Mobile Netw Appl (2014) 19:392–403
DOI 10.1007/s11036-014-0516-9

Behavior and Capability Based Access Control Model for Personalized TeleHealthCare Assistance

Meriem Zerkouk · Paulo Cavalcante · Abdallah Mhamed · Jerome Boudy · Belhadri Messabih

Published online: 14 June 2014
© Springer Science+Business Media New York 2014

Abstract With the growing proportion of dependant people (ageing, disabled users), Tele-assistance and Tele-monitoring platforms will play a significant role to deliver an efficient and less-costly remote care in their assistive living environments. Sensor based technology would greatly contribute to get valuable information which should help to provide personalized access to the services available within their living spaces. However, current access control models remain unsuitable due to the lack of completeness, flexibility and adaptability to the user profile. In this paper, we propose a new access control model based on the user capabilities and behavior. This model is evaluated using the data sensed from our tele-monitoring platform in order to assist automatically the dependent people according to the occurred situation. The design of our model is a dynamic ontology and evolving security policy according to the access rules that are used in the inference engine to provide the right service according to the user's needs. Our security policy reacts according to the detected distress situation derived from the data combination of both the wearable devices and the pervasive sensors. The security policy is managed through the classification and reasoning process. Our classification process aims to extract the behavior patterns which are obtained by mining the data set issued from our Tele-monitoring platform according to the discriminating attributes: fall, posture, movement, time, user presence, pulse and emergency call. Our reasoning process aims to explore the recognized context and the extracted behavior patterns which set up the rule engine to infer the right decision security policy.

Keywords Tele-healthcare · Tele-monitoring · Assistive living · Access control · Classification · Context awareness · User behavior · User capability · User profile · Modeling · Reasoning · Querying

M. Zerkouk (✉) · B. Messabih
University of Sciences and Technology of Oran Mohamed Boudiaf (USTO-MB), Oran, Algeria
e-mail: meriem.zerkouk@univ-usto.dz

M. Zerkouk
e-mail: zerkouk.meriem@gmail.com

B. Messabih
e-mail: belhadri.messabih@univ-usto.dz

P. Cavalcante · A. Mhamed · J. Boudy
Mines-Telecom Institute/Telecom SudParis CNRS Samovar UMR 5157, Evry, France

P. Cavalcante
e-mail: paulo.cavalcante@telecom-sudparis.eu

A. Mhamed
e-mail: abdallah.mhamed@telecom-sudparis.eu

J. Boudy
e-mail: jerome.boudy@telecom-sudparis.eu

1 Introduction

As stated in the statistic reports, the rate of ageing and frail population is growing rapidly. This great emerging flux has attracted the attention of many researchers by focusing their purposes to enhance their daily life by integrating the assistive technologies in the smart environment [1].

Ambient intelligence [2] and context awareness provide an assistive environment allowing dependent people to perform their required services with more autonomy.

For making these living/working spaces more safe and more secure for dependent people [3], We consider the user as a central point by taking into account:

– The specific requirements of these people in terms of protection of their life and regardless to preferences and their impairments (physical, sensory or cognitive).

- The strong vulnerability of some spaces like medical care environments where both reliability and security can affect timeliness and accuracy information for patient monitoring.
- The wide range of involved actors: caregivers, medical staff, nurses, emergency personnel, law enforcement agencies, government/community leaders among which the shared information should be secure, private, reliable and anonymous.
- The variety of living spaces both private (residences) and public (hospitals, workplace, etc.), where sharing information/services between users should be secure and anonymous.

With the growing healthcare and wellbeing context aware applications [4], the Tele-monitoring platforms are becoming an emerging research area for ensuring monitoring and assistance for elder and frail people [5, 6].

In our healthcare tele monitoring platform [7, 8], a continuous care and monitoring the daily living activities and behavior were performed by the integration of the wearable devices and the pervasive sensors to provide more adaptive and personalized assistance. The collected data are mainly categorized into body and environment through the GARDIEN [9], RFPAT [10] and ANASON [11] systems. The data provided by our platform which are acquired from multi source sensors are related to fall, posture, movement, time, user presence, pulse and emergency call. Therefore, a representation process in standard structure is required. Due to the expressiveness, possibility to represent complex and heterogeneous data, the ontologies are more appropriate to model the contextual data. The key feature is the support of semantic reasoning that aims to process the modeled data to derive high, complex and implicit knowledge from raw data.

According to literature review [12], the current access control models are mainly role centered and the dynamicity depends on the occurred context environment changes like location, time, temperature and noise. Even, if provided services are more or less personalized according to the users profile and preferences. They still do not take into account the user capabilities.

In order to develop a personalized and adaptive health care model, so many new challenges have to be taken into account: context awareness, personalization, smartness, adaptability and extensibility.

To address these challenges, we have proposed a context-aware access control model and its related architecture based on user behavior and capabilities [13–15]. The model is based on dynamic ontology which support continuous learning of behavior and capability patterns.

We designed an initial ontology driven knowledge base representing the access rules, context, behavior pattern, profile, services, devices and environment. We used ontology modeling to ensure sharing, reuse, interoperability, flexibility, adaptability of the security policy guidelines. In order to implement our approach, our model relies on three main mechanisms: acquisition, management and security. The context acquisition is provided by our Tele-monitoring platform. The management is ensured focusing on modeling and reasoning process which aims to handle the collected context and to ensure an adaptive access control using the classification process results of the monitored user behavior. Finally, the access decisions are gotten back by means of the querying process.

The reminder of this paper is organized as follows: Section 2 reviews the literature research work according to the context aware framework (acquisition, modeling, reasoning and application). The challenges which motivated our work are given in section 3. Section 4 presents our proposed approach and the key ideas of our model design. Section 5 describes the sensed data environment of our Tele-monitoring platform. Section 6 discusses the need of tracking and how to provide a reactive context aware system and pattern recognition to build the user behavior profile. Section 7 details our security policy management (modeling, reasoning and querying). Section 8 illustrates the implementation of our approach through a scenario while section 9 analyses and discusses the obtained results. The last section concludes the paper.

2 Related Work

In smart spaces, contextual data provided by various embedded devices are used to detect critical situations, to monitor activity daily life and/or to adapt the access control. According to Dey [16], *Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.*

The current research aims to improve the quality of daily life for dependent people where several areas are targeted by introducing many devices in our environments (house, hospital, working space and transport). However, many new contextual data are introduced because the use of wearable devices and pervasive sensors is in a continuous progress as shown in [17, 18]. According to the targeted area, the contextual data considered in our work belongs to user and environment context.

The user context represents any information collected from wearable devices and pervasive sensors. The acquired data mainly include:

- The identity or personal information which can be static or dynamic such us: the name, the age, the sex, the job, the phone number.

- The activity context which represents the activity performed by the user like sleeping, walking, preparing meals, taking showers, moving or going out.
- The profile context which include both preferences and capability of the user like faller, diabetics or disabled.
- The physiological context which corresponds to the data issued from body sensors (hypertension and hyperglycemia).

The environment context represents any kind of information collected by means of the different sensors embedded in both the indoor and outdoor environments. In this work, only indoor environment is taken into account using geographical context and temporal context.

The system handling the contextual data is defined as [16]: *a context aware system, if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task.* In order to explore the following data, we have to follow the life cycle of context management according to the referential model of context aware system.

Our literature review is organized according to four relevant issues [19, 20]: the acquisition, the modeling, the reasoning and the context application.

2.1 Context Acquisition

The acquisition process is required to carry out a context aware system. The context acquisition refers to gathering data from the embedded sensors and the wearable devices. In the literature [17, 18], many sensing techniques used to collect the data are based on: responsibility (pull/push), frequency (instant/interval), context source (sensor hardware, middleware and server) and sensor type (physical/virtual and logical). The sensors used in this process are in a great progress in order to enhance the coverage area. Our study is focused only on the non intrusive sensors which preserve the user privacy (i.e. video cameras are excluded). The general acquired data are collected through different manners and by answering to Whs: who, what, when, and why. These data belong to three categories: the sensed, the derived and the surveyed data. The sensed data are derived directly from sensors (RFID, GPS and Bluetooth) which are mainly: location, time, temperature, humidity, ambient light, user presence and identity. The derived data are extracted from the sensed data (location and time) to recognize the activity, the situation, the behavior and other complex data related to user impairments. For that, many artificial intelligence techniques and data mining algorithms are required. The surveyed data are provided by using a survey involving caregivers to retrieve the preferences, the habits and the hobbies. For many emerged applications of ambient assisted living, there is a lack in terms of acquiring contextual data from multi sources and to use audio sensors for detecting noise, emergency and distress situation in order to infer high and implicit knowledge.

2.2 Context Modeling

Context model is a pattern to represent the object "context" [17]. The modeling process is required to move from the low level to the high level. Hence, many context modeling techniques are developed and discussed in [18] to represent the contextual data: key value, markup, graphical, object oriented, logic based, ontology and multidisciplinary context models. To deal with the heterogeneity, the sharing, the reuse or the formal expressiveness and to represent the collected data into standard form, the ontologies are more suitable for the modeling process. In this research area, many models were proposed to provide the most generalized user and environment model. The user models focused on defining the personal information, activities, preferences and profile [21, 22]. The most emerged environment models are indoor and outdoor environment. The previous proposed models did not represent and deal with behavior, capability and health problem which require the use of multi source sensors.

2.3 Context Reasoning

Context reasoning can be defined as a method of deducing new knowledge, and understanding better, based on the available context [18]

The reasoning process aims to deduce more complex implicit knowledge context from the sensed data. To set up the process, many techniques were proposed in the literature [17, 18]:

- Exact context reasoning: this class is ensured through Bayesian Network-based Reasoning, Logic-based Reasoning, Rule-based Reasoning or Ontology-based Reasoning.
- Inexact context reasoning: this class deals with Fuzzy-based reasoning or Evidence-based reasoning.

Owing to the efficiency, the completeness and the interoperability ensured by means of semantic reasoner [23, 24], we focused on ontology based reasoning where the semantic aspect is supported. Until now, there is not a process reasoning supported by such Tele-healthcare to monitor the emergency, health problems, behavior capability in term of impairments (physical, sensory or cognitive).

2.4 Context Application Areas

Context aware based Access control relies on context data to assign the permission to the users (roles) in the right situation

which makes the model dynamic according to the change of context over the time.

According to our literature study, various access control models are mainly based on complex parameters like: context, trust, privacy, situation, profile.

Extended RBAC models [25–27] are based on context awareness. Their aim is to improve RBAC by assigning the right access more dynamically. The access is based on the context validity by adding to RBAC a single contextual data which is spatial, temporal or environmental [28, 29].

According to [30], the proposed architectures are designed to ensure adaptation and personalization taking into accounts the context evolution over time. Among them we can mention Cobra and context toolkit.

3 Motivations and Challenges

Context awareness, smartness, personalization, adaptability and/or reactivity are considered as open challenging issues that still remain to be resolved. We have to provide more contribution solutions dedicated to people facing specific situations caused by distress or abnormal behavior. In order to address adaptability and personalization issues, it becomes necessary to use multi source data that permit to derive more complex knowledge. The collected data must be managed into standard form and with semantic aspect for both the modeling and reasoning process. More context aware application data are required to enhance the remote monitoring by providing smart and automatic solutions to deal with the occurred emergency for providing adaptive and personalized assistance services. Targeting our objective to provide assistance and tele-healthcare to dependant and frail people, our access control model is motivated by the following challenging features:

- Context awareness: The context awareness feature is required to deal with the dynamic data for ensuring an adaptive service to the arising situation. Both environment and body data are needed to ensure more suitable assistance. In fact, it is necessary to introduce the most significant sensors.
- Reactivity: The reactivity feature is required to make the decisions on the basis of the current contextual data and the past behavior which is stored as historical file.
- Personalization: This is our main security policy feature which requires richer user context (profile, capability, preference, habit, health situation). For this, we need to identify the different situations that will be used in the design of access control model because the profile capability has an important influence on the assignment of the right decisions. Personalized assistance is the most important challenge to be taken into account in such care access control model.
- Adaptability: this is our second major concern. Since the personalization is ensured, the adaptation is required to the identified sensitive user features (profile, capability, preference, habit and health state) to provide the most adaptive service.
- Extensibility: This feature is important considering the smart environment that integrates dynamically more devices and services where more constraints are required to be taken into account.
- Trustworthy: Ensuring reactive system that need to take into account the past behavior and present contextual data at a given time. By this use, the trustworthy is ensured by having more confidence about the users and this feature affects directly the personalization and adaptability characteristics.
- Privacy: Ensuring assistance for the dependent people by taking into consideration the security of their personal life. The monitoring is ensured through the non intrusive sensors which preserve the user privacy (i.e. video cameras are excluded).
- Smartness: This feature is defined by means of the insurance of the reactivity, the personalization and the adaptability when delivering the appropriate service for the specific user.

4 Behavior Capability Based Access Control Approach

The design of access control models is in a continuous progress by including many contextual data sources. However, our contribution is related on the security policy design, behavior capability based access control model and its related architecture which require the main context management process (acquisition, modeling, reasoning and adaptation).

Our targeting security policy is reactive, personalized and adaptive to the user behavior capability, user context and the surrounding environment changes. The decisions are not limited to “permit” or “deny” outcomes. To deal with the assistance service for dependent people the policy is extended to include more and suitable decisions: permission, obligation, recommendation or prohibition which are adapted to the user impairment disability. We focus our work on behavioral trend [31] and the behavior capability mining is the key feature. For that, the right decision is assigned according to the analyzed historical behavior, current context, detected critical situation and capability.

Our access control model aims to implement our security policy specification by means of ontology taking advantages of modeling, reasoning, querying and taking into consideration the semantic aspect, the data heterogeneity of the sensed data which are not limited to environmental devices.

The related architecture is set up by means of the collected contextual data which their richness is due to the combination of both the environment and the patient data acquired from our tele-monitoring platform composed of RFPAT and GARDIEN systems. Monitoring platform provides recording the historical behavior which is used to analyze deeply the monitored user and to provide a reactive context aware system for ensuring the best personalized assistance to the dependent people. Consequently, the generated data allowed us to validate our developed security policy.

Our access control policy is illustrated in the Fig. 1 and set up through the architecture shown in the Fig. 2. The decision is assigned to the user to reach services; depends on the analysis of various elements characterizing the user (behavior, context, situation, profile and capability).

$$Policy = < [B_i(t), Ctx(t), St(t), \Pr(t-1), Cpb], S, D_k >$$

- The behavior $B_i(t)$: which represents what the user is performing at time (t) such us the user is walking, doing any activity where $B_i(t) \in [B_{0,..,}B_5]$
- The present context $Ctx(t)$: The context variable corresponds to the sensed data at the present time and describes the user and the surrounding environment state acquired by means of wearable and embedded devices. The context values are: time, pulse, posture, location. $Ctx(t)=\{C1, C2, C3, Cn\}$
- The situation $St(t)$: which presents the sensitivity situations which is identified from the behavior sensed. In our work, we have identified six sensitive behaviors which are: normal, abnormal, critical, alertness (high and low) blood pressure or emergency (sudden fall).

- The user profile $Pr(t-1)$: Which is required to check the historic of accident.

$$\Pr(t-1) = \{faller, \quad cardiopath\}$$

- The capability (Cpb): which represents the impairments types: deafness, blindness, cognitive or physical.
- The service (S): which represents the asked service by the user.

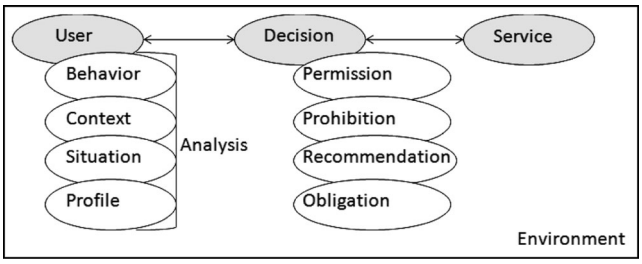


Fig. 1 Security policy specification

- The decision (D_k): which represents the analysis of the user state then a decision is assigned according to the set up policy. $D_k \in \{Permission, Interdiction, Obligation, Recommendation\}$

Our approach is carried out by implementing the main four layers in order to reach our assistance system:

- Data acquisition layer: This basic layer is responsible to collect the sensed data from our platform which is constructed on the basis of RFPAT and GARDIEN.
- Behavior extraction layer: This layer consists in combining the different data describing the context of the user and his environment through the use of different kind of sensors (infrared and accelerometers). Specifically, the monitored user behavior is recorded from many days. The collected data will be experimented to identify the main behavior patterns according to the features set. The obtained results will be used to set up the rule engine.

Security policy management layer:

- Security policy modeling: Once the data collected and the behavior classes identified, a modeling process is required to represent the data on standard form and adding semantic aspect for the different entities describing the user and his environment in order to set up the reasoning process.
- Access control reasoning: In this layer many rules will be defined in order to deduce a new and implicit knowledge about the context, the activity, the situation and to analyze the identified user situation. Finally, the right decision is derived.

Adaptive assistance layer: which is used to send assistance decision taking into account the user capability that might be vocal for blind people, txt for deaf people and repetitive for people suffer cognitive problems. According to the collected data, the constructed ontology is queried to derive the appropriate decision.

5 Sensing Data with Tele-Healthcare Monitoring Platform

Smart environments are an application domain of the most emerged Ubiquitous Computing and Ambient Intelligence. In particular, the smart homes are designed for the dependent and aged people who prefer to live at home with more safety, more autonomy and in high quality health condition. Home healthcare monitoring is an ideal solution to deal with the people with risks and challenges of walking condition (falling) or cognitive (depression, dementia, etc.), people with

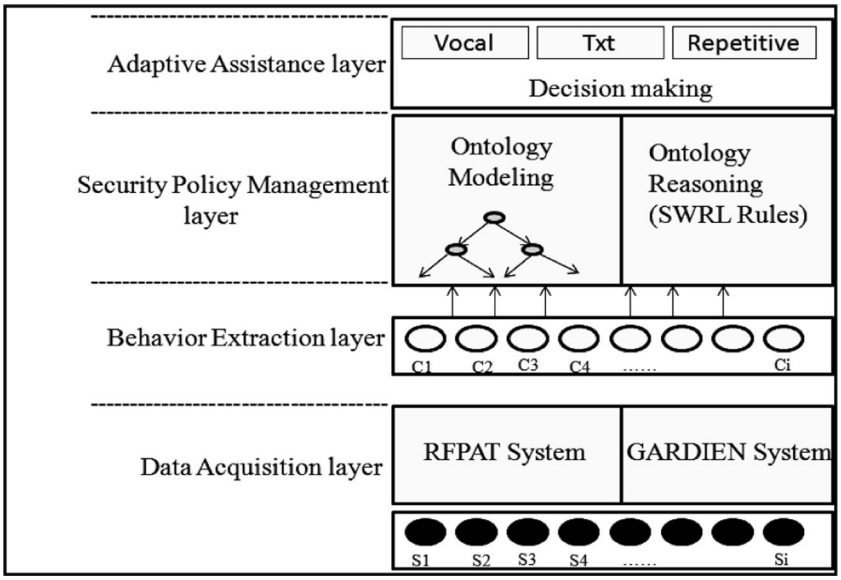


Fig. 2 Access control architecture design

physical impairment (blindness, deafness..), or in need of particular attention (diabetics, asthmatics, etc.) to ensure that elderly people can live safely and independently in their own homes for as long as possible. The recent one which is introduced by the Norwegian Centre for Telemedicine (NST) uses the following definition: *Telemedicine is the investigation, monitoring and management of patients and the education of patients and medical staff, which allow easy access to expert advice and patient information, no matter where the patient or relevant information is located.* These healthcare tele monitoring systems have the potential to improve the quality of older adult's life through the use of smart technologies to sense, alert and automate household priorities, as well as to provide home based healthcare.

A remote patient's monitoring system is integrated in a smart home environment and it can use the fusion results of several observation data such as actimetric and vital signals captured by a device worn by the patient, external sensors such as acoustic and presence signals which is composed of GARDIEN, RFPAT and ANASON. The system is explored in order to ensure a tele-assisante for the dependent people. In this work, the ANASON system has not been yet taken into account. The Fig. 3 shows the integration of the devices and sensors into the environment.

RFPAT system is a portable device designed for remote monitoring that can measure ambulatory vital and actimetric signals recorded on the person. This system is composed of a wearable terminal carried by the patient which can

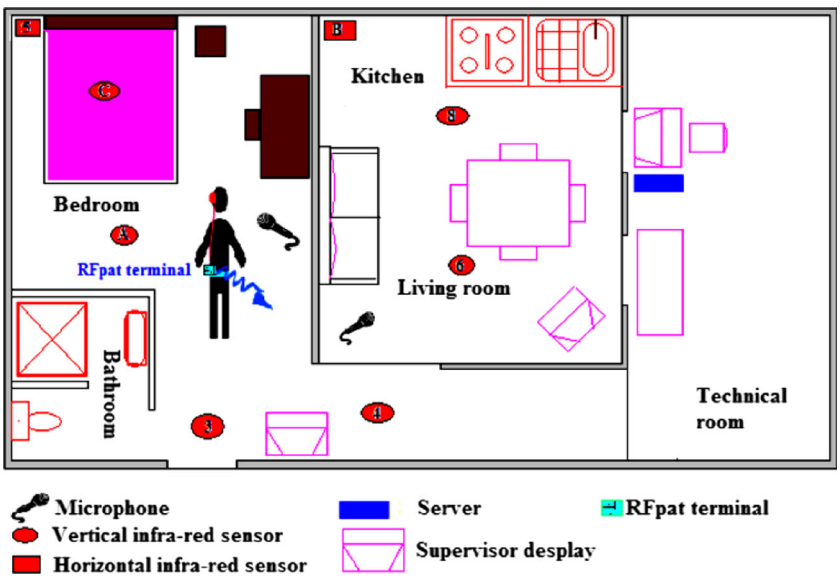


Fig. 3 Healthcare tele-monitoring platform

automatically identifies the different parameters: fall, pulse, movement, posture (lying down or standing).

GARDIEN system consists in a fixed network of wired or wireless infrared motion sensors placed within the smart home environment and external to the person. These sensors are activated by body movements which therefore indicate the presence of a person in the area of interest. The person's posture inclination can also be estimated from the combination of two types of infrared sensors, one for horizontal detection field, the other vertical.

The data used in our experiments are: time, location, pulse, movement, posture and fall.

Definition 1 (Time) The time attribute is used to identify and to distinguish between the different states: the user is located in the room, the user is doing a given activity or the user did a fall. The attribute time is described as follows:

$< Thu\ Oct\ 09\ 18:38:46\ 2008 >$.

Definition 2 (Localization) The localization attribute is captured by the activation of the infrared sensors set up in each room to detect the user presence and when he is moving in the living space. The localization value can be as follows:

$$Loc(t) \in L \text{ where } L = \{Room, Kitchen, Bathroom, Hall, living\ , room\}$$

Definition 3 (Pulse) The pulse attribute is used to oversee the cardiac state of the person where the attribute value is between $\{40,75\}$.

According to the data set, sometimes it goes down 40 and up to 75 this is due to errors measurement because the data are simulated by young researchers around thirty years old.

Definition 4 (Movements) The movements attribute aims to detect the mobility rhythm which vary within the range $\{0,15\}$. After our analysis, we have distinguished three value ranges:

Immobility [0-1]: which means that the person does not perform any activity.
Low mobility [1-7]: which means that the person is less dynamic.
High mobility [8-15]: which means that the person is more dynamic.

Definition 5 (Posture) The posture attribute aims to identify if the person is laying or standing. The attribute value is between $\{0,1\}$ where (0) means standing and (1) means lying. It is important to validate this attribute with the time and the localization values. For instance, if the person is laying in the kitchen at 12 h then the situation is abnormal.

Definition 6 (Fall) Fall attribute value is between $\{0,1\}$ where the falling situation is detected if its value is (1).

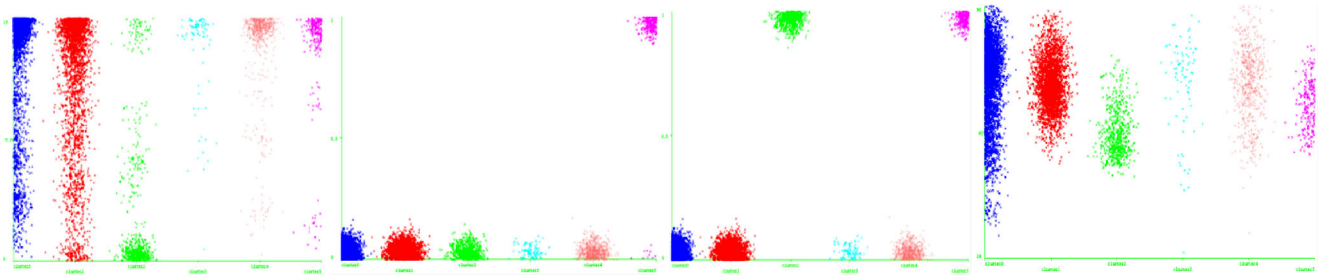
6 Behavior Pattern Extraction

Adaptation and personalization are our main key features in our access control design process. In order to reach this aim, it is required to set up a reactive context aware system by taking into consideration the context timeline and the past behavior. According to Mayrhofer [32], a reactive system provides *the output system at time t only depends on the current and implicitly on past states.*

To react at the right time and derive the most appropriate decision, it is useful to build reactive models. In telemonitoring, data mining is becoming a good solution to analyze the existing patterns by handling contextual data. Data mining provides a set of tools and techniques like clustering and classification to discover the hidden patterns. Our work experiment is based on clustering technique to analyze our data set recorded from our platform. Behavior analysis allows us to derive more implicit knowledge about the capability and the profile. However, the access control decision and assistance services can be personalized and adaptive.

6.1 Clustering

In our work, we have performed a real recording in smart living space where each instance reflects a real scenario in order to identify the user behavior pattern by applying a classification process. This step requires as input the defined feature vector $< F1, F2, F3 \ldots FN >$ describing a user and environment attributes. The generated data set is formed with 6409 vectors. The data used to structure a feature vector are highly heterogeneous which are acquired from multi sources sensors (wearable devices and pervasive sensors). After running a set of experiences by testing many algorithms, we have chosen the one which gives the most appropriate classification; specifically, which algorithm is able to group all vectors that are the most emergent behavior with (fall=1) and (posture =1) into one cluster. The obtained result are appreciated by using the most popular (k-means) Algorithm. The data experimentation is done by varying the desired number of classes until k=6 which is the best carving. Finally, we have obtained six common patterns derived from our experimented data. The obtained patterns are provided as input for the modeling and reasoning process. The results explored in the Fig. 4 are obtained from the knowledge extraction tool Weka [33].



(a) Clusters Vs Activity. (b) Clusters Vs Fall. (c) Clusters Vs Posture. (d) Clusters Vs Pulse.

Fig. 4 Data distribution in each cluster

6.2 Labeling and Discussion

The clustering process is performed in order to aggregate the similar behavior into classes in terms of the situation sensitivity and the detected emergency. The most discriminate parameters are mainly: fall, posture, activity and movement.

The obtained results shown in Fig. 4 are summarized and discussed in Table 1 that will be introduced as input to set up the security policy and especially to set up the rule engine of the reasoning process.

7 Security Policy Management

Reactivity, personalization, and adaptability are the key characteristics of our security policy. Taking into account the different features, it is required to manage the historical and the present contextual data which are collected from multi source sensors. The security policy management is conducted by means of the modeling, the reasoning and the querying process.

7.1 Behavior Capability Based Access Control Modeling

The security policy implementation is set up on the behavior model generated from the clustering process as shown in section 6 which there are six main classes identified exploring the recorded data. The handled data are acquired from different heterogynous sensors. So, a semantic aspect is required to deal with the collected data in order to combine the different nature of the sensed data. Therefore, the ontologies are chosen as mean to carry out our security policy for the formal expressiveness, the reuse, the heterogeneity, the interoperability and the semantic advantages. The proposed ontology is defined through the semantic web technologies, the Ontology Web language (OWL), the Semantic Web Rule language (SWRL), the RDF (Resource Description Framework) and the Simple Protocol Query Language (SPARQL) queries to interact and access to the data. These tools are used to define, represent and implement our proposed model in smart environment. Our conceptual framework of semantic access control policy is based on the definition of the knowledge database (KD), the asserted ABOX, the terminological TBOX and the rule engine to formalize our security policy. Our security model ontology is created with Protege editor [34] as shown in Fig. 5. The ontology is made up by defining the user, the device, the service, the environment and the policy classes as main entities and the interaction between them is performed by means of the semantic relationships.

Security Policy Class includes four subclasses: permission, interdiction, obligation and recommendation where each policy will be defined more precisely as rule in order to assign a policy according to the identified behavior, situation, profile and capability.

Table 1 A cluster analysis of the monitored user behavior

Cluster ID	Cluster description	Cluster Label
0	The user is highly mobile and suffers high blood pressure as shown in the figure (d).	Alertness (hypertension)
1	The user is highly dynamic, no cardiac or falling problems	Normal
2	The user is immobile with the (posture = 1) as shown in the figure (a).	Critical
3	The user suffers low blood pressure as shown in the figure (d) with average mobility. The user does not have falling problem.	Alertness (hypotension)
4	The user has a low mobility without cardiac or falling problems.	Abnormal (disturbing)
5	The user is immobile and suddenly did a fall and (the posture =1) means that the user is laying as shown in the figure (b, c)	Emergency (sudden fall)

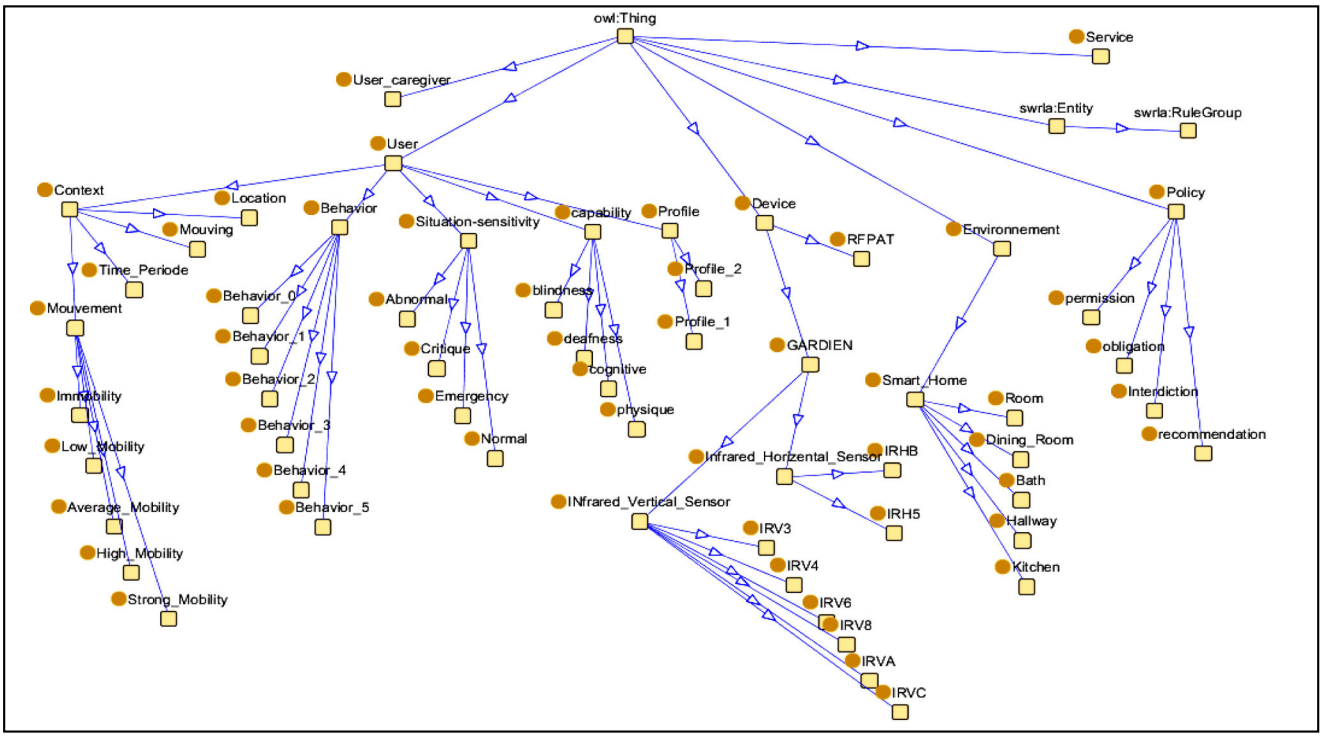


Fig. 5 Ontology of security policy

User Class The user can be the monitored one or the caregiver. In fact, the model distinguishes two user classes. The first one is considered as the main entity which requires representing all the user characteristics. It is defined through the behavior, the profile, the context and the situation subclasses.

- Behavior: that is defined into six subclass behavior from behavior (0) to behavior (5).
- Profile: allowed to store the historical accident, if the person had previously an accident like fall or cardiac problems.
- Context (current situation): this entity defines time, location, movement and moving.
- Situation: the subclass is defined also on four cases: emergency, critical, normal and abnormal.

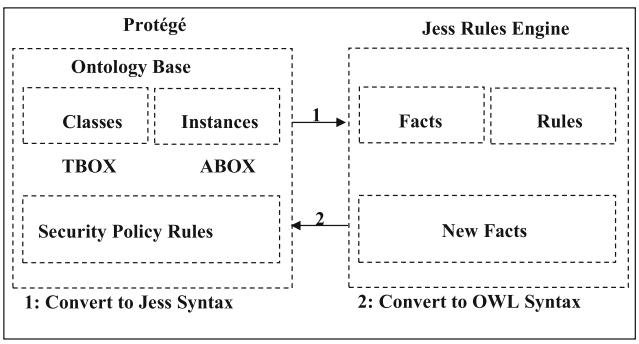


Fig. 6 Reasoning process

The interaction between the identified characteristics is ensured by defining a semantic attributes: asked_service (user, service), has_policy (user, policy), located_in (user, environment). The propriety (notify) serves as relationship with the user caregiver class in the case where an abnormal situation has occurred.

Service Class this entity represents the asked service (lighting on, windows opening, going out, cooking or, taking showers) which are very sensible after an identified distress situation.

Device Class The modeling process is limited to the devices integrated in the house which the used devices are summarized into GARDIEN and RFPAT systems that integrate vertical sensors (IRV 3, 4, 6, A, C) and horizontal sensors (IRH5, IRHB) as represented in Fig. 3. The defined proprieties are: Sensor_X_State.

Environment Class The modeling process is limited to Indoor living space like room, living room, bathroom, and kitchen. We have modeled the smart home shown in the figure (2). The required proprieties to implement this entity are: Equiped_by_sensor_x.

7.2 Reasoning on Access Control Policies

In order to infer the suitable access control decisions, a semantic reasoner is required to infer the decision from a set of asserted observations about dependant people located in their

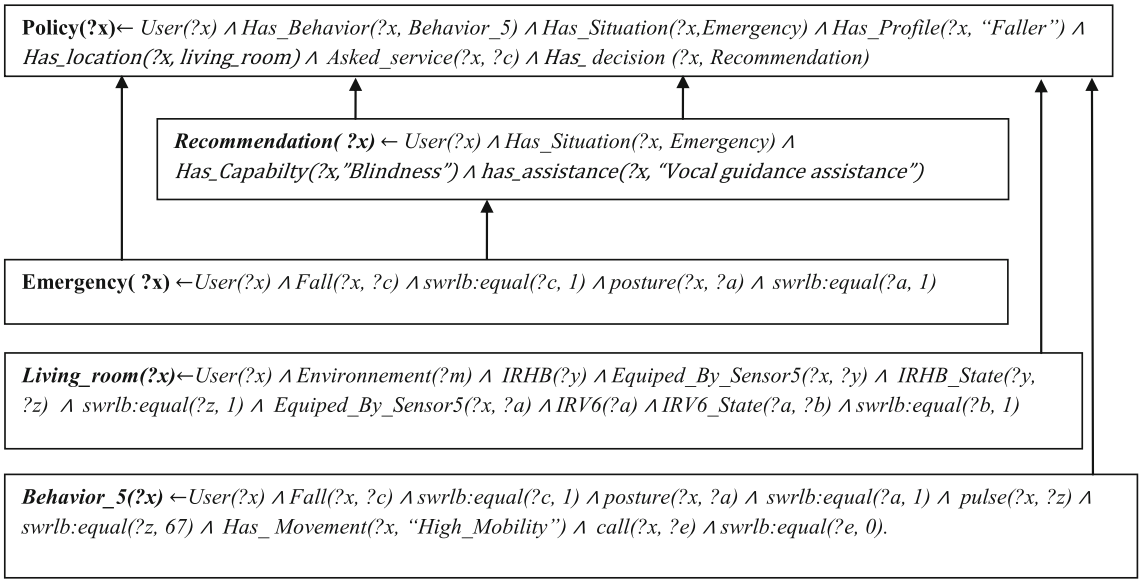


Fig. 7 Decision assignment based inference rules

living space. We specify semantic rules by the means of semantic web technologies as the following form<if conditions then conclusion>to perform the reasoning. Semantic reasoner aims to check the consistency of our proposed ontology model and derive high and implicit knowledge about the behavior, the situation, the profile, the capability and the access control decision about the user. We choose to implement the reasoning by using a complete open source OWL-DL reasoner as pellet (inference engine) [35] based on the forward chaining. As shown in Fig. 6, the reasoning process is performed by transferring and converting the defined classes, instances and the rules defined on Protege into jess syntax (facts, rules) to construct Jess rule engine [36]. After the inferring process, the new deduced facts will be injected as instances in the knowledge base of our ontology.

Our rule engine is distinguished into different categories; we have defined rules that manage: behavior, situation, profile, context, policies and decisions. The behavior rules are designed to express the six main patterns as shown in section 6.1. The rule parameters are mainly fall, position, movement, moving, posture, call and pulse. The movement parameter is distinguished into: Immobility, High and low mobility. The context rules are explored to derive the location context because the location parameter is not explicitly given. Each location value is defined by the combination of the horizontal and the vertical sensor values. The situation rules infer the sensitivity situation (emergency, critical, normal, abnormal, alertness and not assigned) according to the behavior, location and time context. The profile rules aim to check the user falling accidents or cardiac problems. The security policy rules are defined on permission, recommendation, obligation and prohibition which are derived according to the defined rules as illustrated in Fig. 7.

7.3 Adaptive Assistance and Decision Making

Once the data are acquired, a query is constructed in order to get back the decision policy which is performed by means of SPARQL query. The caregiver will be notified, the decision will be displayed and consequently, the caregiver will adapt the assistance according to the distress situation, capabilities and user preferences taking into account the user disability impairments.

8 Validation

In this section, we propose an experimental scenario to show the importance of an adaptive and personalized security policy.

Jean is an old person but recently he becomes frailer and can be found him in distress situation (falling) and he live with blindness disability. This situation began from 2 years ago. For this, he needs an automatic assistance by monitoring his daily activities (going back home, taking shower or preparing meals).

Sometimes Jean has the following critical behavior:
He is sitting on a chair in the living room (office), he reads a newspaper (120″)
He gets up and goes to the bathroom and to the toilet (60″)
He leaves the bathroom; he goes to the kitchen to prepare coffee (180″)
He returned to stay in the living room, and he drinks his coffee (120″)

He gets up, he stumbles and he falls and he stays lying down (120″)

The sensed data are injected into the ontology as instances about the defined classes and it makes use the defined rules to infer the appropriate decision and notification, as illustrated in the Fig. 7.

According to the recorded scenario, the person has fallen in the living room when he drank his coffee. The identified parameters are: (fall=1), (activity=14), (posture =1) and (activated devices: IRV6, IRHB). From the sensed data, the rules infer that the user has behavior pattern_5, an emergency situation is identified; the user is located in the living room because the devices (IRV6, IRHB) are activated and the user is noted that did a fall before where the caregiver must be notified to recommend some assistance guidance in vocal form taking into account the user disability (blindness).

9 Analysis and Discussion

The developed security policy is focused on real data recording for setting up the management process and even the validation decision assignment that is depended on the behavior capability. The specificity of our security policy is due to the use of richer contextual data comprising the environment data (location, time) and the body data (fall, pulse, movement). Owing to the multi source data, we are capable to deduce more complex knowledge which are mainly: behavior, profile, and situation. In order to deal with all these heterogeneous data, we have chosen ontologies to implement our proposed model by taking their advantages of modeling, reasoning and querying. The idea in the use of these data is to ensure more personalized services and assistance. Our aim is reached by the mean of the historical behavior and the profile mining. Specially, the present context permits us to react at the right situation and to ensure more adaptive security policy. After many experiments, the framework is sensitive to the increasing instance number defined by contrast it is not important the rule number. The system supports up to 60 instances of the whole entities. In the other side, there is no limitation in the rule number and the time response of the query doesn't depend on the size of the ontology which is averaged to 0.0080 ms. We hope to improve our security policy by exploring the third system ANASON in the platform tele monitoring. So, it is useful to extend the model and adding more data and rules according to each specific situation. In fact, the model is developed to satisfy the doctors needs and the dependent people living alone where the aim is to assist more adequately this specific population. We note that our developed security can greatly used to identify and authenticate the anonymous users by checking out their historical behavior.

10 Conclusion

The paper presents a reactive, a personalized and an adaptive security policy dedicated to the tele-health care assistance for the dependent and frail people needs. The approach is carried out by means of a proposed model and its related architecture. The novelty of our approach is due to the richness of the contextual data acquired from our Tele-monitoring platform by providing both body and environment data by means of RFPAT and GARDIEN systems. The data particularity is due to the detection of critical situation like fall and distress situation, the simple and the complex data are used to develop our security policy. The main steps followed in this work are: sensing data, pattern and behavior extraction, modeling, reasoning and decision making. The derived assistance decisions are mainly: permission, obligation, recommendation or interdiction. The policies are adapted and personalized to the user behavior capabilities and profile.

For further validation of our approach, we intend to work on three improvements. The first one relates to the use of sound data by the integration of the ANASON system in order to study more complex patterns. The second one consists in making the system proactive to predict more contexts. The third one takes into account the outdoor environment (transport or working spaces).

References

1. Marion A, Hersh D, Michael A, Johnson U (2008) Disability and assistive technology systems. In assistive technology for visually impaired and blind people (pp. 1–50). Springer, London
2. Cook DJ, Augusto JC, Jakkula VR (2009) Ambient intelligence: technologies, applications, and opportunities. Journal of Pervasive and Mobile Computing 5(4):277–298
3. Douglas M, Guang-Zhong Y (2009) Body sensor networks for sport, wellbeing and health. In: Sensor networks. Springer, Berlin Heidelberg, pp 349–381
4. Salmeri A, Licciardi CA, Lamorte L, Valla M, Giannantonio R, Sgroi M (2009) An architecture to combine context awareness and body sensor networks for health care applications, in ambient assistive health and wellness management in the heart of the city (icost), pp 90–97. Springer, Berlin Heidelberg
5. Varshney, U. (2009) "Pervasive Healthcare Computing: EMR/EHR", Wireless and Health Monitoring.
6. Atallah, L., Lo, B., Yang, G-Z. (2012). Can pervasive sensing address current challenges in global healthcare?, Journal of Epidemiology and Global Health, (pp. 1– 13)
7. Cavalcante PAA (2012) Réseaux Évidentiels pour la fusion de données multimodales hétérogènes : application à la détection de chutes", Institut Mines Télécom SudParis, thesis reoprt
8. Medjahed, H. (2010) "Distress situation identification by multimodal data fusion for home healthcare tele monitoring", Institut Mines Télécom - Télécom SudParis,thesis report.
9. Steenkeste, F., Bocquet, H., Chan, M., and Vellas, B. (1999). "Remote monitoring system for elders in a geriatric hospital", in

Promoting Independence & Quality of Life for older persons: an international conference on aging Arlington, (pp. 2–4).
10. Baldinger, J.-L., Boudy, J. B., Dorizzi, Levrey, J.-P., Andreao, R., Perpère, C., Delavault, F., Rocaries, F., Dietrich, C., and Lacombe, A. (2004). Tele-surveillance System for Patient at Home: the MEDIVILLE system", in Computers Helping People with Special Needs, (pp. 400–407), Springer.
11. Istrate D, Castelli E, Vacher M, Besacier L, Serignat J-F (2006) Information extraction from sound for medical tele monitoring", information technology in biomedicine. IEEE Transactions 10(2): 264–274
12. Asmidar. A, Roslan. I., Jamilin, J. (2009). A Review on Extended Role Based Access Control (E-RBAC) Model in Pervasive Computing Environment. In International Conference on Intelligent Pervasive Computing, IEEE, (pp. 533–535).
13. Zerkouk, M., M'hamed, A., Messabih, B.(2012) User behavior and capability based access control model and architecture. NetCoM '12 : The Fourth International Conference on Networks & Communications, (pp. 291–299), New-York : Springer
14. Zerkouk M, M'hamed A, Messabih B (2013) A user profile based access control model and architecture. International journal of computer networks & communications (IJCNC) 5(1):171–181
15. M'hamed, A., Zerkouk, M., El Husseini, A., Messabih, B., El Hassan, B. (2013). Towards a context aware modeling of trust and access control based on the user behavior and capabilities . ICOST '13 : 11th International Conference On Smart homes and health Telematics, (pp. 69–76). London : Springer
16. Dey A (2001) Understanding and using context. Journal of Personal and Ubiquitous Computing 5(1):4–7
17. Zhang D, Huang H, Lai CF, Liang X, Zou Q, Guo M (2013) Survey on context-awareness in ubiquitous media. Multimedia Tools and Applications 67(1):179–211
18. Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. (2013). Context Aware Computing for The Internet of Things: A Survey. Journal of IEEE COMMUNICATIONS SURVEYS & TUTORIALS, (pp. 1–41)
19. Chaari T, Ejigu D, Laforest F, Scuturic VM (2007) A comprehensive approach to model and use context for adapting applications in pervasive environments. J Syst Softw 80(12):1973–1992
20. Hong J, Suh E, Kim K, Kim S (2009) Context-aware system for proactive personalized service based on context history, journal. Expert Systems with Applications 36(4):7448–7457
21. Riboni, D., Bettini, C., "OWL 2 modeling and reasoning with human activities, In *Pervasive and Mobile Computing*", pp.(*379–395)* (*2011)*
22. Chen L, Nugent C (2009) Ontology-based activity recognition in intelligent pervasive environments. International Journal of Web Information Systems 5(4):410–430
23. Kadouche R, Pigot H, Abdulrazak B, Giroux S (2010) Support vector machines for inhabitant identification in smart houses. In ubiquitous intelligence and computing, (pp. 83–95). Springer, Berlin Heidelberg
24. Copetti A, Leite JCB, Loques O, Neves MF (2013) A decision-making mechanism for context inference in pervasive healthcare environment. Decis Support Syst 55(2):528–537
25. Wrona, K., and Gomez, L. (2005). Context-aware security and secure context-awareness in ubiquitous computing environments, XXI Autumn Meeting of Polish Information Processing Society, (pp. 255–265).
26. Sadat Emami S., Amini M., Zokaei S.(2007). A Context-Aware Access Control Model for Pervasive Computing Environments. International Conference on Intelligent Pervasive Computing, IEEE, (pp. 51 – 56).
27. Yao. H, Hu. H, Huang B., Li. R. (2005). Dynamic Role and Context Based Access Control for Grid Applications, Proc. Of The Sixth International Conference on Parallel and Distributed Computing, Applications and Tecology, (pp. 404 – 406).
28. Choi, J., Kang, D., Jang,H., and Eom, Y.I. (2008) Adaptive Access Control Scheme Utilizing Context Awareness in Pervasive Computing Environments, In IEEE International Conference Performance, Computing and Communications. (pp 491 – 498).
29. Sliman L, Biennier F, Badr Y (2009) Security policy framework for context-aware and user preferences in e-services. J Syst Archit 55: 275–288
30. Qin W, Shi Y, Suo Y (2007) Ontology-based context-aware middleware for smart spaces. Tsinghua Science and Technology 12(6):707–713
31. Favela J (2013) Behavior-aware computing: applications and challenges. Journal IEEE Pervasive Computing 12(3):14–17
32. R. Mayrhofer, H. radi, and A. Ferscha. (2004). Recognizing and predicting context by learning from user behavior," Radiomatics: journal of Communication Engineering, special issue on Advances in Mobile Multimedia, 1, 30–42.
33. Weka, http://www.cs.waikato.ac.nz/ml/weka/
34. Protégé, http://protege.stanford.edu/
35. Pellet, http://clarkparsia.com/pellet/
36. Jess, http://www.jessrules.com/jess/