Building and modeling a sustainable expert system, using UML language

Violeta N OPRIȘ
Ph.D. Student, The Military Technical Academy, Faculty of Military Electronic and Information Systems, Bucharest
E-mail: violeta.opris@yahoo.ro

Abstract. The Unified Modeling Language (UML) is the successor of multitudes of oriented analysis and design methods. This model saves energy, resources and also secures the required infrastructure. It is also the result of a process of introducing standardization into object-oriented analysis and design. The paper concentrates to build UML diagrams and to highlight the structure of modules for the expert system. The UML diagrams are useful at a certain point in the system development and have a certain utility in the research paper. This new approach ensures that the expert system is successful and sustainable in the future. Integral elements of sustainable expert systems are research and innovation activities. In this context, guided by system user needs, UML is used in an iterative and incremental approach based on abstraction levels. The personal contribution in this paper is modeling the proposed expert system, using UML diagrams. These are used to represent and visualize modeling elements for an intrusion detection expert system.

1. Introduction
This research paper aims to demonstrate the value of the proposed solution to improve the current infrastructure of expert systems, automate complex processes, monitor networks, intrusion detection, generate reports, increase the performance of the solution by using new information technologies and improve access to available services through system functionalities.

The integrated expert system includes online service components, downloadable and recorded intrusion services, event schedules, the ability to integrate with other systems, the ability to build an integration pilot with external systems, a knowledge base, user interface, automatic and remediation. The expert system is based on an algorithm and a knowledge base.

An important goal is that access to the expert system by users is safely done. The users are assigned to a module and have configured rights and access roles, the group they belong to and the access password. As the organizations have tried hard to monitor and optimize their impact within society, the researchers aim to reduce the impact of businesses on social and natural environment.

The expert system also includes a reporting and statistics module, making it a particularly useful tool for assessing and detecting intrusions. Another goal of intrusion detection activity is to prevent the consequences of intrusion by implementing an effective security control expert system.

The expert system benefits using UML language are:
• availability 24/7 hours;
• knowledge base for storing information and resolving problems;
• competitive access to information and event planning;
• detecting suspect elements that can be considered intrusions;
• automatic remediation and keeping the history of the performed operations;
• managing the detected intrusions;
• tracking possible attacks;
• engine deduction for exploiting the knowledge base;
• monitoring network events;
• fundamental management decisions through reports;
• determining the deviation from normal behaviour;
• assigning tickets and solving problems;
• evidence of events and their storage in a secure location;
2. Previous work. Design methods for expert system

This section has as main objective understanding the concept of modeling. Modeling the expert system ensures effective communication between those involved in the system development [4]. In documenting the expert system to detect intrusions, modeling is considered a learning process.

In this paper, graphical patterns are created using the various UML diagrams to get a clear picture of the main components of the expert system.

Approaching the expert system through UML diagrams leads to various advantages. An important advantage is the quick understanding of the connections between the expert system and the external environment and the non-inclusion of technical aspects of implementation in the analysis phase. Likewise, there are two categories of system models in practice: the logical model that focuses on how the system works and the physical model in which the way the system will be implemented is presented.

The modeling of the system is useful because the diagrams will be modified to be mapped to the requirements of the projected system. A feature of modeling is the flexibility to ensure the consistency of system representation.

For the development of the system, the interactive modeling process is used, which leads to the probability of detecting errors from the analysis phase, eliminating nonconformities and detecting possible omissions [4].
The intrusion detection expert system on cloud computing infrastructure is a specialized IT system that allows computerized monitoring of computer security in order to manage network traffic [5].

The key features of the expert system are:

- it is a technology-based IT solution that ensures the security of the monitored systems regardless of location and time: browser based solution;
- innovative: an innovative tool for identifying, managing intruders in a network, especially with regard to vulnerabilities;
- ensures the entire flow of intrusion monitoring activity in a network;
- accessibility: friendly, accessible, graphical user interface, labels and messages that provide the user with ease in navigation and operation, general knowledge of operating software applications;
- high availability: in terms of trading / multiuser / competitor as well as in terms of each component;
- data security and integrity: access is automatically based on credentials;
- parameterization: the uniqueness of information by eliminating redundant information;
- manageability: in the sense that the system includes mechanisms that enable end-user hierarchy, definition of user / role / group access rights, user logs;
- scalability and flexibility: response to a high degree of parameterization that allows rapid and easy changes within the system, configurable and able to meet the needs of a progressive number of users.

The architecture of the model system has three levels:

- user interface;
- computer system server;
- database.

Business flow activities involve identifying intrusions, panning the desired events, automatically troubleshooting identified issues, communicating between users using the messaging module, scanning events that occur on a network, generating reports, managing organizations and system users, assigning tickets for the IT security team, special administration of the knowledge base, inventory of goods [10].

The modeled expert system in this research paper is a dedicated intrusion detection activation solution, making it an innovative and extremely useful tool.

3. Expert system overview

The concept of developing an expert system is in the attention of the research community. Developing an intrusion detection expert system is a multidisciplinary and complex task. An important factor is the lack of research and general methodology for the development of expert systems managed on cloud computing infrastructures [5].

The system modeled in this paper is an expert system based on artificial intelligence and modeled using the UML language. Artificial Intelligence (AI) is a field of research in computer science. An important definition of AI was given by John McCarthy in 1955: "a car that behaves in a way that could be considered intelligent if it were a man."

Progress of strong AI-based expert systems is in continuous development, almost all simulations of intelligence are based on common rules and algorithms.

In the case of the classical expert systems, different areas of interest and research for AI that have been researched are distinguished:

- expert systems;
- neural networks;
- automatic learning;
- data mining;
- artificial view;
• voice processing;
• processing in natural language.

An essential feature of AI is the ability to learn, with or without external aid, for continuous improvement. Initially, AI was conducted in the field of psychology, which was based on linguistic intelligence. An important example is the Turing test, which consists of a conversation in natural human language with a machine that has been programmed specifically for this test.

Traditional expert systems can be categorized as follows:
• systems that think rationally;
• systems that act as people;
• systems that act rationally.

The concept of modernity of expert systems involves their migration to an innovative research area. Migrating classical (ES) expert infrastructure into cloud computing is a complex process that requires careful and deliberate planning [2]. This process can have unexpected costs, interoperability, security gaps and can create significant obstacles. But cloud computing has benefits and today most organizations use it [5].

The expert system has key features such as performance, easy to understand, trustworthy and highly responsive. It also has training, assisting in decision-making, diagnosis and substitution of human decision makers. Mapping the cloud computing with expert an system requires organizations not to have large data centre. They can store, process and analyse information using cloud computing [5]. This could reduce widespread energy consumption that balances economic and environmental performance. Cloud computing comes with the ability to exchange information on multiple platforms, from different locations, inside and between users [2].

4. Modeling the expert system using UML
Unified Modeling Language is the successor to the multitude of oriented analysis and design methods. The use of the UML language depends on the complexity of the real system to be modeled, the project management and realization method, the type of computer system to be achieved, and the level of detail required in the design phase [6].

In this context, guided by system user needs, UML is used in an iterative and incremental approach, based on abstraction levels.

To model the expert system proposed in this research paper, UML diagrams are used to represent and visualize modelling elements for intrusion detection [1].

4.1. Use Case Diagram
The Use Case Diagram is built for expert system to describe the functionality of the system from the users’ point of view (Figure 1). It contains actors and uses case. Actors are system elements that generate or receive events, and a case of use is a sequence of actions triggered when an actor calls the system to complete a process [6].

The use case diagram is also used to specify system boundaries and specifies the interaction that takes place between the actors and the expert system.
4.2. Class Diagram
The static structure of the expert system, viewed as an ensemble of object classes and relations between classes, is represented by the class diagram [6].

The class diagram presents the structure of the system from a general point of view. In close connection with it, the object diagram highlights objects and links between them [1].

Object diagrams show particular cases and facilitate understanding of complex data structures. Classes correspond to semantics of entities in the real system. A class designates a group of objects that have similar properties, common behaviour, and common relationships with other objects.

4.3. Activity Diagram
By performing the activity diagram, the behaviour of the intrusion detection expert system is described by introducing implementation elements. The diagram of activities of the expert system has in structure the following elements: action, transition, decision [6].

The action from the point of view of the expert system belongs to a stage in the execution of an algorithm. The operations performed within the system can be seen as a chain of actions and detailed in elementary operations [3]. Also, the actions can be grouped into activities to simplify diagrams interacting in the system.

The transition from one action to another is graphically represented by an arrow labelled eventually with the name of the event that determines the transition and the condition of occurrence of the event [1].

4.4. State Diagram
In this paper, the state diagram is used to describe the behaviour of a class's objects through states and events [3].

Using the state diagram for the expert system leads to the following advantages [6]:
- it provides a description of the usage case;
- it is built only for classes with significant dynamic behaviour;
- it models the lifecycle of a single class, highlighting eventual events sent to another class in the system;
- it contains only one initial state and one or more final states determined by the conditions of occurrence of the event.

Figure 1. Use Case Diagram
4.5. Sequence Diagram

The sequence diagram illustrates interactions between objects across a case scenario (Figure 2). Each object is represented by a rectangle in which the name is entered. The object's line of life is specified by a vertical bar.

Messages are represented by horizontal arrows from the transmitter to the receiver. Assuming that the time runs from top to bottom, the order of reference is given by the position on the vertical axis. The elements presented in the sequence diagram are translated into the class diagram [6].

![Sequence Diagram](image)

**Figure 2. Sequence Diagram**

Starting from the initial specifications of the expert system, the proposed solution has a technical architecture consisting of a back-office component that will be exploited by dedicated staff from the entire system administration and a Front Office component, accessible via the Internet to users represented in particular by IT security specialists; a trading component that will handle system authorization requests and an archiving component.

![DB expert system model](image)

**Figure 3. DB expert system model [9]**
The proposed system includes the following modules: event planning, messaging, automatic remediation, inventory, users, reports, scanning, knowledge base, organizations and tickets (Figure 3).

Schedule functionality module provides the ability to customize events in a computer system, network scanning, event monitoring, task assignment.

The Message functionality module is a user-friendly model for easy communication between the organization's departments and the monitoring of the entire infrastructure that is supposed to be innovative.

The Troubleshooting functionality module provides users with automatic task resolution, by the initial software configuration and previous information (Figure 4).

![Figure 4. Troubleshooting functionality](image)

The Assets Functionality module is a mechanism that automatically checks inventory of software products for the proper operation of the entire IT system.

The Users Functionality module assumes management of the IT system, which includes user groups configuration, user creation, workstation management.

![Figure 5. Users functionality](image)

The Reports Functionality module is a particularly useful tool for evaluating and predicting network intrusions and problems.

The Scans Functionality module provides the ability to scan unplanned events that can affect the entire computer system.
The Knowledge Base Functionality module is designed so that each operation is stored in a database, while being the answer to ambiguous solutions to intrusion detection problems (Figure 6).

The Organizations Functionality module facilitates the management of the organizations that have the proposed expert system for development.

The Ticket Functionality module involves the implementation of a full-feature management functionality for the vendor-specific ticketing flow to users specific to the IT department.

5. Conclusions

The final conclusions of the scientific research paper highlight the main contributions, both theoretical and practical.

In the paper, it is described and modeled an expert system for detecting intrusions from a network mapped with cloud computing infrastructure. By analysing UML diagrams, we have noticed that it is essential to understand the expert system interface and modules. Despite the aforementioned findings, the UML diagrams highlight a new model that helps to develop an expert system.

The expert system has a modular structure for optimal use and increased security, a cloud-based infrastructure being a new concept [11]. The proposed IT solution will be provided as a public or private cloud, helping organizations to create security in initiatives to detect network intrusions, also substantially reducing costs.

Considering the benefits of the model, this study provides new approaches of investigating the UML language used for development.

It is difficult for organizations to develop and integrate an expert system into innovative environmental and economic performance tools. Although, it could increase stakeholders trust, but companies have to prove their ability to minimize costs and to improve efficiency.

The solution has many modules, which can be expanded as research and development directions: event planning, messaging, automatic remedies, inventory, users administration, organizations, scanning, tickets, reports, knowledge bases. Of course, this system appears against ever-changing threats, also supporting compliance with existing technologies. Old security software is complex, expensive and ineffective.

This study reveals that the expert system UML model has a significant influence on information security. Starting on-demand scalability from expert system, the paper roughly introduces the new structure and components of the expert system. As a future research work, we plan to design a strong expert system.
References

[1] Udrică M, Mihăilescu M, Opriș V, Ionită R, Improving The Decisional Process By Using UML Diagrams, Journal of Knowledge Management, Economics and Information Technology, Bucharest 2012

[2] Dumitru L, Eftimie S, Mihăilescu M, Nita L, Opris V, Racuciu C, A Novel Architecture for Authenticating Scalable Resources in Hybrid Cloud, 11th International Conference on COMMUNICATIONS, Bucharest, 2016

[3] Mihaielșcu M, , Opriș V, Beteringhe A, Enhancing UML with Security, 2nd INTERNATIONAL CONFERENCE SEA-CONF, Academia Navală Mircea Cel Bătrân, Constanța, 2016

[4] Paunica M, Opriș V, Opriș M, Tanase G, Financial Performance Improvement Through Sustainable Development, The 12th International Conference Accounting and Management Information Systems, Bucharest, 2017

[5] Opris V, Opriș M, The expert system development technologies in cloud, 3rd INTERNATIONAL CONFERENCE SEA-CONF, Academia Navală Mircea Cel Bătrân, Constanța, 2017

[6] Sisteme informatiche economice – probleme și soluții, Mioara Udrică, Vatuiu T, Lipcanu A, Varjoghe S, Editura Hamangiu, Universitatea Titu Maiorescu, 2014

[7] Saufi, N.A.A., Daud, S., Hassan, H., 2016, Green Growth and Corporate Sustainability Performance, 7th International Economics & Business Management Conference, 5th & 6th October 2015.

[8] Williams, B., 2012, The Economics of Cloud Computing, Cisco

[9] http://astah.net/editions/professional

[10] https://www.tutorialspoint.com/mvc_framework/mvc_framework_introduction.htm

[11] http://www.ibm.com/cloud-computing/us/en/cloud-solutions/cloud-security