems Handbook* pp. 1–35.
URL: *http://www.springerlink.com/index/X8622U506942LU28.pdf*

Roberts, M., Ducheneaut, N., Begole, B., Partridge, K., Price, B., Bellotti, V., Walendowski, A. & Rasmussen, P. (2008). Scalable architecture for context-aware activity-detecting

mobile recommendation systems, *World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a*, IEEE, pp. 1–6.

Rocha, C. C. (2010). *A Context-Aware Authentication Approach Based on Behavioral Definitions*, Master's thesis, Federal University of Santa Catarina, Florianopolis, SC, Brazil.

Romero-Mariona, J., Ziv, H. & Richardson, D. (2008). SRRS: a recommendation system for security requirements, *Proceedings of the 2008 international workshop on Recommendation systems for software engineering*, ACM, pp. 50–52.
URL: *http://portal.acm.org/citation.cfm?id=1454266*

Sathish Babu, B. & Venkataram, P. (2009). A dynamic authentication scheme for mobile transactions, *International Journal* 8(1): 59–74.
URL: *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.155.4468&rep=rep1&type=pdf*

Shi, E., Niu, Y., Jakobsson, M. & Chow, R. (2011). Implicit authentication through learning user behavior, *Information Security* pp. 99–113.

Su, X. & Khoshgoftaar, T. (2009). A survey of collaborative filtering techniques, *Advances in Artificial Intelligence* 2009: 19.

Toninelli, A., Montanari, R., Lassila, O. & Khushraj, D. (2009). What's on users' minds? toward a usable smart phone security model, *IEEE Pervasive Computing* pp. 32–39.

Uden, L. (2007). Activity theory for designing mobile learning, *International Journal of Mobile Learning and Organisation* 1(1): 81–102.
URL: *http://inderscience.metapress.com/index/EW9VEADD3EUFJHV3.pdf*

van der Heijden, H., Kotsis, G. & Kronsteiner, R. (2005). Mobile Recommendation Systems for Decision Making, *Mobile Business, International Conference on* 0: 137–143.
URL: *http://www.computer.org/portal/web/csdl/doi/10.1109/ICMB.2005.68*

Zhan, J., Hsieh, C., Wang, I., Hsu, T., Liau, C. & Wang, D. (2010). Privacy-preserving collaborative recommender systems, *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 40(4): 472–476.
URL: *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5411745*