

iWebCare: an Integrated Web Services Platform for the Facilitation of Fraud Detection in Health Care e-Government Services

Thomas Dimakopoulos, Kyriakos A. Kassis, Efstratios Nikoloutsos

Agilis SA Statistics & Informatics

Akadimias 96-100

106 77, Athens, Greece

{Thomas.Dimakopoulos, Kyriakos.Kassis, Stratos.Nikoloutsos}@agilis-sa.gr

Panos Alexopoulos, Panos Georgolios, Kostas Kafentzis,

IMC Research,

Fokidos 47, Athens, Greece

{palexopoulos, kkafentzis, pgeorgolios}@imc.com.gr

Xanthi Benetou, Tassos Tagaris

Institute of Communication and Computer Systems, National Technical University of Athens,

Zografou Campus, Athens, Greece

{xbenetou, tassos}@biomed.ntua.gr

Abstract

The iWebCare project (EC Fund: FP6-2004-IST-4-028055) aims at designing and developing a flexible fraud detection web services platform, which will be able to serve e-government processes of fraud detection and prevention, in order to ensure quality and accuracy and minimize loss of health care funds. The approach the project adopts involves the introduction of a fraud detection methodology combining business process modelling and knowledge engineering as well as the development of an integrated fraud detection platform combining an ontology-based rule engine and a self-learning module based on data mining offered together as an advanced and flexible web-based fraud detection service.

iWebCare promotes interoperability in two ways; through its generic and extendible ontological framework that can be adapted to virtually any e-government process which needs to be examined for fraud and through its technical architecture which is based on web services and facilitates the cooperation with other existing e-government systems. The users of the iWebCare platform, who in the course of the project will be authorised actors involved in the health care business, will be able to access the iWebCare services via the Internet. They will be able to detect erroneous or suspicious records in submitted health care data sets, ensuring homogeneity and consistency and promoting awareness and harmonization of fraud detection practices among health care systems in the EU.

1. Introduction

Fraud is an issue with psychological, economic and legal ramifications for both the public and private sector spanning geographic regions. The last EHFCN (European Healthcare Fraud and Corruption Network – <http://www.efhcn.org>) conference produced agreement among members on a common definition of fraud: “Civil fraud is the use or presentation of false, incorrect or incomplete statements and/or documents, or the non-disclosure of information in violation of a legally enforceable obligation to disclose, having as its effect the misappropriation or wrongful retention of funds or property of others, or their misuse of purposes other than those specified”.

Other definitions of fraud present it as a type of corrupt conduct and risk for organizations that cannot be eliminated. In broader terms fraud is the deliberate and premeditated act perpetrated to achieve gain on false ground. The effects of fraud are economic (reduced operational effectiveness), legal (depriving resources from rightful claimants) and psychological (damage moral and reduce confidence in government).

The consequences of e-government fraud are numerous. For example, in the healthcare domain fraud causes the raise of the cost of health care benefits for everybody. According to the Deputy Health Minister of Scotland Lewis Macdonald (<http://www.scotland.gov.uk>) the potential losses to healthcare across Europe from fraud and corruption are estimated to be at least 30 billion euros each year and may be as high as £100 billion. For most employers, fraud increases the cost of providing benefits to their employees and, therefore, their overall cost of doing business. That translates into higher premiums and out-of-pocket expenses as well as reduced benefits or coverage. Healthcare fraud, can also impact the quality of the received care. When dishonest providers put greed ahead of care, proper diagnosis and treatment may be ignored and patients may be put at risk solely to generate higher dollar claims.

The approaches that are adopted for fighting fraud are common between the various e-government domains and include:

- The creation of anti-fraud and anti-corruption culture among service providers, healthcare suppliers, healthcare payers, healthcare users and ultimately among citizens.
- The use of all possible presentational and publicity opportunities to act as a deterrent to those who are minded to engage in e-government fraud or corruption
- The use of effective prevention systems so that when fraudulent or corrupt activities are attempted, they will fail.
- The professional investigation of all cases of detected or alleged fraud and corruption.
- The imposition, where fraud and corruption is proven, of appropriate sanctions – namely civil, criminal and/or disciplinary processes. Multiple sanctions should be used where possible;
- The seeking of financial redress in respect of resources lost to fraud and corruption and the return of recovered resources to the area of patient care or services for which they were intended;
- The development of a European common standard of risk measurement (baseline figures), with annual statistically valid follow up exercises to measure progress in reducing losses to fraud and corruption throughout the EU.
- The use of detection systems that will promptly identify occurrences of healthcare fraud and corruption

Our interest towards fraud detection lies into the technological aspect of fraud fighting and in particular in the area of fraud detection systems. In this area organizations and agencies seek multiple layers of fraud detection methods and tools ranging from rule-based systems ([8]) to predictive modelling approaches. We believe that in all these methods and approaches, ontologies can play a significant role as they have a lot to offer in terms of interoperability, expressivity and reasoning.

In this paper we intend to describe a reference architecture for the creation of a fraud detection platform and to illustrate a methodology for building domain specific fraud ontologies. This methodology is accompanied and supported by a generic fraud ontology which acts as a reference framework and a basis for building such specialized ontologies.

2. iWebCare Integrated Web Services Platform

The iWebCare platform will be accessible via Internet from authorised actors involved in the health care business (general inspectors of health care, social security funds, internal auditing departments in public hospitals, etc). They will be able to detect erroneous or suspicious records in submitted health care data sets, ensuring homogeneity and consistency and promoting awareness and harmonization of fraud detection practices among health care systems in the EU. The service will be developed according to the Service-Oriented Architecture approach that allows for easy access and seamless integration with legacy systems.

The guiding design rational behind the platform's architecture is to facilitate interoperability and to allow for extensibility while preserving a considerable degree of implementation-platform-independence. Key factors to this objective are the adoption of widely accepted standards (XML, SOAP, Web Services, WSDL, J2EE) as well as emerging standards (SOA and BPEL) and the use of Open Source Software. In parallel, IDA and PEGS as well as knowledge and expertise acquired from other R&D projects (mainly GovML and TERREGOV) have been considered during architectural analysis.

2.1. iWebCare generic approach

The applicability of the architectural approach in other application domains is depicted in figure 1. The various data elements that will be “scanned” from the iWebCare platform as suspicious for potential fraud are considered as application specific. These elements are in the form of multidimensional files structured in the form of XML documents. These XML documents are fed from the different actors to the iWebCare service and their consistency is checked against the concepts that are contained in the ‘health care ontology’ (considered as domain specific since it is specifically designed in order to accommodate concepts from the domain of health care). The lower level of the persistence layer includes the rules that are expressed as variables (of different type such as nominal, ordinal, composite, text, etc.) and domains of definition of these variables. So, the information that relies in the rules repository can be considered as independent from the specific domain and can be also applied in other e-gov domains that are likely to be fraudulent (financial audits, tax, customs, etc.)

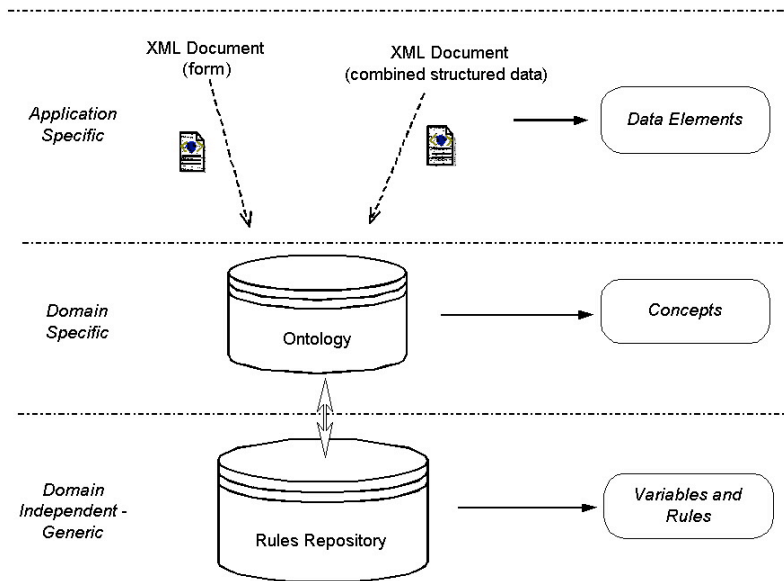


Figure 1. Generic approach for covering other application domains

2.2. Main Architectural Considerations

The most central role, in the system’s design, of all the mentioned technologies is that of the Web Services technology. The Integrated Web Services Health Care Fraud Detection Platform can be conceived, from a high level point of view, as a set of web services cooperating in order to accomplish a main goal; the detection of suspicious (either erroneous or fraudulent) data submissions. Behind the layer of those web services lies a layer of pure programmatic modules implementing the business logic of the services and further behind lies a persistence layer responsible for preserving all those pieces of information that are required to be permanent in the system. On top of these layers lies a web-based user interface layer for the maintenance of the whole system. Hence the Platform is a multi-layered system.

The system architecture consists of the following basic sub-systems:

- A *web service client* (e-gov application) that is installed in the operating environment of the health care data provider and performs preparation of the datasets (in XML format) that will be submitted to the iWebCare platform
- A central *iWebCare Web Service* which is capable of interfacing (through SOAP) with the eGov applications, receiving and validating the XML incoming datasets. The module is also responsible for authorization and authentication of the users
- A *fraud detection engine (FDE)* module that is responsible for using domain specific rules in order to validate a submitted dataset. The domain specific rules are provided by the ontology module to the FDE. Thus the FDE is not domain specific. Another responsibility of the FDE module is the production of reports that present the results of the fraud detection process.

- The purpose of the *Self Learning Module Web Service* (SLWS) module is to create/update rules for a certain domain. This is achieved by applying specialized data-mining algorithms and by learning from error-free and fraudulent datasets. As a result, the self-learning module interfaces with the ontology module in order to update the rules repository.
- A specific *Health Care Ontology (HCO)* which represents the domain-dependent. It is responsible for mapping domain concepts with XML datasets and with variables and rules of the rules repository. The ontology module is responsible for interacting with the rules repository.
- A *repository of validation rules* which is responsible for managing fraud detection rules and rulesets and their associated metadata. Rules are expressed in Specific Rule Language (XML rule language) or in Binary Models. The module is maintained by a web interface provided and it is also fed by rules created by the self-learning module and forwarded via the ontology module.

These modules interact between them via clear SOAP interfaces. iWebCare architecture has been graphically depicted in package, component and sequence diagrams that comply with the adopted software development methodology (RUP), utilise UML notation and have been generated using standard CASE tools (Enterprise Architect).

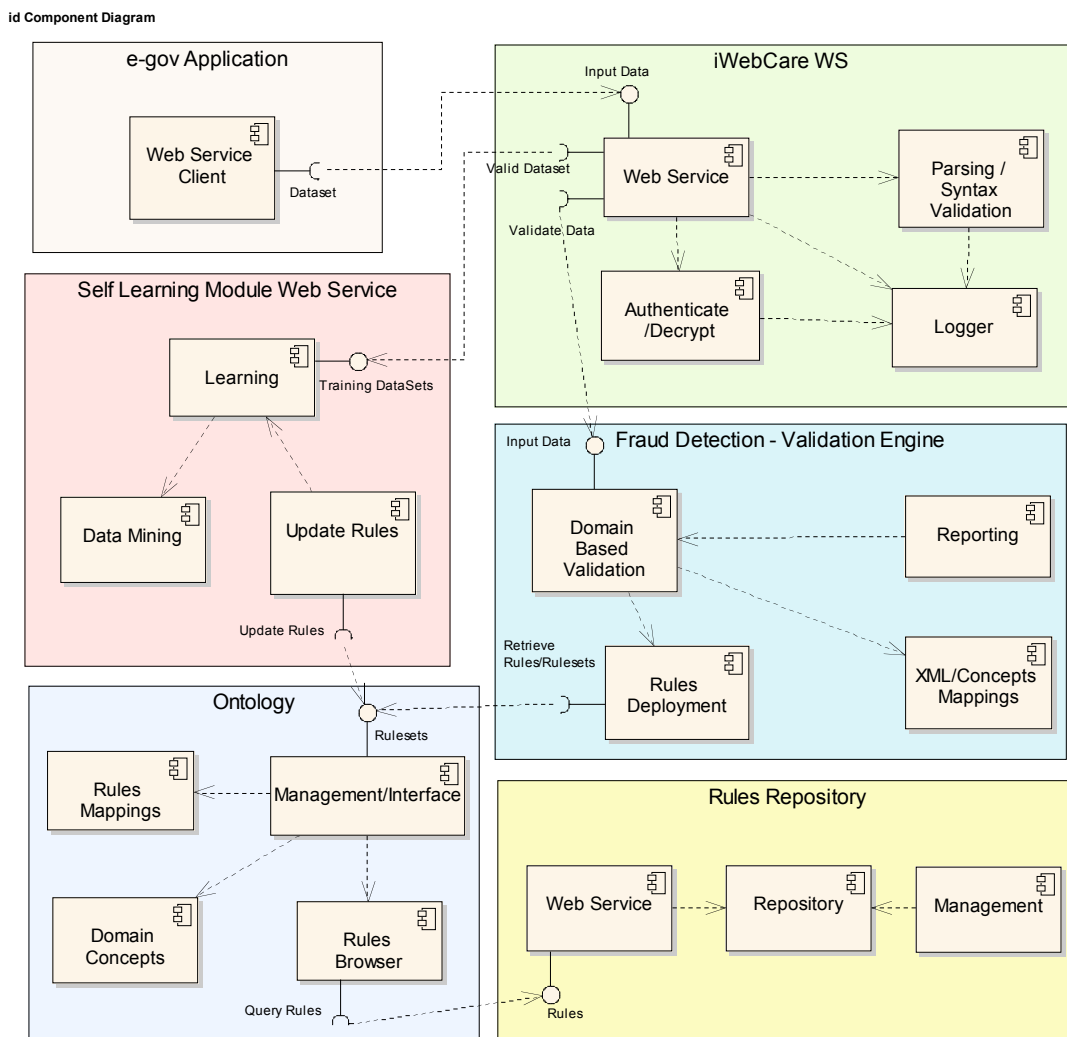


Figure 2. Component Diagram of the iWebCare platform

2.3. Security And Data Protection issues

The iWebCare platform handles very personal and sensitive data. For example the prescription details have a collection of information about the patient, the doctor and the pharmacist and the procurement details address and name from the employees and the organizations.

The project eGOV handle public information, the communications between the client and the web services is based on XML messages. The similarity of the eGOV and iWebCare projects is very close on the XML messages, the architecture and the Security requirements. The eGOV project performed a questioner to collect data to determine how important is the data security for the public and the governments. The results are show below and the whole section is a part of the document eGOV-D111. Public services usually tend to have several security and privacy implications. The majority in both groups regarded security clearly as an important issue and hardly any of the interviewees felt that it was a matter of little importance (Figure 3).

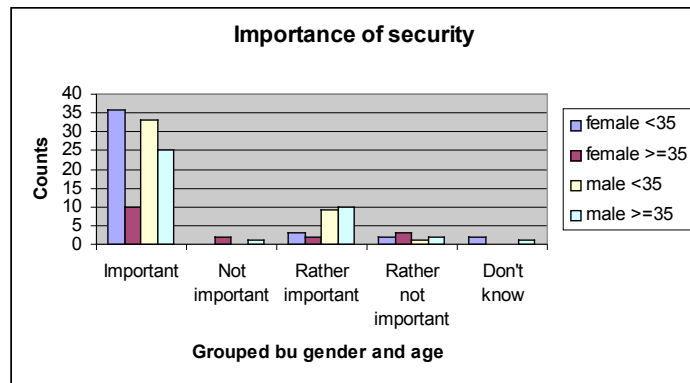


Figure 3. Importance of security issues according to citizens

Using Components from Terregov Security Module the iWebCare can handle authorization and authentication using Certificates and Open LDAP server. Also the extensive use of XML Signatures and XML Encryption is applied in all the XML Messages to maximize data protection and data privacy.

2.4. Data Mining Approach

Data mining is used in the iWebCare project to automatically extract structures from data and generate predictions on new fraud instances in order to assist fraud inspectors in identifying novel cases of fraud and helping them to concentrate their search on the most suspicious cases in large databases of possible fraud cases.

Data Mining allows to automatically extract structures from data, and generate predictions on new fraud instances in order to assist fraud inspectors in identifying novel cases of fraud and helping them to concentrate their search on the most suspicious cases in large databases of possible fraud cases. Data mining techniques and approaches that are used in the iWebCare project are based on the CRISP process model (<http://www.crisp-dm.org>), which defines the steps mentioned below. These steps form an iterated process, in which previous decisions are frequently re-evaluated under the light of new insights as the process and hence the understanding of the structures behind the data increases:

1. **Business Understanding:** understanding the application domain. Identifying domain experts, understanding the problem-relevant domain-specific vocabulary, identification of important background knowledge. In particular, understanding the goal of the analysis. In the context of the iWebCare project, business understanding is formally implemented in the Business Process Models.
2. **Data Understanding:** understanding the data set that is being examined, i.e. its semantic, variable descriptions, specific data formats. This task is heavily interconnected with business understanding. In the iWebCare project, ontologies are used to give a formal description of data sets and allow for data understanding to operate on more a formal level, thereby reducing the overhead in the data understanding phase for similar data sets.

3. **Data Preparation:** converting the data from the application-specific format into a format needed for the modeling step, cleaning the data, computation of derived features, feature and subset selection.
4. **Modeling:** the actual analysis of the data using algorithms from Machine Learning or Statistics.
5. **Evaluation:** checking the correctness and applicability of the model in the application context with respect to the goals of the analysis task.
6. **Deployment:** integration of the discovered knowledge in the user domain. Practical application of the model, including pre-processing steps. In iWebCare, the deployment step will consist of the final fraud detection platform

The modeling step has been in the focus of research in Machine Learning and Statistics. Many data analysis algorithms have been developed. Readily available open-source environments like R (<http://www.R-project.org>) Yale (<http://www.sf.net/yale/>), or Weka (<http://www.cs.waikato.ac.nz/~ml/weka/>), contain a large, steadily growing variety of data mining methods. The other steps in the KDD process are usually treated in a more ad-hoc manner, even though it is widely acknowledged that these steps are very much responsible for the success of Knowledge Discovery projects;

2.5. Fraud Ontology

2.5.1. Role of the ontology

Ontologies can play a vital role in both the rule-based and data mining fraud detection approaches. Apart from the rules, a really important component of a rule-based system is its knowledge base. An important issue in knowledge bases is the knowledge representation paradigm they adopt as the latter influences the type and quality of reasoning that can be made within the knowledge-based system.

Ontologies are knowledge models that represent a domain and are used to reason about the objects in that domain and the relations between them ([12]). Thus, a knowledge base may use an ontology to specify its structure (entity types and relationships) and its classification scheme. In such a case, the ontology, together with a set of instances of its classes constitutes the knowledge base.

The use of ontologies and ontology-related technologies for building knowledge bases for rule-based systems is considered quite beneficial for two main reasons:

- Ontologies provide an excellent way of capturing and representing domain knowledge, mainly due to their expressive power.
- A number of well established methodologies, languages and tools ([10]) developed in the Ontological Engineering area can make the building of the knowledge base easier, more accurate and more efficient, especially in the knowledge acquisition stage which is usually a bottleneck in the whole ontology development process.

Ontologies are also very important to the data mining area as they can be used to select the best data mining method for a new data set. When new data is described in terms of the ontology, one can look for a data set which is most similar to the new one and for which the best data mining method is known, this method is then applied to the new data set. In this way, there is no need for trying out every known method on the new data set, but the one (or few) that is most promising can be directly selected.

2.5.2. Development Methodology

The methodology we follow for building our fraud detection ontology is based on the suggestion that fraud is actually an operational risk for an organization and as such it should be treated through a risk management process. Risk management (RM) ([11],[15]) is the process whereby public organizations may methodically address the risk associated to their activities with the goal of achieving a sustained benefit within each activity and across their portfolio of activities. The focus of RM is to identify, measure and treat these risks in order to reduce their probability of happening.

In a similar fashion, our methodology defines a process for identifying, measuring and treating fraud in the context of e-government services. This process comprises three steps: a) establishment of the fraud context, b) identification of fraud within this context and c) transformation of this information into an ontological model.

Establishment of the fraud context within an organization involves defining the type of fraud the organization wishes to fight and identifying the business processes fraud occurs upon. This is done through a business process modelling procedure that records the fraud susceptible business processes of the organization and their context. On the other hand, fraud identification involves the description of potential fraud cases that could occur within the

organization and of corresponding detection methods. This identification is done in two ways, namely by acquiring organizational knowledge regarding fraud from experts and by utilizing data mining methods in order to extract unknown fraud patterns.

The final step of the methodology involves transforming the knowledge derived from the two previous steps into an ontology so that it can be utilized by fraud detection systems. This step usually requires following some formal knowledge engineering procedure.

Obviously, these three steps should be repeated for each different domain or case study meaning that the proposed methodology is an iterative procedure. In order to minimize the effort required in each iteration we created a generic fraud ontology that acts as the basis for building domain specific fraud ontologies.

2.5.3. Ontology architecture

The fraud ontology is practically a generic framework for defining domain and case specific fraud ontologies that are to be used in ontology-based fraud detection systems. Among others, this framework should be easily adaptable and extendible to different domains and types of fraud. This was made possible through a multi-layer architectural design of the fraud ontology that makes the latter adaptable, extendible and to a significant degree reusable.

This architecture consists of three independent but interconnected layers each one defining its own set of ontologies (see Figure 4)

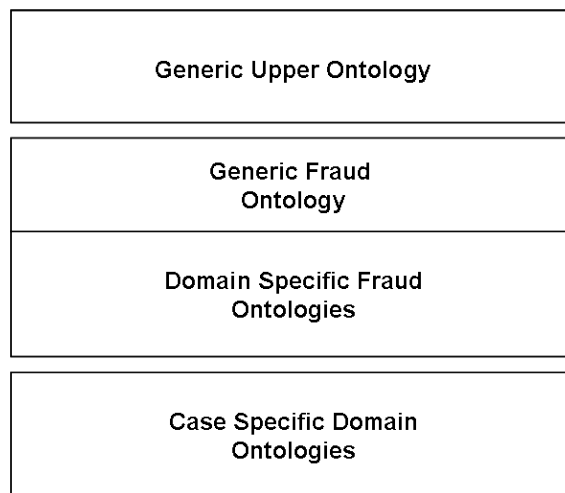


Figure 4. Fraud Ontology Layered Architecture

The bottom layer (or case specific layer) consists of domain ontologies which model the business processes of the specific cases that are examined for fraud, e.g. a specific organization in social security. The concepts and relations contained in these ontologies are practically derived from the business process analysis of the particular case and from the knowledge of the corresponding domain experts. The main purpose of the case specific layer is to provide the basic knowledge on which fraud detection rules or data mining techniques are going to be based on. Reusability of existing ontologies is applicable not only in the sense of best practices transfer from one case to another.

The middle layer (or fraud domain layer) comprises of ontologies which model fraud related knowledge such as fraud types and fraud detection processes. The content of these ontologies reflects the knowledge of fraud domain experts and it is primarily used as the basic means for expressing the fraud detection rules that these experts provide.

The middle layer could be considered as having two sublayers, a domain-specific one and a generic one. The domain-specific sublayer models the fraud characteristics of the domain at hand, e.g. social security or public procurement. The generic sublayer provides more abstract and generic knowledge that constitute the basis for applying knowledge-based approaches into virtually any fraud susceptible field. A small fraction of the generic fraud ontology is depicted in figure 5. As it can be seen from this diagram the fraud ontology contains concepts representing fraud actors, fraud cases etc and relations linking actors with motivations and cases with actors.

Finally, the upper layer, namely the Generic Upper Ontology, captures generic and domain-independent knowledge that helps minimize redundancy and duplication of knowledge within the overall ontology.

The most important of the advantages such a layered architecture provides, are the following:

- Modularity: When a large-scale ontology is composed out of smaller ontologies then its development and maintenance are easier and more efficient.
- Reusability: When the independent parts of the ontology are well defined and separated then it is highly possible that these parts can be reused in other similar applications.
- Extensibility: With the layered architecture, and more specifically with the generic ontologies, it is far easier to extend the ontology so that it can cover domains of application other than the existing ones.

2.5.4. Case study – TSAY

TSAY is the insurance body of all healthcare professionals in Greece and its main focus concerning healthcare fraud is detected in the prescription reimbursement domain. Since TSAY is a health insurance body organization, one of the most common services it offers to its members is the payment of the drugs they consume. This payment has mainly the form of reimbursement meaning that a TSAY's member purchases the drugs s/he needs from a pharmacist paying only a percentage of the actual cost and then the pharmacist claims the rest of the money from TSAY.

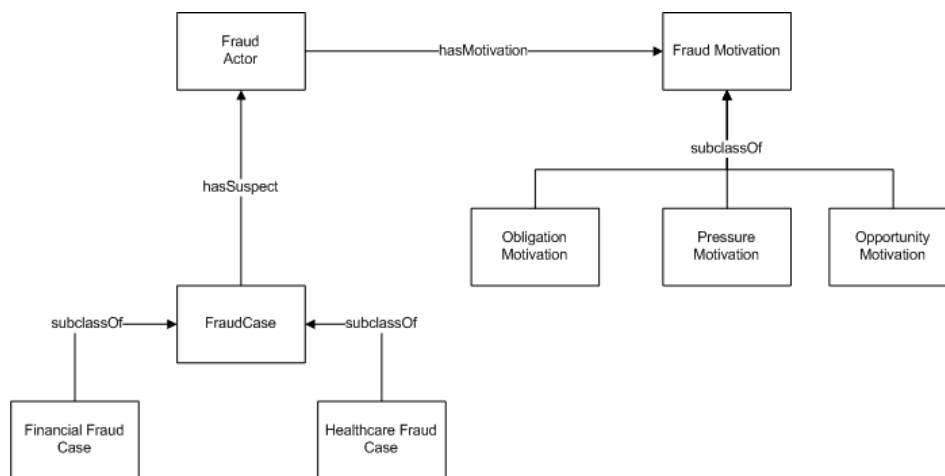


Figure 5. Generic Fraud Ontology

However, it is often the case that the prescriptions TSAY is asked to reimburse contain erroneous or deliberately inaccurate data so that larger sums of money can be claimed or inappropriate drugs can be prescribed. Or, it is possible that prescriptions contain data which when viewed isolated do not indicate fraud but when considered along with other prescriptions they form some suspicious pattern of misbehaviour.

Of course, the cases targeted for detection do not necessarily constitute fraud from a legal point of view because it might be that the inaccurate data are due to human error or that the objectionable misbehaviour can be explained by reasons that are not obvious. However, even then, the need for detection remains strong since fraud in this case can be considered to be synonymous to waste in the form of monetary losses from the reimbursement of inappropriate prescription.

The rules identified comprised two main categories, namely auditorial rules and medical rules. Auditorial rules try to detect incomplete prescriptions and invalid or miscalculated data while medical rules try to detect prescriptions in which the data are inconsistent from a medical point of view.

An example of an auditorial rule is when a prescription contains no diagnosis at all for the drugs that it prescribes and an example of a medical rule is when the diagnosis written on the prescription is not included in the indications of the prescribed drugs.

In the case of TSAY the fraud domain is that of prescriptions. According to our methodology the first required step was the establishment of the fraud context namely the description of the prescription domain. Thus, a business process modelling procedure was performed and a complete business process model of the prescription domain was developed. The high level processes contained in that model were:

- The issuance of prescription booklets to TSAY members by the Fund
- The issuance of prescriptions by doctors to patients that own these booklets
- The inspection of prescriptions by the ministry of health.

- The filling of members' prescriptions by the pharmacists
- The reimbursement process of TSAY for filled prescriptions.

According to the business process analysis, prescription issuance, inspection and filling occur outside the organization and TSAY has no control over the events that take place there. This meant that these processes could not be a part of TSAY's fraud detection mechanism. On the other hand, the prescription reimbursement process was considered perfect for applying fraud detection methods and rules.

These methods and rules (the TSAY fraud identity or the second step of the methodology) were provided by people involved in the prescription process, namely doctors, pharmacists, TSAY's inspectors (patients could also be included).

The rules identified comprised two main categories, namely auditorial rules and medical rules. Auditorial rules try to detect incomplete prescriptions and invalid or miscalculated data while medical rules try to detect prescriptions in which the data are inconsistent from a medical point of view.

An example of an auditorial rule is when a prescription contains no diagnosis at all for the drugs that it prescribes and an example of a medical rule is when the diagnosis written on the prescription is not included in the indications of the prescribed drugs.

The third step of applying our methodology was the actual building of the TSAY specific ontologies. These ontologies are the TSAY domain specific fraud ontology and the TSAY case specific domain ontology.

The first contains the knowledge regarding the prescription domain and utilizes the business process model created in the previous steps. The second models the fraud types and fraud detection methods and rules for the prescription domain and utilizes the knowledge derived from the domain experts. Both are built under the generic upper and fraud ontologies so that the development effort and knowledge redundancy are minimized. Figures 6 and 7 present fractions of these two ontologies.

Figure 6 depicts the refinement and specialization of a generic fraud case to the social security domain and especially to prescription related fraud. Several fraud cases identified in step 2 of the methodology are represented as concepts in the domain ontology.

Figure 7 presents the representation of a prescription as viewed by TSAY experts. The different concepts – entities, their characteristics and their relationships are depicted in the ontological model. It is clear from the figure that even this particular part of the TSAY case specific ontology can be transferred and applied to another organization that faces a similar increased risk in its prescription process with minor adaptation.

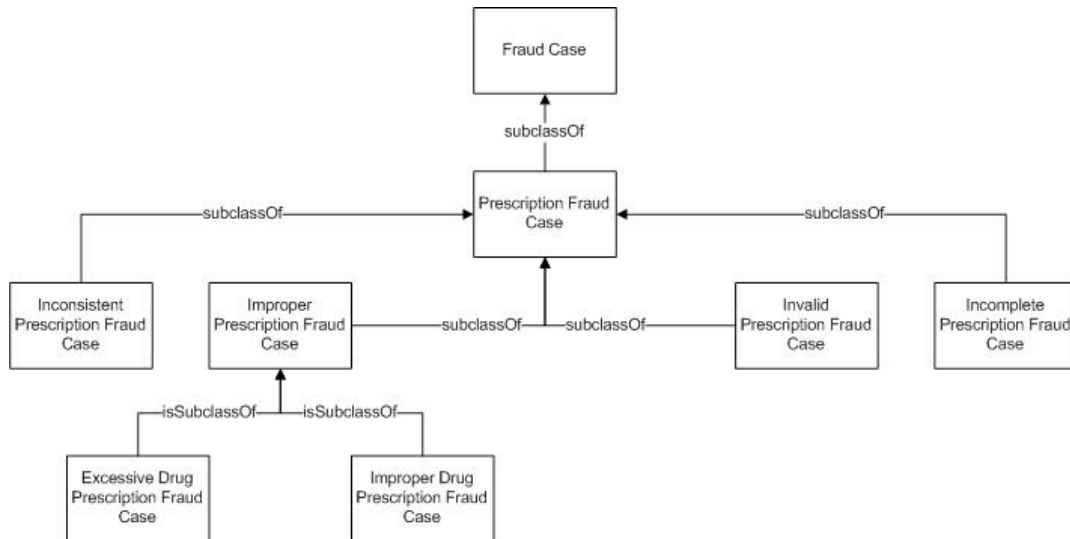


Figure 6. TSAY Domain Specific Fraud Ontology

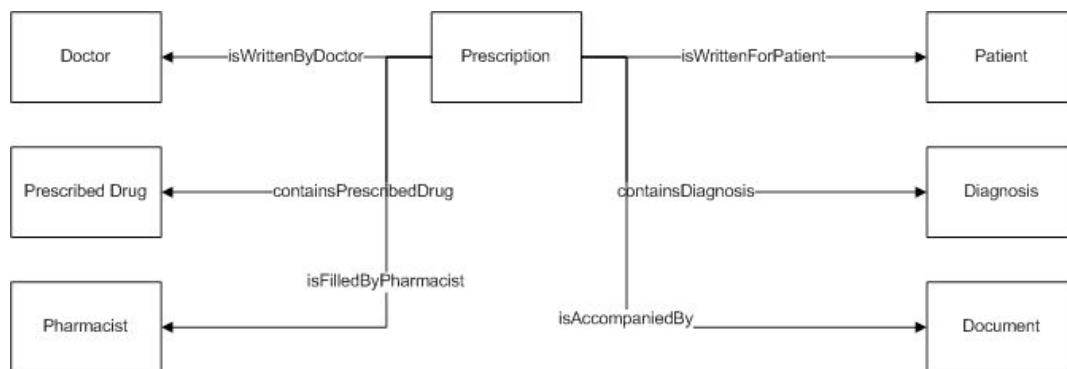


Figure 7. TSAY Case Specific Domain Ontology

3. Conclusions

The objective of this paper was to present the minimum requirements in order to deploy an integrated web services platform which will improve the e-government processes of fraud detection in the EU health care industry by enhancing the identification of fraud cases through the utilisation of data mining techniques and by developing an advanced and flexible, web-based fraud detection service.

The applicability of the platform will be assessed through the execution of two pilot applications at the user's sites (one at NHS UK and one at TSAY Greece). Identification of fraudulent cases in real working conditions will be done and the technical work performed will be validated against these actual pilot cases. The first results of the assessment are expected in 2008.

4. Acknowledgments

The work presented in this paper is funded by European Commission (FP6-2004-IST-4-028055).

5. References

- [1] IDABC - Content Interoperability Strategy, Working paper, September 2005
- [2] IDABC - European Interoperability Framework For Pan-European Government Services (version 1.0), EC 2004.
- [3] The Web Services-Interoperability Organization (WS-I), Basic Profile version 1.1, Final material (10-04-2006) available at <http://www.ws-i.org/Profiles/BasicProfile-1.1.html>
- [4] Inspector IST project (IST-2000-26347) Deliverable D1.2 A data and process model of the architecture of the validation system,
- [5] Bass L., Clements P., Kazman R. Software Architecture in Practice, Addison Wesley, April 2003.
- [6] Bass L., Clements P., et al., Documenting Software Architectures, Addison Wesley, May 2003.
- [7] Baader F., Calvanese D., McGuinness D. L., Nardi D., Patel-Schneider P.F.: The Description Logic Handbook: Theory, Implementation, Applications. Cambridge University Press, Cambridge, UK, 2003.
- [8] Belhadji, B. & Dionne, G., 1997. Development of an Expert System for Automatic Detection of Automobile Insurance Fraud, Ecole des Hautes Etudes Commerciales de Montreal- 97-06, Ecole des Hautes Etudes Commerciales de Montreal-Chaire de gestion des risques.
- [9] Blackburn, Patrick, Maarten de Rijke, and Yde Venema (2001) Modal Logic. Cambridge Univ. Press
- [10] Gomez-Perez Asuncion, Oscar Corcho, Mariano Fernandez-Lopez (2004) Ontological Engineering. *Springer-Verlang London Limited*
- [11] Crockford, Neil (1986). An Introduction to Risk Management (2nd ed.). *Woodhead-Faulkner. 0-85941-332-2*
- [12] Gruber TR (1993) A translation approach to portable ontology specification. *Knowledge Acquisition* 5(2):1999-220
- [13] Hand D., Mannila H., Smyth P. (2001). Principles of Data Mining. *MIT Press, Cambridge, MA*
- [14] Kerremans, Koen, Tang, Yan, Temmerman, Rita and Zhao, Gang (2005). Towards Ontology-based E-mail Fraud Detection. In: C. Bento, A. Cardoso and G. Dias, (eds.) Proceedings of EPIA 2005 BAOSW Workshop of 12th Portuguese conference on AI, Covilha, Portugal, p. 106-111.
- [15] Lam, James (2003). Enterprise Risk Management: From Incentives to Controls. *John Wiley. ISBN-13 978-0471430001*
- [16] The Web Services-Interoperability Organization (WS-I), Basic Security Profile version 1.0, Working Group Draft (17-08-2006) available at <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>