12th IMEKO TC10 Workshop on Technical Diagnostics
New Perspectives in Measurements, Tools and Techniques for Industrial Applications
June 6-7, 2013, Florence, Italy

Detection and measurement of information system risks through adaptive management diagnostic expert systems

Justinas Janulevičius[1], Lauryna Šiaudinytė[2], Antanas Čenys[3], Nikolaj Goranin[4]

[1] *Vilnius Gediminas Technical University, Research Laboratory of Security of Information Technologies, Saulėtekio al. 11, Vilnius, Lithuania, e-mail: justinas.janulevicius@vgtu.lt*
[2] *Vilnius Gediminas Technical University, Institute of Geodesy, Saulėtekio al. 11, Vilnius, Lithuania, e-mail: lauryna.siaudinyte@vgtu.lt*
[3] *Vilnius Gediminas Technical University, Research Laboratory of Security of Information Technologies, Saulėtekio al. 11, Vilnius, Lithuania, e-mail: antanas.cenys@vgtu.lt*
[4] *Vilnius Gediminas Technical University, Research Laboratory of Security of Information Technologies, Saulėtekio al. 11, Vilnius, Lithuania, e-mail: nikolaj.goranin@vgtu.lt*

Abstract. Current growth of usage of IT systems in almost every field of industry causes rapid optimization of production and maintenance of goods and processes. Nevertheless, wider usage of automated IT systems has it's drawbacks as well: while most of the IT solutions fully exist in an online environment, certain risks for assets stored within the systems exist. Diagnosing and measuring damages, generated by harmful events can have a strong impact on further evolution of the owners, therefore it is very important to assess the possible risks and apply preventive actions prior to their occurrence. Moreover, risk assessment is an extremely diligent process, requiring much expertise and estimating every possible event and it's possibility. Since this process can easily be described as a complex decision-tree, a rule-based expert system can be facilitated to generate the needed expertise on risk assessment. The precision of risk measurement can be increased by using continuous reasoning instead of discrete. Fuzzy-logic based reasoning is proposed instead of Boolean. Possible IT risks vary depending on the technologies popular at given time, so this type of data is considered as sensitive. Therefore it must have a possibility to be updated at any time to provide the end-user with the most actual data. This leads to proposition of an adaptive hybrid fuzzy-logic and rule-based expert system for preventive early diagnostics of threats and measurement of risk of IT assets.

I. Introduction

Constantly growing demand for IT systems in most fields of activity comes with a great deal of following problems. Not only is it very important to convert all of the previously acquired and used information to a form, suitable for the IT system, but also a great deal of effort has to be spent to ensure the safety of data, stored in such systems. Appropriate and on-time diagnostics of vulnerabilities is the key factor for ensuring proper functioning of any system [3].
While there have been a number of attempts of introducing diagnostic systems to data risk assessment, they were either adapted for a narrow field of application or came as commercial products. The main aim of this research is to develop a model for a flexible, adaptive diagnostic expert system. The main field of the design is early diagnostics and measurement of threat for automated risk assessment systems, facilitating expertise. Nevertheless such design can be easily implemented for many diagnostic systems, including automated self-diagnostics of complex mechatronic systems as well as decision support solutions.

II. Information risk assessment

Data, regardless it's type or format, faces threats of confidentiality, integrity and availability [2]. Therefore to eliminate or minimize the effect of such threats certain risk assessment methodologies exist. The process of risk management includes identification of assets, threats, vulnerabilities, threat probabilities and damage volume. Given this data it is possible to measure risk, that is considered as threat probability multiplied by the damage volume. Knowing the risk allows optimal application of mitigation means.
In this context, threat is considered to be any danger given asset is facing with possible harm. Such threats can either be of intentional or accidental nature. Technical documentation usually describes threat as “a potential cause of an incident, that may result in harm of system and organization [6]”.
Information risk assessment is a complex multi-perspective process of evaluating possible cases of damages. It is

the first step in risk management process. It consists of definition of quantity and quality values for each situation and identified threat. Risk assessment process follows a certain pattern consisting of threat identification, threat probability identification, assets sensitivity determination, extraction of critical values and controls. Although patterns for risk assessment exist, this process is very sensitive and must be adjusted to every individual situation. Therefore IT risk assessment is a process requiring expertise and expert knowledge. While the pattern of this process can be easily described in a formal manner, it gives an assumption for usage of intelligent computer agents to perform this process. A system of intelligent computer agents forms an intelligent autonomous reasoning expert system fully compatible of taking over all the processes in risk assessment.

III. Expert system as an early diagnostic tool

A. Hybrid rule-based expert systems incorporating fuzzy logic

Though a classic expert system is considered to perform reasoning based on the rule-based concept it shows one major drawback considering the accuracy of the generated inferences: this type of system operates in Boolean logic, providing only two options (*TRUE* or *FALSE*) for a conclusion, while human-like reasoning usually is not that strict. This means that a human expert performing a task of such kind would take in a higher number of options into account for each situation, giving more precise evaluation. So the expert system needs an ability to have transitional weights. This means that instead of values *TRUE* (weight - 1) or *FALSE* (weight – 0) there have to be ones like *MOST LIKELY, MAYBE, OCCASIONALY, ALMOST NEVER*, etc. This is where the concept of fuzzy logic comes to use [6, 4].
Fuzzy logic allows replacing crisp values by fuzzy ones, that are based on probabilistic idea of gaining any value between 0 and 1, or being described as an interval.
Introducing fuzzy logic to a rule-based system enables the usage of benefits of those to architectures – while rule-based expert systems offer clear reasoning and absolute step-by-step traceability of reasons for a conclusion, incorporation of fuzzy logic improves the accuracy of the reasoning process, improving the whole measurement of risk [5, 9].

B. Mamdani Fuzzy-logic reasoning

While there are two main methods - the Mamdani and Sugeno methods for realization of fuzzy-logic rule-based models, the most popular is the Mamdani fuzzy-logic reasoning method [1]. It consists of the fuzzification of input variables, evaluation of rules, aggregation of rule outputs and defuzzification of output values. This model shows strength because of it's intuitive features as well as simplified human input possibilities, a feature very important for the proposed design.
Value fuzzification is achieved by determination of input values and the relation of these values to the fuzzy sets that represent the value. Shown in the diagram (Fig. 1) we have a generic fuzzy diagram consisting of two triangular fuzzy sets *A* and *B*. The fuzzification of values is achieved by finding the level of fuzzy grades of each fuzzy set based on the value x_i.

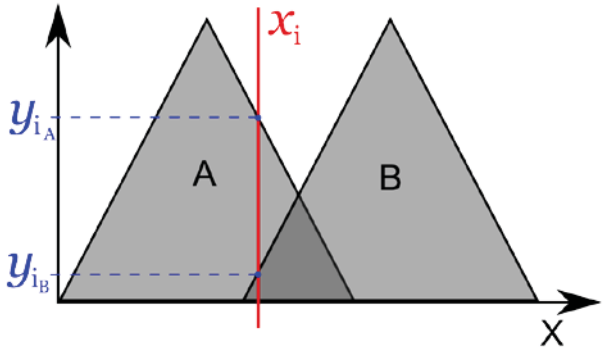

Figure 1. Generic diagram representing fuzzy sets and value fuzzification

Having the inputs fuzzified allows them to be applied to the antecendents of given fuzzy rules and apply the results to the membership function of the consequent. The correlation is performed by clipping the consequent at the value of truth (y_i) of the antecendent.
Having the fuzzy values of the consequents leads to the aggregation of the rule outputs. All the sets of consequents are combined into a single fuzzy set.

Defuzzification of the given output is achieved by applying the centroid defuzzification method, where the crisp value is calculated by finding the center of gravity of the set and the value that it represents (1):

$$g = \frac{\Sigma x_i \cdot u(x_i)}{\Sigma u(x_i)} \tag{1}$$

here: g – center of gravity, x_i – value, $u(x_i)$ – degree of membership of the value.

D. Knowledge engineering

Expert systems tend to work as a substitute for a human-experts, sharing their knowledge for reasoning and inferencing. Although expert systems show great strengths in availability, non-biased, emotionless reasoning, instant results and possibility of getting full explanation of given results, there is one major issue for this kind of expertise: providing the system correctly with the expertise [7]. Knowledge, provided for the system is the main factor causing the system to be as exact and objective as it can get. To achieve this the knowledge, transferred to the system in the form of rules, has to be acquired from multiple experts.
The process of knowledge engineering in this field consists of design of the system, definition of the information that has to be acquired, rule generation and providing each rule with probabilistic impact values.
Fuzzy-logic, used in this design allows description of events and probabilities in a structured natural language, associating these with probabilistic values. Not only this simplifies the process of expert knowledge engineering but also allows broader methods of presentation of expertise.
Rules in this system can be *one-input one-output*, or *multiple-input one-output* type. An example of *one-input one-output* fuzzy rule is: *if* X is A then P, or as a real world example: *if* THE CLOUDS *are* THICK *then* RISK FOR RAIN IS HIGH.

IV. Architecture of the system

A. General overview

The architecture of this system is based on two main components: the front-end user interface and the back-end server part (Fig. 2). The user interface deals with client subject data collection and result presentation, the back-end deals with data and expertise storage, new expertise acquisition from external sources, inference traceability and report generation. This kind of architecture ensures that the expertise provided is based on the newest available data, with the least resources required from the client. Therefore it ensures accessibility, actuality and easy usage without the need of any special software or hardware on the clients side except for the basic PC with an access to the internet.

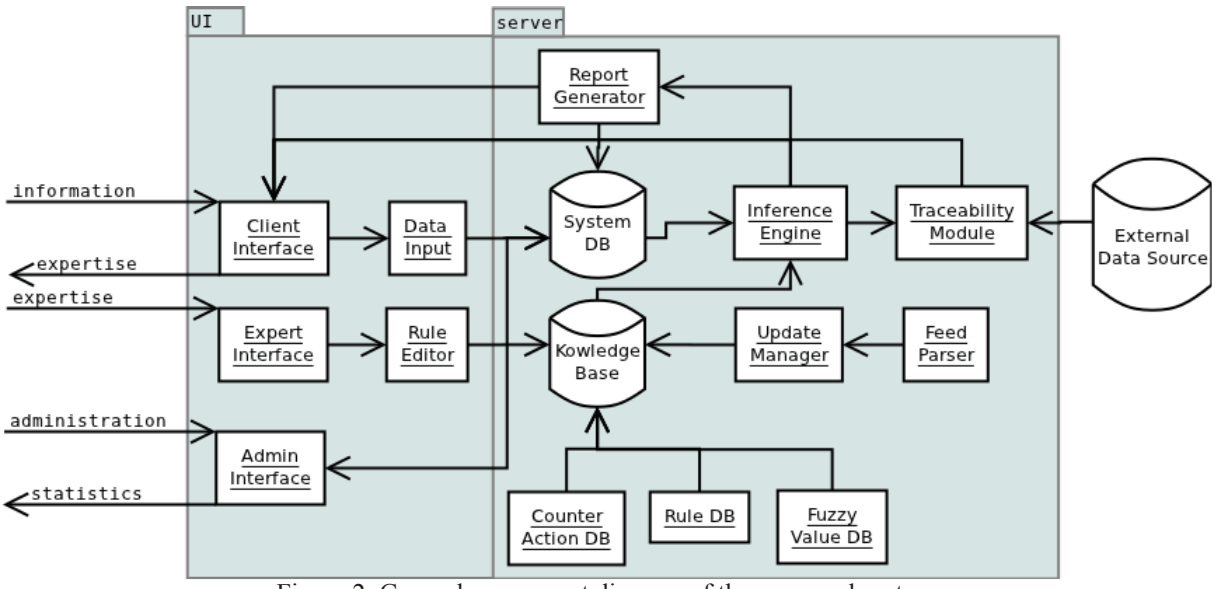

Figure 2. General component diagram of the proposed system

B. Update mechanism

There are certain application fields for an expert system, that requires to work with sensitive data, that provide competitive results only if working with the most up-to-date data, meaning that given knowledge is only actual for a limited period of time. This is also the case of this study – risk management in IT is a very dynamic process that changes dramatically over time. New technologies and, consequently, threats have to be taken into account to provide the end-user with a complete overall report of the risks.
To achieve these goals, the system's knowledge base has to be constantly updated with actual information, acquired from various sources of information [8]. Given the fact that most of the information about the threats and risks is published in periodic technical documentation and this documentation is presented in a known, structured form leads to an assumption that this role can be automated as well. To achieve this an automatic module for extracting data from this documentation is to be developed. This module, as shown in Fig. 3, consists of documentation fetcher, information parser, rule generator and rule import to knowledge base tool. The document fetcher periodically checks known sources for new versions of available documentation and fetches it as soon as newer version is detected. This documentation is then processed by information parser that deals with this natural language (NL) text by extracting the information, needed for the knowledge base of the expert system. Once the module has new facts available, it generates rules from this kind of information. The rules are then checked for duplication on the system's database. If the new rule has an exact match in the database it is ignored, if it has new or updated information it is imported and taken into account for the overall risk evaluation.

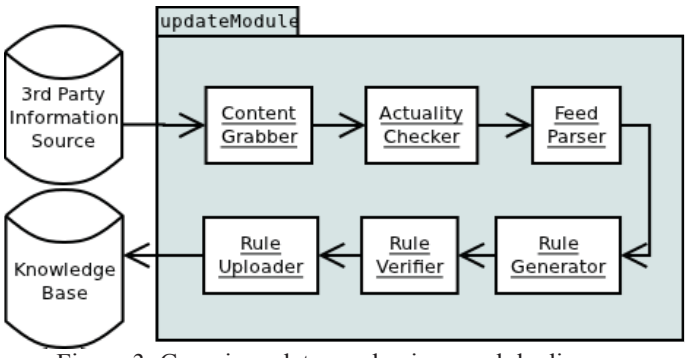

Figure 3. Generic update mechanism module diagram

V. Conclusions

Expert systems is a way of transferring the needed expertise from a human-expert to an information system. It leads to an improvement of availability as well as reduction of costs per one expertise. An expert system as a risk assessment and measurement tool is offered.
Dealing with potentially sensitive data requires special features of the system, enabling to keep up-to-date and provide the end-user with actual results. An automated update mechanism, able to fetch and parse rules automatically from a third-party source is described and offered.

References

[1] Castellano, G., Fanelli, A. M., Mencar, C., "Design of transparent mamdani fuzzy inference systems", *Third internationaly Conference on Hybrid Intelligent Systems (HIS) 2003*, Victoria, 2003.
[2] Clarke, J. *et al.*, *Consumerization of IT: Risk Mitigation Strategies*, European Network and Information Security Agency ENISA, Heraklion, 2012.
[3] Clarke, J. *et al.*, *Consumerization of IT: Top Risks and Opportunities*, European Network and Information Security Agency ENISA, Heraklion, 2012.
[4] Giarratano, J.C., *Expert Systems: Principles and Programming, Fourth Edition*, Course Technology, Connecticut, 2001.
[5] Gordon, A.L.S., Belik, I., Rahimi, S., "A Hybrid Expert System for IT Security Risk Assessment", *International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA '10),* Las Vegas, 2010.
[6] ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*, International Standardization Organization, Geneva, 2008.
[7] Kendal, S., Creen, M., *An Introduction to Knowledge Engineering*, Springer, New York, 2011.
[8], Marinos, L., Sfakianakis, A., *ENISA Threat Landscape Responding to the Evolving Threat Environment*,

European Network and Information Security Agency ENISA, Heraklion, 2013.
[9] Surmann, H., Selenschtschikow A., "Automatic generation of fuzzy logic rule bases: Examples I", *First International ICSC Conference of Neuro-fuzzy Technologies,* pp. 75-81, Cuba, 2002.

References

This research is funded by the European Social Fund under the Project No. **VP1-3.1-ŠMM-08-K-01-012.**