J Inf Process Syst, Vol.12, No.4, pp.688~710, December 2016
http://dx.doi.org/10.3745/JIPS.03.0056

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Novel Approach for Integrating Security in Business Rules Modeling Using Agents and an Encryption Algorithm

Nawal Sad Houari* and Noria Taghezout*

Abstract

Our approach permits to capitalize the expert's knowledge as business rules by using an agent-based platform. The objective of our approach is to allow experts to manage the daily evolutions of business domains without having to use a technician, and to allow them to be implied, and to participate in the development of the application to accomplish the daily tasks of their work. Therefore, the manipulation of an expert's knowledge generates the need for information security and other associated technologies. The notion of cryptography has emerged as a basic concept in business rules modeling. The purpose of this paper is to present a cryptographic algorithm based approach to integrate the security aspect in business rules modeling. We propose integrating an agent-based approach in the framework. This solution utilizes a security agent with domain ontology. This agent applies an encryption/decryption algorithm to allow for the confidentiality, authenticity, and integrity of the most important rules. To increase the security of these rules, we used hybrid cryptography in order to take advantage of symmetric and asymmetric algorithms. We performed some experiments to find the best encryption algorithm, which provides improvement in terms of response time, space memory, and security.

Keywords

Business Rules (BR), Business Rules Management System (BRMS), Encryption Algorithms, Security Agent

1. Introduction

Currently, the establishment of information systems involves more and more experts with wide-ranging expertise. The business requirements expressed at the departure of the conception evolve and occur frequently. As such, the more the system is flexible, the more the updates can be mastered [1].

In a traditional approach, business logic is buried in computer application code making maintenance difficult. One principle of software engineering is the use of models using different approaches, methods, and techniques. The representation of business rules is one of the approaches that is being increasingly used [1].

In computing science, a business rule is a high-level description that allows controlling and/or making a decision using enterprise specific concepts. Thus, business rules describe what an expert needs

Manuscript received July 9, 2015; accepted October 15, 2015.
Corresponding Author: Nawal Sad Houari (sad.houari.nawal@gmail.com)
* Dept. of Computer Science, University of Oran1 Ahmed BenBella, BP 1524 EL Mnaouer Oran, Algeria (sadhouari.nawal@edu.univ-oran1.dz, taghezout.noria@univ-oran.dz)

to do to make a decision [2]. They capitalize on the enterprise's knowledge and translate its strategy by describing the actions to lead for a given process. They are generally written in a controlled natural language [3]. Generally speaking, business rules management has given birth to the business rules management system (BRMS) technology, which has rapidly become the best solution for the problem of effectively maintaining business rules. The rules can be defined in the form of simple rules (as IF <conditions> THEN <actions>), decision tables, or decision trees [4,5].

In knowledge based systems, the knowledge and reasoning of a human expert can be captured and stored in the form of a complex rules network. Therefore, the manipulation of the business expert's knowledge generates a need for information security and other associated technologies. The notion of cryptography has emerged as a basic concept in business rules modeling.

Cryptography is the art of encoding messages. Pictorially, cryptography can be compared to a safe (i.e., a visible protection that is inviolable as long as we do not know the code to open it) [6]. Although there is a consensus that cryptography has existed for centuries, it has only been with the advent of computer science that modern cryptography has been considered a science in and of itself. Particularly, the study of this science is based on the three following pillars [7]:

- Confidentiality: Ensures that information is only accessible to those who are allowed access.
- Authenticity: Permits proving the identity of a person or the origin of data.
- Integrity: Ensures that data has not been accidentally or intentionally modified by a third party.

The purpose of this paper is to present a cryptographic algorithm based approach to integrate the security aspect in business rules modeling. To increase the security of the rules, we used the well-known hybrid or mixed cryptography, in order to take advantage of symmetric and asymmetric algorithms. The exchange of the secret key is carried out thanks to the public key algorithm answering the question of secure key exchange. The communication that follows is encoded by using the secret key algorithm. This can permit to benefit from fast systems treating important volumes of data [8]. We simulated some symmetric encryption algorithms, such us DES, Blowfish, RC4, and AES. We used the RSA asymmetric encryption algorithm to encrypt the key.

This paper is organized as follows: in Section 2, we present a brief review of business rule management systems and we also provide a review of multi-agents systems and collaborations. Section 3 describes some other related works and our contribution. The most important encryption algorithms are presented in Section 4. In Section 5, our suggested agents-based approach is given. To illustrate the feasibility of our proposed approach, the results of our experiments are given in Section 6, and we discuss these results in Section 7. Finally, Section 8 concludes our study and out-lines our future research directions.

2. Background

BRMS is software that manages and supports the business rules of an organization or an enterprise. The objective is to have clear rules that are unambiguous and comprehensible by all, especially by not experienced experts in information technology. The method is to separate the business logic (rules) of the logic system (programs, development languages, databases, operating systems) from an application so that the business logic can evolve separately from the application code [9].

BRMS is applied to guarantee to the users non-programmers certain independence in the conception and maintenance of their rules. It permits to develop some rules without programming [9]. The classical architecture of BRMS is given in Fig. 1 [10].

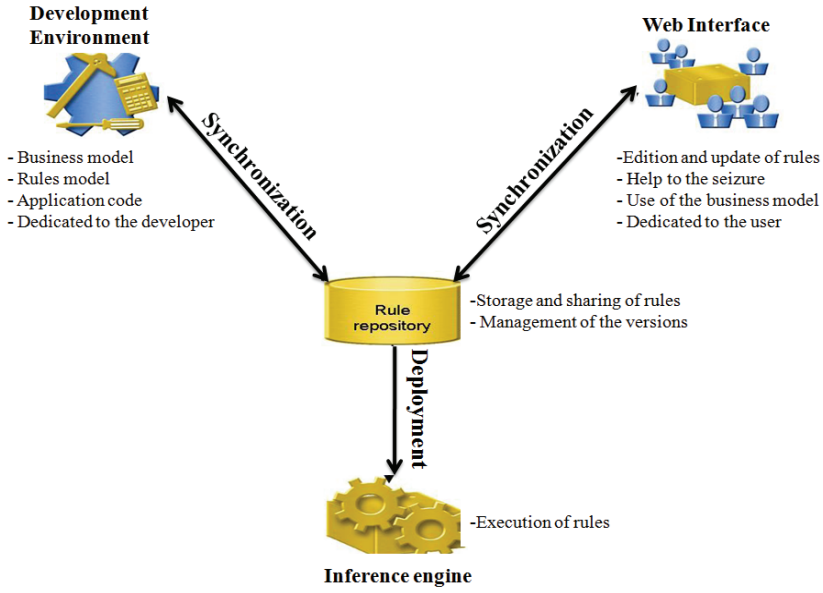

Fig. 1. The classical architecture of a business rules management system (BRMS) [10].

BRMS solutions automate operational decisions in business applications. They reduce the maintenance costs of these applications and improve the collaboration between business and IT teams. Thus, BRMS allows a system to accomplish the following tasks [9]:

- Develop rules without programming.
- Business experts to participate directly in the management of rules.
- Automate decisions and manage frequent modifications of the rules.
- Reduce development costs.
- Improve reaction and adaptation capacities facing the changes.

In the next section, we will introduce the fundamental concepts under the two main points of collaboration and agent-based modeling techniques.

2.1 Collaboration

Collaboration is working with others to do a task and to achieve shared goals. It is a recursive process where two or more people or organizations work together to realize their shared goals. Structured methods of collaboration encourage introspection on behavior and communication. These methods specifically aim to increase the success of teams as they engage in collaborative problem solving [11].

Collaboration in business can be found both inter- and intra-organization, and ranges from the simplicity of a partnership and crowd funding to the complexity of a multinational corporation. Collaboration between team members allows for better communication within the organization and

throughout the supply chains. It is a way of coordinating different ideas from numerous people to generate a wide variety of knowledge [11]. Collaboration is the joint effort of multiple individuals or work groups to accomplish a task or project. A wide range of collaborative software (also known as groupware) is available for enabling collaborative communication. Collaboration may be asynchronous, in which case those collaborating are not necessarily working together (or in communication) at the same time. On the opposite hand, collaboration can also be synchronous (known as real-time collaboration), in which collaborative partners work together simultaneously and are in communication as they work [12].

In BRMS, the collaboration between business experts plays a very important role for capitalizing on knowledge and expertise.

2.2 Agents

A software agent can be defined as an encapsulated computer program situated in some environment that is capable of flexible, autonomous action in that environment in order to meet its design objectives [13]. According to Ferber and Perrot [14], "An agent can be defined as an autonomous entity, real or abstract, which is capable to act on itself and on its environment, which, in a multi-agent universe can communicate with other agents, and whose behavior is the consequence of its knowledge and interactions with other agents". Among an agent's features, we focused on:

- Capable to act in an environment.
- Dispose of their own resources.
- Can communicate directly with other agents.
- Possess expertise and offers services.
- Capable of perceiving its environment.

The multi-agent system (MAS) offers a new dimension for cooperation and coordination in an enterprise. The MAS paradigm provides very suitable architecture for the design and implementation of integrative business information systems. With agent-based technology the support for the development of complex information systems is introduced by natural decomposition, abstraction, and the flexibility of management for organizational structure changes. The MAS consists of a collection of autonomous agents that can define their own goals and actions and that can interact and collaborate with each other through communication. In a MAS environment, agents work collectively to solve specific problems. It provides an effective platform for coordination and cooperation among multiple functional units in an organization [15].

According to Ferber and Perrot [14], a multi-agent system is composed of

- The environment E: Represents the space where agents can move;
- A set of situated objects O: This means that at it is possible to associate with any object that is in position in E;
- A set of agents A: Considered as particular objects representing the active entities of the system;
- A set of relations R: Unites the objects (especially the agents) between them;
- A set of operations OP: Allows the agents of A to produce, consume, transform, and manipulate the objects of O. This corresponds to the ability of agents to perceive their environment.

3. Related Works and Contributions

BRMS is a promising technique used to facilitate the edition, creation, modification, and management of business rules. It also improves decision making in organizations. In other research related to this several works exist. We provide the most important ones in the subsection below.

3.1 Related Works

First, the work presented in [16] proposed the conception and implementation with a multi-agent system that coordinates an expert system and a neural network to construct production orders to produce labels. The fundamental goal of MAS is to construct a manufacture order. MAS possesses the following agents: tool agent, machine agent, coordinator agent, spy agent, and scheduler agent. However, one limitation is that the scheduler agent employs FIFO politics, even though it is the simplest ordering/queuing mechanism. Therefore, it is necessary to develop strong scheduling politics to provide more realistic plans.

Second, the methodology proposed in [17] has been used to help business experts and developers to link the business rules at the business level with the rules that are implemented at the system level. In order to lead into the formalization of the business environment to the extent required for business rule management, the business modeling technique has been identified in the BRME (business rule management in enterprises) project. The approach recognizes five sub-models. However, one limitation is that the expert must introduce his/her business rule in a pseudo language and doing so requires some knowledge of programming.

The study developed in [10] is an approach that manages the consistency of the business rules published from OWL ontologies at the time of their evolution. Two methods are presented: the first permits the edition of the business rules in a controlled natural language from OWL ontologies and the second manages the consistency of these rules at the time of the corresponding ontology evolution. The authors used the BRMS IBM WebSphere ILOG JRules to edit the business rules. However, one limitation is that this approach doesn't cover all changes relating to ontology.

3.2 Our Contributions

The main objective of our study is to guarantee the security (confidentiality, authenticity, and integrity) of the business rules that are introduced by the experts to encourage them to capitalize on their knowledge and to have confidence in the system. In doing so, we used an encryption algorithm to improve the system's security and to guarantee the confidentiality, authenticity, and integrity of the business rules. The modeling has been based on agents to increase the execution speed of processes and the effective response, and to guarantee the collaboration between business experts. Our contributions are not restricted to this objective, as we were inspired by all of the works cited below [10,16,17] and our study covered the following key-points:

- Design and implementation of a collaborative system (BRMS) dedicated to business experts.
- Covering the security aspect and its integration into the whole system.
- Implementing an agent-based architecture where the security agent and the translator agent play an important role.
- Providing a convivial and ergonomic editor as a collaborative interface for the experts.

This paper focuses on the generation of decisions, which can be facilitated by executing the suggested rules in an automatic manner. The method for considering the consistency of business rules management, which is given in [10], was beneficial to our work.

In the next section, we describe in detail our agent-based approach with more attention given to the security aspect of the rules.

4. Cryptography Algorithms

A cryptographic algorithm is a mathematical function used in the process of encryption and decryption. It works in combination with a key to encrypt the plaintext. The security of encrypted data is entirely dependent on the strength of the cryptographic algorithm and the secrecy of the key [18, 19]. There are mainly two major families of encryption: symmetric and asymmetric. A symmetric encryption uses the same key to encrypt and decrypt; unlike asymmetric encryption, which uses two different keys – a public key for encrypting and a private key for decrypting [19].

4.1 Symmetric Cryptography Algorithms

Below we mention the most important algorithms.

4.1.1 DES (Data Encryption Standard)

The DES [20] is a block cipher system. It usually operates on blocks of 64 bits and uses a key of 56 bits that will be transformed into 16 sub-keys of 48 bits. Encryption takes place in 16 rounds. The message, previously converted in the binary, is divided into blocks B_i of 64 bits. For each block B_i, the following steps are applied:

An initial permutation (IP) is performed on the bits of block B_i. We call G_0 and D_0 the parts that are 32 bits to the right and left of the obtained block.

We repeated the following procedure 16 times:

- $G_i = D_{i-1}$
- $D_i = G_{i-1}$ XOR $f(D_{i-1}, K_i)$
  Where K_i is a block of 48 bits of the key K, and f is a function composed successively of a bit expansion, a XOR, a bit reduction, and a bits permutation.
- We recomposed a block B'_{16} by recovering D_{16} and G_{16} in this order.
- We performed the inverse permutation of the initial permutation (IP^{-1}).

4.1.2 Blowfish

Blowfish [20] performs coding by blocks of 64 bits and uses a variable-length key. The algorithm is divided into two parts: an expansion part of the key and an encoding part of the data. The expansion part of the key consists of converting the key (maximum 448 bits) into several sub-keys. The data encryption is carried out during 16 iterations. Each iteration consists of a key-dependent permutation and substitution that is dependent on the key and data. All operations are XOR and are additions to words of 32 bits.

4.1.3 RC4 (Rivest Cipher 4)

RC4 [21] is a stream cipher algorithm (by flux) with a variable-length key (from 1 to 256 bytes), developed in 1987 by Ron Rivest. It is a pseudo-random generator that generates a sequence of bytes. These bytes are then combined with the text to be encrypted by a XOR. Two steps are necessary for encryption: initialization using the key and the encryption of the plaintext. The first step generates two tables of 256 bytes according to the key: a table *K* initialized with the byte of the key and a table P (called a state table, which is the flux applied on the clear text) initialized with the numbers of 0 to 255 that are permuted pseudo-randomly according to the table *K*. The second step consists also in permutations to perform the encryption. Note that all additions are performed modulo 256.

4.1.4 AES (Advanced Encryption Standard)

AES [22] is a block cipher algorithm. Data is processed by blocks of 128 bits, 192 bits, or 256 bits for clear and cipher texts. AES operates on rectangular blocks of 4 rows and N_c columns, in which each term $x_{i,j}$ (called byte) is composed of 8 bits ($b = b_7b_6b_5b_4b_3b_2b_1b_0$), and can be represented algebraically as polynomials of degree ≤7 ($b = b_7X_7 + b_6X_6 + b_5X_5 + b_4X_4 + b_3X_3 + b_2X_2 + b_1X + b_0$) with coefficients in {0, 1}. The length key can be 128, 192, or 256 bits [20]. AES operates on a 4×4 matrix (when the length of the message is 128) whose inputs are words of 8 bits. The clear message was cut into 16 blocks of 8 bits and filled in from top to bottom and left to right. The four steps of a round are [22]:

- SubBytes: Each entry is replaced by another word of 8 bits given by a correspondence table;
- ShiftRows: Inputs are shifted in a circular left shift of a number of squares depending on the line;
- MixColumns: Each column is replaced by a new column obtained by transforming the column in a polynomial and multiplied by a fixed polynomial;
- AddRoundKey: Each input is replaced by the OR exclusive between this input and the corresponding input in a 4×4 matrix built from the key.

Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

4.2 Asymmetric Cryptography Algorithms

4.2.1 RSA (Rivest-Shamir-Adleman)

RSA encryption [23] was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. It is based on the prime factorization of an integer. The principle of RSA is as follows:

- Randomly generate two primes (p and q), then multiplying them to generate the number n.
- Determine $\varphi(n)$ / $\varphi(n) = (p - 1) * (q - 1)$
- Determine e / p, $q < e < \varphi(n)$
- Determine d / $e*d \bmod \varphi(n) = 1$ and p, $q < d < \varphi(n)$
- The couple (n, e) is the public key encryption, while the couple (n, d) is its private key
- To encrypt a text, we applied: $c = m \wedge e \bmod n$
- To decrypt a text, we applied: $m = c \wedge d \bmod n$

Where, m is the plaintext message and c is the encrypted message.

Before being encrypted, the original message must be decomposed into a set of integers M of values between 0 and n-1. For each integer M it is necessary to calculate $c \equiv m \wedge e \bmod n$. The encrypted message is comprised of the integers sequence c. To decrypt c, d is used, and we recovered the clear message by $m = c \wedge d \bmod n$.

4.3 Theoretical Comparison

Fig. 2 presents a theoretical comparison between the cryptography algorithms mentioned in the previous section, considering the following criteria: creation date, designer(s), type, block size, key size, number of iterations, security level, and execution speed.

Criteria \ Algorithms	DES	Blowfish	RC4	AES	RSA
Creation date	1981	1994	1987	2000	1977
Designer (s)	IBM	Bruce Scheneier	Ron Riverst	Joan Daemen and Vincent Rijmen	Rivest, Shamir and Adleman
Type	Symmetrical bloc	Symmetrical bloc	Symmetrical flow	Symmetrical bloc	Asymmetrical
Block size	64	64	/	128, 192 or 256	/
Key size	56	Variable (max = 448)	Variable (1 to 256 octet)	128, 192 or 256	2048
Number of iterations	16	16	/	10, 12 or 14	/
Security level	Low	Military	High	High	Military
Execution speed	Average	Fast	Very fast	Fast	Slow

Fig. 2. Comparison between encryption algorithms.

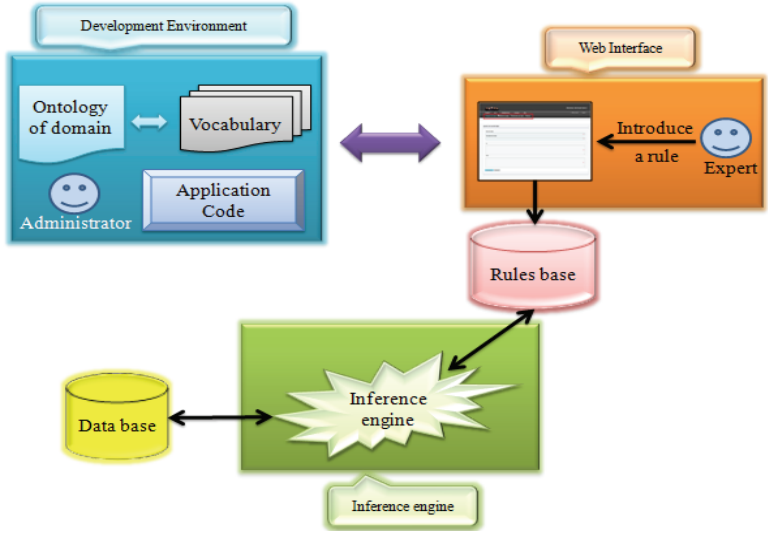

Fig. 3. The proposed system is given here [9].

5. Proposed Approach

We propose integrating an agent-based approach in the framework. This solution utilizes a security agent (SA) with domain ontology. This agent applies an encryption/decryption algorithm to allow for the confidentiality, authenticity, and integrity of the most important business rules [9].

Our approach capitalizes on the knowledge of business experts in regards to business rules by using an agent-based platform. This offers a facility to the experts for the standardization and auditability of the business rules. We propose using domain ontology in order to generate the business model corresponding to the enterprise. The BRMS is composed of several components, as described in Fig. 3 [9].

5.1 Development Environment

The development environment encourages collaboration between the developers and business experts. This step consists of defining the business model and the rules model as well as some essential functions corresponding to the needs [9].

5.2 Web Interface

This component is dedicated to business experts so that they can create and update their business rules. The interface must be convivial and as ergonomic as possible, in order to provide different functionalities to business experts [9].

5.2.1 Rules edition

Thanks to the generated business language, a business expert can write the rules in an autonomous manner. A rule is composed of a condition and an action. Therefore, the expert must specify the two parts. The process needs to pass through several steps until the final storage in the rules base. These steps are given below [9].

5.2.1.1 Syntactic verification module

This module provides a syntactic analysis to the experts in order to avoid mistakes that render the system unusable, for example:

R1: If an employee's salary exceeds the salary of his director then mark this employee as having a special status ➔ rule syntactically correct.

R2: If an emplyee's salary exceeds the salary of his director then mark this employee as having a special status ➔ rule syntactically incorrect.

To solve this problem, our system handles these errors in the beginning.

5.2.1.2 Semantic verification module

This service is composed of two sub-modules, which are:

- Synonym verification: This is made possible by using the domain ontology to translate the business rule, for example:

> **R1:** If an employee's salary exceeds the salary of his director then mark this employee as having a special status.
>
> **R2:** If an employee's salary is superior of his director's salary then the status of the employee is special.

- Verification of the rule's validity: This module detects if the rule is valid or not.

5.2.1.3 Technical translation module

Once introduced by the expert, the rule must be translated into a technical rule that is capable of being executed by the inference engine.

5.2.1.4 Consistency management module

The BRMS will provide a consistency management of the rules to avoid some ambiguities. In our case, we focused on contradiction, redundancy, equivalence, invalid rules (in the semantic verification module), and rules that are never applicable to knowledge management.

5.2.1.5 Security module

The business rules must be accessible for the company's business experts. However, access to these business rules must be highly secure. The establishment of a security system requires:

- Authentication: The identification of an expert is possible through an authentication process. There are many tools that have been developed for this, such as code PIN, login, banking card, badge, fingerprint, retinal scan, and vocal recognition.
- Encryption: This is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. This term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption) and then unscrambling it (known as decryption) [18].

5.2.1.6 Applicability module

A business rule can be syntactically correct, semantically correct, and consistent, but it is not exact. So, to solve this problem of accurateness the rule is sent to a meta-expert to check if it is correct or not.

5.2.1.7 Storage module

If the meta-expert judges that the business rule is correct, then he/she suggests storing it in the final rule base.

Fig. 4 describes the most important steps to introduce a business rule.

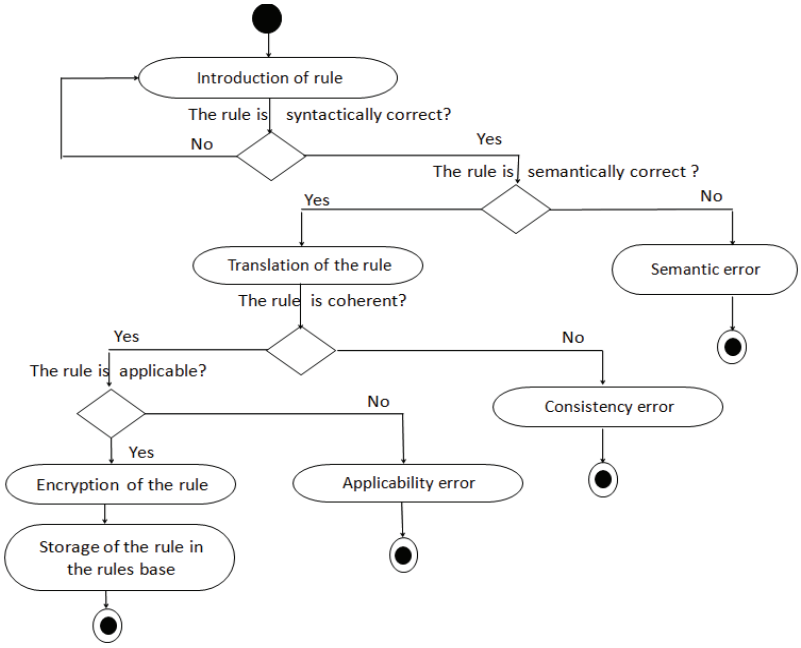

Fig. 4. Activity diagram of our system.

5.2.2 Our agents

To achieve all functionalities, we used an agent-based system that is composed of five agents (see Fig. 5) [9].

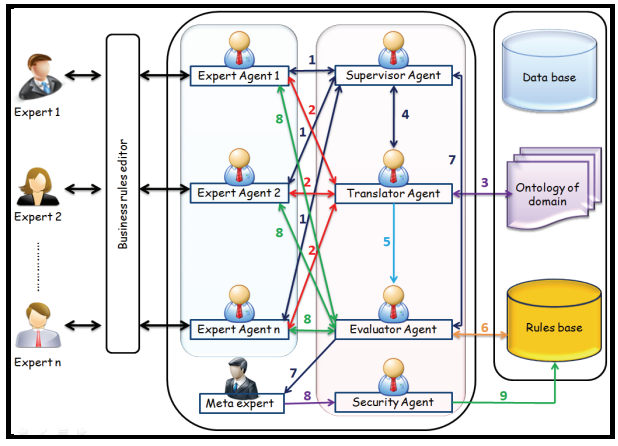

Fig. 5. The proposed agent-based architecture [9].

- Expert agent: Responsible for the recuperation of the rules seized by the expert. This agent saves the rules and transmits them to the Translator agent.
- Supervisor agent: Performs all control tasks in the system.

- Translator agent: The heart of our system that retrieves the rule from the Expert agent, browses the domain ontology, and extracts the set of concepts that correspond to the introduced rule. Finally, this agent sends the technical rule to the Evaluator agent.
- Evaluator agent: Responsible for assessing the consistency of the business rules. This agent recovers the rule translated by the Translator agent and accesses the rules repository to test if this rule poses a problem with another rule, and if it is does, the Evaluator agent sends a message to the Expert agent; otherwise this agent validates the rule.
- Security agent: Responsible for encrypting and decrypting the business rule. This agent uses the AES algorithm to encrypt and decrypt the business rules (see Section 6).

5.3 Inference Engine

According to the diagram presented in Fig. 3, an inference engine generally consists of three parts [9]:

- The "rule set" component contains the set of rules represented in a technical language.
- The "working memory" component contains the set of objects (the facts) of the application that will permit triggering the execution of the rules.
- The "diary" component contains the set of the eligible rules.

6. Implementation

This section is divided in two parts. The first part is dedicated to the collaborative graphical interface, which is where the experts will be able to introduce their knowledge in a simple form (rule). The editor gives them the possibility to update their rules, visualize the contents, and launch simple or advanced research by using some key-words.

In the second part, we present some experiments for choosing a suitable encryption algorithm for the forming of rules.

6.1 Execution Scenario

Below is a simple example to illustrate our approach.

Miss Nawal is an expert in the company. She accesses the developed platform in order to capitalize on her knowledge and her experiences in a particular domain. She must follow some steps.

Miss Nawal wants to introduce the following business rule to create her proper discount (the rules used here are extracted from a detailed case study of the work done in [24]). We preferred using the known rule base for our scenario in order to compare the most relevant results.

The rule is as follows: *If the customer's state is MIN and the customer's category is GOLD and the date of the order is between January 1 and January 31, 2015, then give a 10% discount on the order and add this message to the order "As a GOLD customer, you have received a 10% discount on your order".*

Once access is guaranteed, the business rule editor will be visualized as described in Fig. 6.

Miss Nawal can search for a rule (see Fig. 7), as the developed platform offers business experts advanced research that is essentially based on some keywords or criteria. The business expert can complete all fields or only some fields. The search result is shown in table format, which contains all of

the information related to the business rule(s).

By using the platform, the expert will be able also to update or delete the rule.

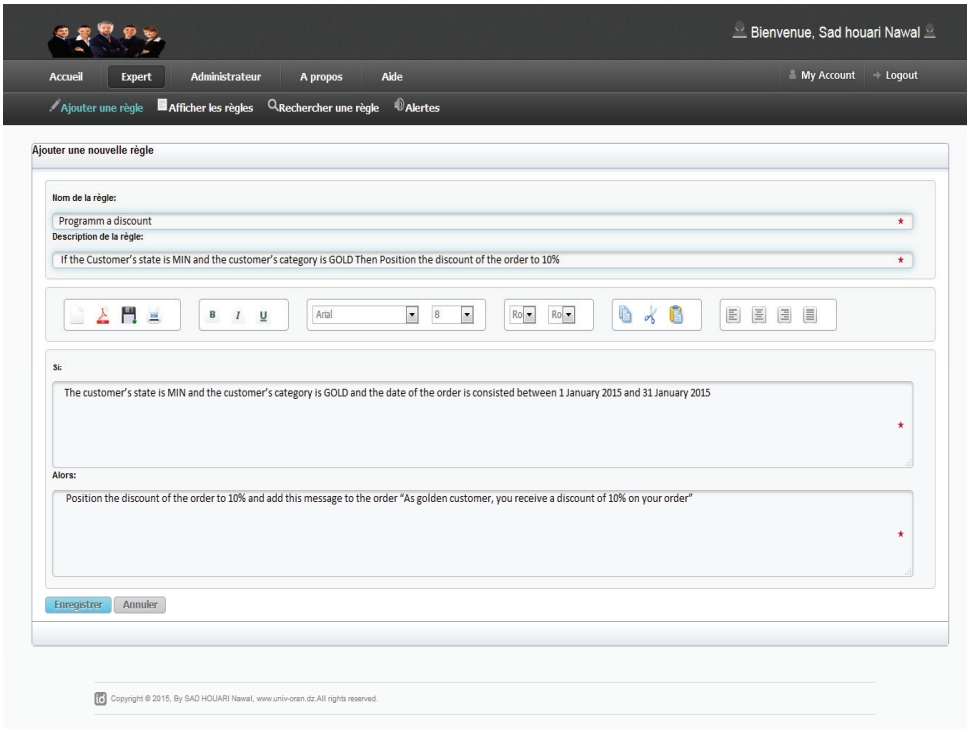

Fig. 6. Business rules editor.

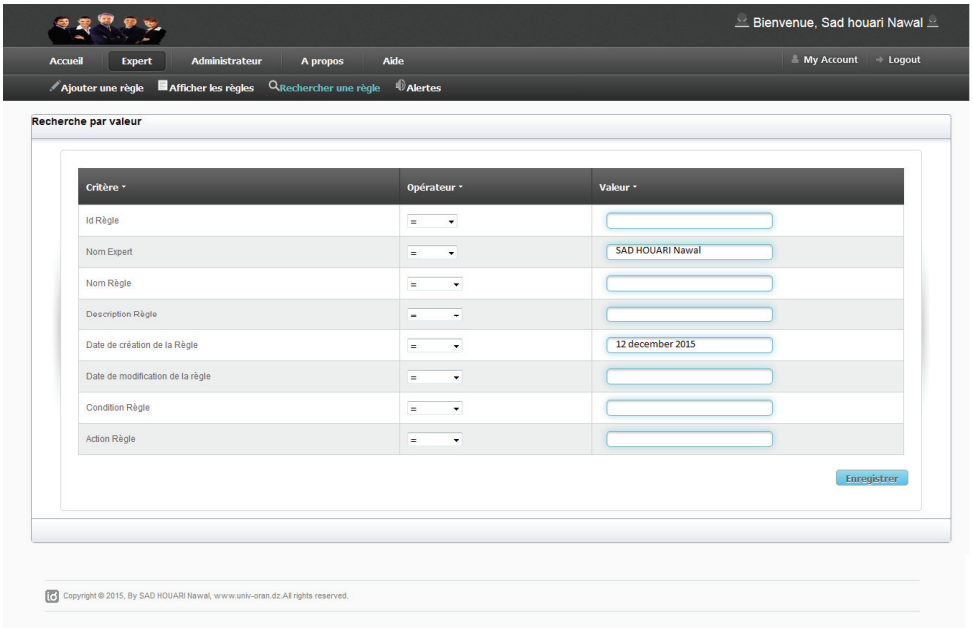

Fig. 7. Search a rule.

6.2 Experimentations

To study the behavior of encryption algorithms in BRMS, we designed and implemented a simulator in order to choose the most suitable and adapted encryption algorithm. We visualized, analyzed, and compared the obtained results by simulating the following encryption algorithms: DES, Blowfish, RC4, and AES.

We chose to use Java as an implementation language and NetBeans 7.0 as a recent open-source runtime environment. We launched the simulations on a computer with Intel Core i5-3230M CPU 2.60 GHz with 4 GB RAM.

We discuss the results of our experiments in the subsections below.

6.2.1 Experiment 1: Response time (ms) with the four encryption algorithms

To measure response time and properly compare competing algorithms, we launched a simulation with only one business rule. Fig. 8 shows that the response time using the RC4 algorithm was reduced and that it had better behavior compared to other competitor algorithms.

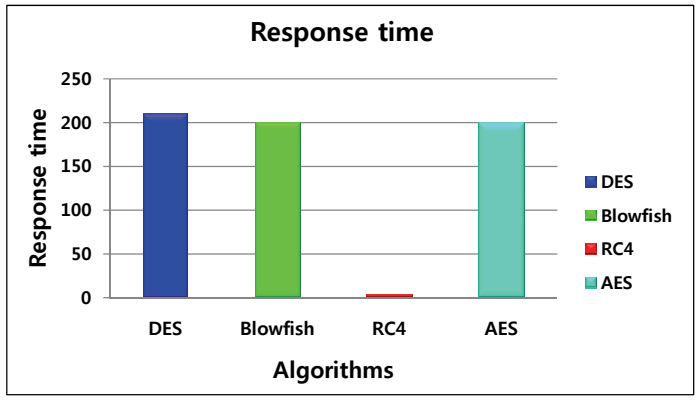

Fig. 8. Response time with the four algorithms.

6.2.2 Experiment 2: Response time (ms) with a different rules base

To measure the impact of the rules number variation on the response time, we varied the number of rules from 10 to 70 by steps of 10. When the number of rules increased, the RC4 response time was always enhanced compared to other competing algorithms (see Table 1).

Table 1. Simulation results 2

Encryption algorithms	10	20	30	40	50	60	70
DES	220	240	260	270	290	300	330
Blowfish	210	220	220	210	210	230	230
RC4	0	10	10	10	16	16	20
AES	210	220	220	221	221	222	222

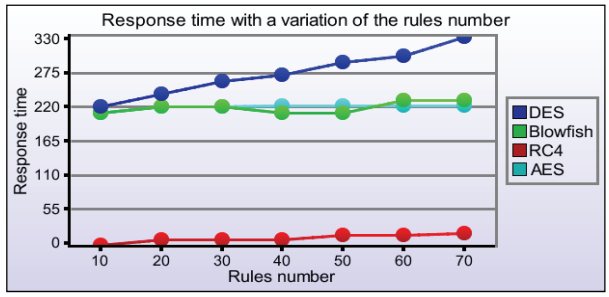

Fig. 9. Response time with a variation of the rules number.

To compare the execution speed with the four algorithms, we calculated the average response time (see Table 2). As shown in Table 2, we can deduce that a rule encrypted with an RC4 algorithm has an average response time (estimated at 11.71 ms) that is greatly reduced compared to other algorithms.

Table 2. Average response time (Experiment 2)

	DES	Blowfish	RC4	AES
Average response time (ms)	272.85	218.57	11.71	219.42

The goal of this experiment is to show that the RC4 algorithm allows scaling. As shown in Fig. 10, the RC4 response time was always better compared to other algorithms with different numbers of rules (the number of rules was varied by 10 steps). According to the results presented in Figs. 9 and 10, the RC4 algorithm provided a gain of 95.70% compared to DES, 94.64% compared to Blowfish, and 94.66% compared to AES.

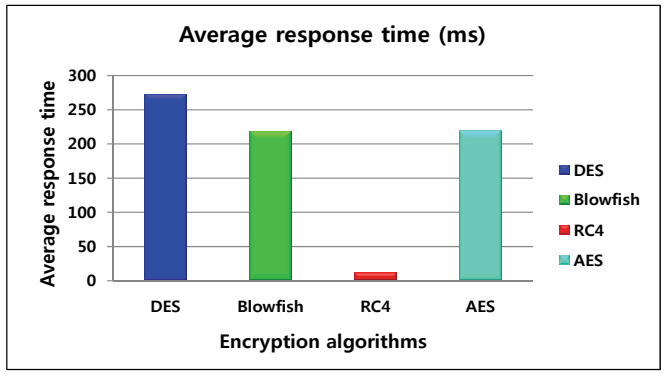

Fig. 10. Average response time with a variation of the rules number.

6.2.3 Experiment 3: Response time (ms) with variations in the size of the rules

The objective of this experiment was to study the impact of rule size on the response time. As shown in Table 3, we noticed that the rule size influences the response time that means, plus the rule size increases plus the response time increases. However, with the RC4 algorithm, the response time was always better compared to other algorithms (0 ms).

The results of this experiment are shown in Fig. 11.

Table 3. Simulation results 3

Encryption algorithms	62	79	122	211
DES	187	188	202	219
Blowfish	156	172	186	203
RC4	0	0	0	0
AES	187	187	203	219

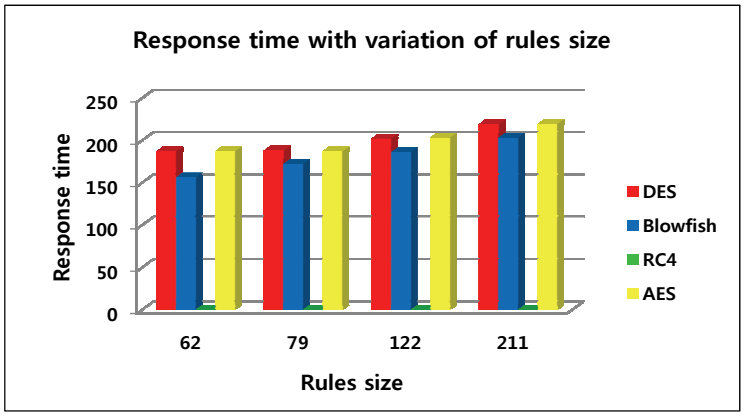

Fig. 11. Response time with variation of rules sizes.

We calculated the average response time (see Table 4), in order to compare the execution speed with the four algorithms.

The results presented in Fig. 12 show that RC4 has better behavior compared to the other algorithms. From Table 4, we can estimate that the average gain for the RC4 was 100% compared to DES, Blowfish, and AES.

Table 4. Average response time (Experiment 3)

	DES	Blowfish	RC4	AES
Average response time (ms)	199	179.25	0	199

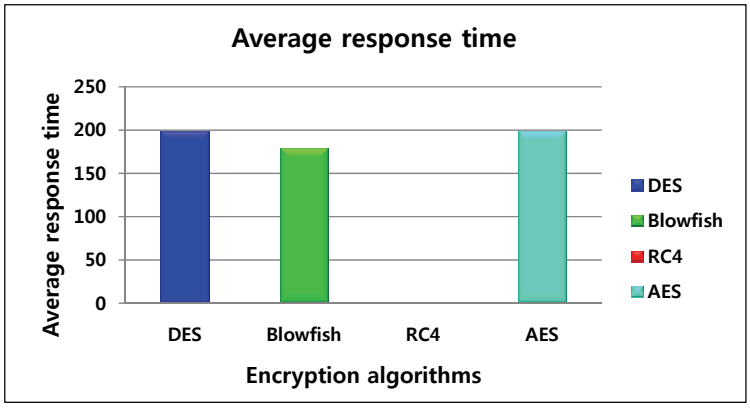

Fig. 12. Average response time with variation of rules sizes.

6.2.4 Experiment 4: Memory space with the four encryption algorithms

To measure memory space and properly compare competing algorithms, we launched a simulation with only one business rule. Table 5 shows that the memory space using the RC4 algorithm was reduced and had better behavior compared to other algorithms.

The results of this experiment are shown in Fig. 13.

Table 5. Simulation results 4

	DES	Blowfish	RC4	AES
Memory space (bytes)	7923920	8180312	3762552	8090072

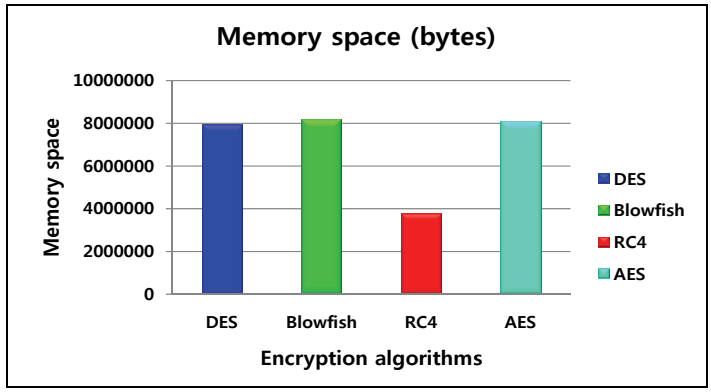

Fig. 13. Memory space with the four algorithms.

6.2.5 Experiment 5: Resistance to the attacks

It is noteworthy that none of the codes already presented guarantees perfect security. However, we considered a code to be safe enough if the computing time to decrypt the encrypted message without the key was not possible on a human scale [20].

Over the past 25 years, the DES algorithm has proven to be a strong algorithm. The only currently known attack is purely academic and has no impact on the practice security of the algorithm. Unfortunately, its weakness resides in the length of the key, which is only 56 bits. Indeed, some calculations showed that it was possible to do an exhaustive research of the key in 256 tests. These calculations are feasible in a limited time and at a relatively reasonable cost [20]. To overcome this, the 2-DES was developed, which consists of encrypting the clear message twice with the DES algorithm. Unfortunately, this doesn't really bring supplementary security because an "attack in the middle" is sufficient to get an expensive cryptanalysis time, but feasible [20]. The solution resides in the use of 3-DES, against which no effective type of attack is known. The message is encrypted with a key k1 and then decrypted with a key k2 before being re-encrypted with the key k1. The use of only two keys (instead of 3) doesn't decrease the security but reduces the computation time. The best known attack against this system is around 2,112 and is therefore impractical if the same key is not used more than 256 times. Unfortunately, even if this way of coding proves safe, it remains quite slow. Indeed, the encryption by DES has a relatively medium speed, and the 3-DES is practically 3 times slower. In addition the DES algorithm treats only blocks of 64 bits [20].

Blowfish is a very powerful algorithm in terms of security in appearance and is very fast. A study organized by *Doctor Dobbs Journal*, showed that Blowfish contained some flaws. In practice, these flaws are not exploitable. Blowfish is relatively new and not very widespread. As such, there is not enough information yet to say if this algorithm is truly powerful [20].

The RC4 encryption is extremely fast and is probably the fastest algorithm used today. However, it has some security flaws that can be exploited more effectively than an exhaustive key search. Fluhrer, Mantin, and Shamir clarified two weaknesses in the specification of the RC4 algorithm [20]. The first rests on the fact that there are large sets of weak keys, that is to say, key which only a few bits are sufficient to determine many bits in the state table S (with high probability), what affects directly the output data; this attack is called "invariance weakness" [20]. The second known attack is the known IV (initial value) attack. It requires, as its name suggests, the knowledge of the IV, which may be the case when it circulates in clear on the network, as well as the knowledge of the first byte of the message M (to find). In a certain number of cases (solved cases, following the expression of Fluhrer, Mantin, and Shamir), the knowledge of these two elements permits the deduction of some information about the key *K* [20]. According to the three researchers, these two attacks are applicable and can permit a complete recuperation of the key with an efficiency that is superior to the attack. However, it is necessary to know that these attacks are not feasible in all cases. So the use of the RC4 encryption in the SSL protocol, for example, is made in order to avoid those two types of attacks [20].

The AES has been deemed totally safe and operational in any type of environment. It effectively answers these requirements, since an exhaustive search of the key is absolutely not envisaged in a limited amount of time (as in, nearly 149 billion years) and has no known attack at this day. It is very effective in terms of speed (much more than the DES). Its memory resource needs are also very weak and it is very easy to implement. This induces a wide variety of platforms and applications. This algorithm can be implemented in software as well as hardware (cabled). Finally, the AES algorithm is relatively simple. These are, among others, these criteria that pushed the world of third generation of mobile to adopt this algorithm for its Millenage authentication scheme [20].

6.2.6 Experiment 6: Security level and performance

The strength of the cryptographic algorithms is not the same as each one has a different level of security. In Table 6 present some information about their levels of security and their performances [25].

Table 6. The security level and performance of the algorithms

	DES	Blowfish	RC4	AES
Security level (/5)	2	5	3	5
Performance (/5)	2	5	5	4

6.2.7 Experiment 7: The objective function

The result of the previous experiment showed the efficiency of Blowfish and AES in terms of security and RC4 and Blowfish in terms of performance. Thus, to obtain a final decision, we calculated the objective function given in Eq. (1), according to two arguments, namely, the security level and the performance of the algorithm.

$$F(X)=S+P \quad (1)$$

Where, F is the objective function, X is the encryption algorithm, S is security level of the algorithm X, and P is performance of the algorithm X.

The obtained results are shown in Fig. 14.

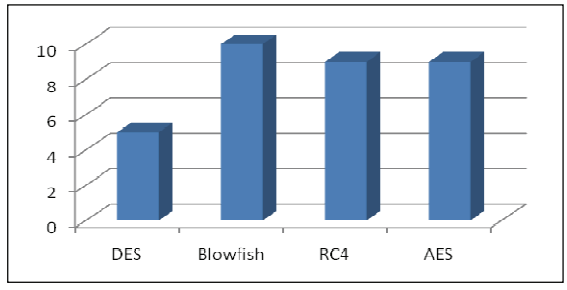

Fig. 14. The objective function.

The results presented in Figure 14 show that Blowfish has better behavior compared to the other algorithms.

6.2.8 Experiment 8: Agent performance

Fig. 15 presents the execution time of the system agents in milliseconds (ms). The execution time of the Expert agent was equal to 281 ms, the execution time of the Translator agent was equal to 780 ms, the execution time of the Evaluator agent was equal to 280 ms, and the execution time of the Security agent was equal to 200 ms.

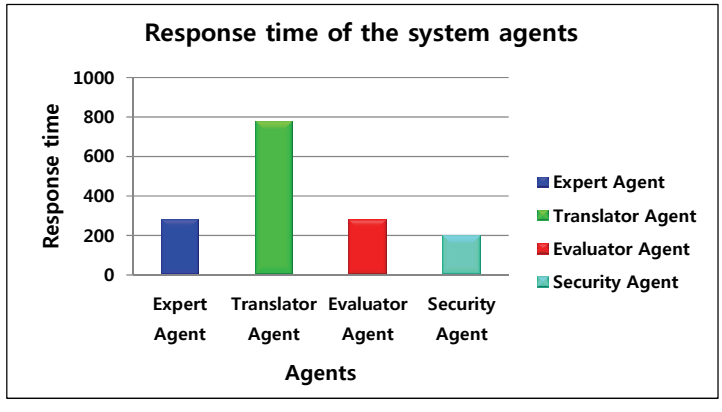

Fig. 15. Response time of the system agents.

6.2.9 Experiment 9: Encryption of the key

A key is data that encrypts and decrypts information after treatment by an algorithm. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secret of the key [19]. As such, the key is the most secret and most important information exchanged

between the sender and the receiver. In our case, we used RSA to encrypt the key. Public keys are stored in a directory. As for the private key, a hash function is applied to the private key then it is ready to be encrypted and stored.

Table 7 presents the execution time of the RSA algorithm and the graphic results of this experiment are shown in Fig. 16.

Table 7. Response time with RSA

Encryption algorithm	10	20	30	40	50	60	70
RSA	2578	3930	6290	9940	11574	14002	16740

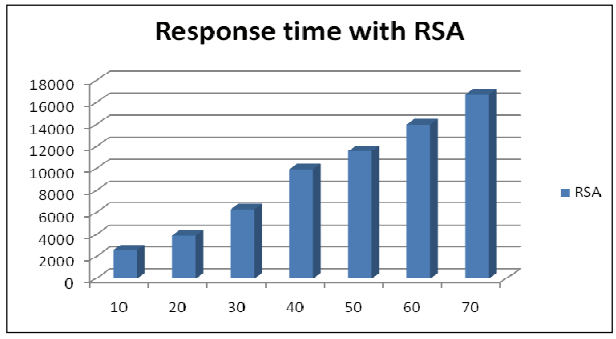

Fig. 16. Response time with RSA.

7. Discussion

According to [26], the efficiency criteria to consider when choosing an algorithm are as follows:

- Security level: resistance to cryptanalysis.
- Key length: security vs. generation costs, transmission, storage.
- Debit.
- Block size: security vs. complexity (implementation cost).
- Complexity of the encryption function: security vs. cost (development and hardware).
- Error propagation.

We tried, through the experiments already presented, to evaluate and study the behavior of each algorithm and to choose the best algorithm to use in rules modeling.

In order to answer to the question: "What is the best cryptographic system–system to secret key or system to public key?" We summarized the advantages and disadvantages of each family in Table 8.

Table 8. Advantages and disadvantages of secret key algorithms and public key algorithms [25]

Cryptosystem	Advantage	Disadvantage
Secret key	- Fast	- Difficulty to distribute the keys
Public key	- Use two different keys - Provides guarantees of integrity and non-repudiation by electronic signature	- Slow and require a lot of calculation

The two basic cryptosystems suffer from additional problems and each has its specificities. The strength of the public key algorithms resides in the key distribution, while the secret key algorithms are very efficient in encryption speed [27]. Thus, the goal of increasing the security of encryption systems certainly passes by the combined use of these two techniques known as hybrid or mixed cryptography [28]. That is to say, in order to take advantage of symmetric and asymmetric algorithms, the modern encryption systems most commonly used are hybrid systems consisting of both secret key algorithms and public key algorithms. The exchange of the secret key is done thanks to the public key algorithm answering the question of secure key exchange. The communication that follows is encoded with the secret key algorithm, which benefits from fast systems that are capable of treating important volumes of data [7].

The previous experiments have shown the effectiveness of the RC4 algorithm in terms of response time and memory space, Blowfish in terms of security level and performance (the results of Blowfish and AES converge in terms of safety and performance level), and AES in terms of resistance to the attacks and complexity. So, while combining the all, we can say that AES is the best algorithm and the most suitable for integration into our BRMS.

Since the solidity of an algorithm depends strongly on the key, we used the RSA algorithm to protect our encryption key.

8. Conclusion

A business expert is one who has acquired significant knowledge and competence in a business field or discipline through years of experience. Although a business expert is a qualified, competent, professional, and experienced specialist in a particular domain, he/she is also human and can make some mistakes.

A big problem today is that system knowledge is always embedded within the minds of business experts, and that knowledge is considered the intellectual capital of the enterprise. However, the solution for how enterprises can still survive after these experts depart is the use of business rules modeling. This encapsulates that knowledge as a content that can be managed by the company in a format that allows for easy transition during personnel turnover. Another advantage of business rules modeling is when this knowledge expressed as business rules can be analyzed automatically, yielding an opportunity to infer additional business intelligence embedded within the set of rules.

Our main objective is to construct a system capable of capitalizing on the expert's knowledge and to keep track of their expertise in a particular domain. The modeling is based on agents to increase the execution speed of processes and effective responses. Therefore, the manipulation of the expert's knowledge generates a need for information security and associated technologies. The notion of cryptography has emerged as a basic concept in business rules modeling.

In order to increase the security of such rules, we used the well-known hybrid or mixed cryptography, so as to benefit from symmetric and asymmetric algorithms. The secret key exchange is done thanks to the RSA public key algorithm. The communication that follows is encoded by using the AES secret key algorithm. We have demonstrated the efficiency of the AES algorithm in terms of response time, space memory, and security through several sets of experiments.

The prototype is currently in progress and is being tested for an ergonomic evaluation especially some company experts are using the collaborative interface to capitalize their knowledge.

References

[1] D. Mouhamed, S. Maabout, K. Musumbu, "Génération automatique de règles métier par enrichissement sémantique de modèles," 2007; https://liris.cnrs.fr/inforsid/sites/default/files/a661c1Ungr88gvmII.pdf.

[2] V. Legendre, G. Petitjean and T. Lepatre, "Gestion des règles «métier»," *Génie Logiciel*, no. 92, pp. 43–52 , 2010.

[3] Chniti, P. Albert, and J. Charlet, "Gestion de la cohérence des règles métier éditées à partir d'ontologies OWL," in *Proceeding of the 22nd French National Conference on Knowledge Engineering (IC2011)*, Chambéry, France, 2011, pp. 589-606.

[4] D. Loshin, "Business rules," in *Business Intelligence*, 2nd ed. Waltham, MA: Morgan Kaufman, 2013, pp. 147-163.

[5] M. L. Nelson, J. Peterson, R. L. Rariden, and R. Sen, "Transitioning to a business rule management service model: case studies from the property and casualty insurance industry," *Information & Management*, vol. 47, no. 1, pp, 30-41, 2010.

[6] "La cryptographie definition," http://tpe-messages-secrets.e-monsite.com/pages/la-cryptographie/.

[7] Berzati, "Analyse cryptographique des altérations d'algorithmes," Ph.D. dissertation, University of Versailles Saint-Quentin en-Yvelines, 2010.

[8] M. Videau, "Critères de sécurité des Algorithmes de Chiffrement à clé secrète," Ph.D. dissertation, PARIS 6 University, 2005,

[9] N. Sad Houari and N. Taghezout, "A combined use between rules, ontology and agents in BRMS design: application to SME in Algeria," in *Proceedings of International Conference on Artificial Intelligence, Energy and Manufacturing Engineering (ICAEME'2015)*, Dubai, 2015, pp. 11-17.

[10] Chniti, "Gestion des dépendances et des interactions entre Ontologies et Règles Métier," Ph.D. dissertation, PARIS 6 University, 2013.

[11] "Collaboration definition," https://en.wikipedia.org/wiki/Collaboration.

[12] "Collaboration definition," http://whatis.techtarget.com/definition/collaboration.

[13] S. Ram and J. Liu, "An agent-based approach for sourcing business rules in supply chain management," *International Journal of Intelligent Information Technologies*, vol. 1, no. 1, pp. 1-6, 2005.

[14] J. Ferber and J. F. Perrot, Les systèmes multi-agents, vers une intelligence collective. Paris: InterEditions, 1995.

[15] D. Lavbic and R. Rupnik, "Multi-agent system for decision support in enterprises," *Journal of Information and Organizational Sciences*, vol. 33, no. 2, pp. 269-284, 2009.

[16] Lopez-Ortega and I. Villar-Medina, "A multi-agent system to construct production orders by employing an expert system and a neural network," *Expert Systems with Applications*, vol. 36, no. 1, pp. 2937-2946, 2009.

[17] M. Bajec and M. Krisper, "A methodology and tool support for managing business rules in organisations," *Information Systems*, vol. 30, no. 6, pp. 423-443, 2005.

[18] "Cryptography definition," http://searchsoftwarequality.techtarget.com/definition/cryptography.

[19] G. Soula, "La sécurité des réseaux numériques, cryptologie et autres techniques," 2008 ; http ://cybertim.timone.univ-mrs.fr/enseignement/doc-enseignement/informatique/securite%20reseaux%20techniques/docpeda_fichier.

[20] R. B. Philippe, "Principaux algorithmes de cryptage," 2002 ; http ://prolland.free.fr/works/security/algo_crypto.pdf.

[21] V. Bernet-Rollande and S. Lallemand, "Rapport de TX Etude d'une attaque contre l'algorithme RC4," 2010.

[22] "Advanced Encryption Standard," http://math.univ-lyon1.fr/~roblot/resources/masterpro_chapitre_4.pdf.

[23] Lan and B. Vandevelde, "Panorama des algorithmes de cryptographie," 2011; http://veille-techno.blogs.ec-nantes.fr/wp-content/uploads/2011/10/Crypto_final.pdf.

[24] Stineman, "Pourquoi des règles métier?: un cas pour les utilisateurs métier de l'informatique," 2009; ftp://public.dhe.ibm.com/software/fr/ilog/IBM_ILOG_-_Pourquoi_des_regles_metier.pdf.

[25] "Quel algorithme de chiffrement symétrique (symmetric cipher) choisir?" 2012; http://www.blog-des-telecoms.com/quel-algorithme-de-chiffrement-symetrique-symmetric-cipher-choisir/.

[26] Bruasse-Bac, "Algorithmes de chiffrement par bloc," https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/Algorithmes%20de%20chiffrement%20par%20bloc.pdf.
[27] Ali Pacha and N. Hadj-Saiad, "La Cryptographie et ses principaux systèmes de références," *RIST: revue d'information scientifique et technique*, vol. 12, no. 1, pp. 173-193, 2002.
[28] "Hybrid encryption," https://www.techopedia.com/definition/1779/hybrid-encryption.

Nawal Sad Houari

She received her Master degree in Information System Technologies at University of Oran1 Ahmed BenBella, Algeria in 2013. Currently, she is a Ph.D. student in Computer Science Department at the same University. Her research interests include business rules modeling, Artificial Intelligence, Security, multi-agents system and knowledge management.

Noria Taghezout

She is an assistant professor at University of Oran1 Ahmed BenBella, Algeria. She holds her doctorate thesis in MITT at PAUL SABATIER UNIVERSITY in France in 2011. She also received another doctorate thesis in Distributed Artificial Intelligence from University of Oran1 Ahmed BenBella in 2008. She holds a Master degree in Simulation and Computer aided-design. She conducts her research at the LIO laboratory as a chief of the research group in Modeling of enterprise process by using agents and WEB technologies. Since she studied in UPS Toulouse, she became a member of the EWG-DSS (Euro Working Group on Decision Support Systems). She is currently lecturing Collaborative decision making, Enterprise management and Interface human machine design. Her seminars, publications and regular involvement in Conferences, journals and industry projects highlight her main research interests in Artificial Intelligence.