Mathematical Modelling in Cyber Security Management

Electra MITAN
National institute for Research and Development in Informatics - ICI Bucharest
electra.mitan@ici.ro

Abstract: Cyber security is the most critical aspect of the technological-based lives. The increasing interest in it leads to adopt computer architectures, with a close relationship between hardware, sofware and security. The paper presents the case of applying a Multi-Attribute Decision Making model and Onicescu solving method, in order to select a hardware - software infrastructure used to acquire and process the information concerning computer security incidents. Each pair hardware - software infrastructure is evaluated using a set of characteristics. The pair with the greatest evaluation value is the optimal solution.

Keywords: Cyber Security, Critical Infrastructure, Data Base Management System, Multi-Attribute Decision Making

INTRODUCTION

The rapid development of modern information and communication technologies has had a major impact on the social whole, which has led to transformations in the functioning of the economic, political and cultural, but also on the daily life of the individual. Easy access to ICT is one of the prerequisites for the proper functioning of modern society.

The cyber space does not know borders; it is characterized by dynamism and anonymity, being able to generate both opportunities for the development of the information society based on knowledge and risks to its functioning (at the individual, country and even cross-border level).

Romania is pursuing the development of a dynamic information environment based on interoperability and services specific to the information society. At the same time, the fundamental rights and freedoms of the citizens, the interests of national security, in an appropriate legal framework must be ensured. A computerized society is more vulnerable, and ensuring the security of cyber space must be a major concern of all the actors involved, especially at the institutional level, where it is necessary to develop and apply coherent policies.

Each year the public and private organisations invest millions of euros on hardware devices, security software and technologies; the cyber security will increase inside these organisations, but they are still vulnerable.

To ensure computer security is to provide of the means, methods and mechanisms for preventing the unauthorized destruction, modification or use of software and computer systems data.

At European level, but also in each member state, there are multi-level structured bodies that follow the evolution of the anthropic IT incidents produced by IT means in order to establish policies to combat this phenomenon.

ENISA, the European Union Agency for Cybersecurity, is a centre of expertise for cyber security in Europe which helps the EU and EU countries to be better equipped and prepared to prevent, detect and respond to information security issues (https://www.enisa.europa.eu).

ARNIEC, the Management Agency of the National Network for Education and Research, manages and develops the RoEduNet network that provides data communication services for the research and academic institutions of all degrees in Romania (https://www.edu.ro/search/node/arniec). In the European context, the Agency is a member of the GEANT consortium (which is a fundamental element of Europe's e-infrastructure, delivering the pan - European network for scientific excellence, research, education and innovation), the network that interconnects all research and education networks in European Union countries (https://www.geant.org).

critical manufacturing, emergency services, communications, information technology, financial services, government facilities, healthcare and public health, materials and waste. The main attacks on critical infrastructure / industrial control systems can be included in five groups that depend on the attacker objectives: corruption of information, denial of service, disclosure of information, theft of resources, physical destruction *[Maniatakos, 2017]*.

The risk management practices for the better protection of the communications critical infrastructure must be evolved. In order to accomplish this, a common set of guiding security principles to foster 'security-by-design' are necessary and can be done by building security concepts into hardware - software from the developmental stages to the "end of life" (fcc.gov/annual-reports).

CERT-RO (National Cyber Security Incident Response Center) is a specialized organizational entity with independent structure of expertise and research and development in the field of cyber infrastructure protection. CERT-RO is also national contact point with similar structures that analyzes the procedural and technical dysfunctions at the level of cyber infrastructures (cert.ro). The main activities concern to ensure cyber security through strong regulations, to share NIS implementation challenges, to balance cyber security and privacy in order to developa strong cyber security industry.

ORNISS (National Registry Office for Classified Information) performs regulation, authorization, evidence and control tasks on the protection of classified information (orniss.ro). The protection of classified information was a prerequisite for Romania's accession to NATO but also after obtaining full membership. The occurrence of security incidents can interrupt the flow of classified information, which can mean the impossibility of effective participation in the relevant activities of the Alliance. It is a national strategic interest, therefore, it is necessary to ensure the protection of classified information by: a) a proper management of them by each owner, in accordance with the regulations in force; b) security education, part of the Euro-Atlantic security culture, an education necessary to form a proactive attitude, with the broad, conscious and responsible involvement of the Romanians.

Security policies include a worldwide certification process; thus, global secure security systems can be built. A computer system includes: tangible elements (servers, PCs, laptops), and intangible elements (system content, processes). Physical protection is related to the protection of the tangible part, i.e. the physical protection of the equipment. Security services protect the intangible part - confidentiality of information (access is allowed to authorized persons), integrity of information (protection against malicious changes of information), availability of computer system. Critical infrastructure sectors include: energy, dams sector, nuclear reactors, chemical, defense industrial base, food and agiculture, transportations systems, water and wastewater systems, commercial facilities,

Computer security gained a bigger importance in the fight against different events occasioned by computer attacks. According Norton (https://www.nortonsecurityonline.com), nowadays computer crimes refer to: virus performing in a computer, answering a fake e-mail, entering an electronic site that captures personal data, person that accessed the email / social network account of another without permission, responding to on-line scam, fraud during making on-line card payment, receiving an e-mail / a call from a computer company saying the computer is infected. The interest for cyber security is constantly increasing and requires the use of high performance computers. The relationship between hardware, software and security is very close.

The increasing interest in cybersecurity leads to addopt computer architectures turning it into a close relationship between hardware, sofware and security.

Security features require special components (hardware, software). From the technical point of view, there are two major aspects:

- network communication security (Internet security, public communication network);
- information security system (information protection based on completeness, confidentiality, authorized access).

The design of a security network involves the construction of a modular architecture consisting of: servers, management system, networks, external connections (Internet, WAN), system access providers (Internet, telephony network providers). The physical infrastructure includes networks, sub-networks, components (applications, computer system, communication features); for each one are identified possible attacks and / or technological answers (cryptographic systems, tunneling characteristics, filtering address, control stations, firewall configuration, authentication, intrusion detection systems) *[Bulakh et al., 2016]*.

The infrastructure of the information systems must be optimal to ensure the functionality of the system, corresponding to the efficiency requirements. The paper presents how to build the optimal of a software - hardware infrastructure starting from available entities.

After a short review on characteristics of Data Base Management Systems (DBMSs), the security databases focusing on their characterization vector (distribution, structuring, number of users, size, dynamics, storage, content) are presented. The modelling mathematical methodology highlights the optimum over a homogeneous set of independent entities and two models for optimum choice problem are presented: Decision Theory model and Multi-Attribute Decision Theory model. Solving a multi-attribute decision problem supposes its normalization. There are presented a normalization method and a solving method. An example is included to prove support in choosing the infrastructure on which the database runs for the acquisition of incident information.

SECURITY DATABASES

A database is an organized collection of information / structured data, electronically stored in a computer, and usually controlled by a DBSM. The main criteria based on which the databases are divided are: distribution, structuring, number of users, size, dynamics, storage, content, as follows:

- distribution of data and applications - centralized, distributed, federative, mobile databases;
- structuring data - structured databases (hierarchical, relational, object-oriented), unstructured (audio / video, topological, Big Data);
- number of users - single-user, multi-user databases;
- size - small, medium, large, very large databases;
- data dynamics - operational, analytical databases;
- data storage mode - databases stored on disk, stored in memory;
- digital content - traditional databases (scientific, technical-economic, managerial, administration, socio-humanistic), audio/ video, multimedia, space, documentation, bibliographic, security.

Security databases handle all incidents registered in computer systems/ Intranet networks/ a well-delimited area of the Internet. The following incidents are considered as important ones that must be registered and used by the decision-making bodies in ensuring the computer security:

- appearance of viruses, worms etc on a computer in the secured area;
- sabotage the firewall installed for the protection of some web applications;
- poor functioning of electronic mail systems by word viruses, flooding messages;
- poor functioning of search engines on the Internet through overruns of advertisements or information requested by the user in a previous session;
- violation of account (username and password) to access an application;
- non-observance of access rights to certain information;
- ignoring the secret character of encrypted information;
- destruction of the integrity of the files / databases.

The following incident information is recorded:

- information about the place of the occurrence, the date of occurrence, the damages produced and the way of solving the incident;
- information processed graphically, statistically, reports to international bodies with attributions in computer security.

Internet-based computer users have providers of this service that must manage the sub-network formed by their clients' computers. As a consequence, a first level of the database for the acquisition of incident information can be formed from the databases of Internet providers. The case of large computer networks is a special one. Network administrators also deal with security; they must also manage a database for the acquisition of incident information. This is the case for corporations, banks, businesses, etc. If these databases run independently, each of them must be coupled with a central database, hosted by a national body with tasks in computer security (for example, CERT) that can perform complex and complete analyzes at the Romanian level. According to the case analysis from the point of view of distribution, it can be concluded that the DBMS must be able to generate a federative database.

Each network administrator takes care of several computers linked to each other; this topology will obviously influence the spread of viruses in the network. The network entry server, on which the network firewall is installed, will create a precedence relation with the rest of the computers. It has to consider that the upper level contains strongly interconnected analysis indicators. The database needed to record incidents must be one that allows structuring, and moreover, it must be *relational*.

Considering the number of users, it is obvious that the database must be multi-user.

There may be several hundred databases at the first level (local) and one database at the top level (national). Perhaps it would be more rational for the system to have three levels, which means there is an intermediate level at the county level that would take over the functions initially provided for the national level. Thus, it remains with the function of maximum synthesis and offers decision support for the establishment of future development policies of tools related to computer security. It should also be kept in mind that the system must be interconnected with other national systems with which it has to exchange information on request or periodically. In conclusion, the database is *very large*.

Database manages very large volumes of current data and in addition the statistical data must be kept in order to be able to determine the evolution of certain phenomena related to computer security. As a consequence, the storage medium of the database will be the disk.

At the basic level, any delay in recording the incidents will lead to the wrong decision making of operative decisions. At the upper level, by doing tactical or strategic processing, may require the basic level to update its data before launching the specific processing of this level. Thus, the basic level of the database must be operational, the upper level must be analytical.

Considering the content, the database is *traditional*. Within this class it is of a managerial type because it had to take into account the management of the information security activity at operational, tactical and strategic level.

Based on this, the pattern considered specific to DBMSs capable of generating databases for recording incidents has the characterization vector: federative, relational, multi-user, very large, operational + analytical, disk, security.

An example is SECURITY-DATABASE (France) that contains data needed for IT security and expertise for real-time anticipation of hazards with an impact on IT infrastructure (hardware and software). CWE (Common Weakness Enumeration), OVAL (Open Vulnerability and Assessment Language). It is compatible with CVE (Common Vulnerability Enumeration), CAPEC (Common Pattern Enumeration), CWE (Common Weakness Enumeration), OVAL (Open Vulnerability and Assessment Language) (security-database.com).

MATHEMATICAL MODELING METHODOLOGY

In order to highlight the optimum over a homogeneous set of independent entities with computable or observable charateristics, the modelling mathematical methodology supposes the following steps:

- considering the entities with their charateristics an analyse can be done to point the goal of the mathematical model;

- taking in consideration as many charateristics as possible, a complete and complex taxonomy can be done (Everitt et all., 2009); using this taxonomy, each entity is assocated to a class;

- the items belonging to classes that are not suitable for the purpose of optimization are eliminated;

- a mathematical model is accomplished by making use of MADM theory; the entities with their characteristics and all the necessary information for optimization are highlighted *[Yoon & Hwang, 1995; Tzeng & Hwang, 2011]*;

- over the mathematical model, problems are generated and solved using different optimal choice problems;

- if a multiple optimum is obtained, a procedure that uses of an extended set of attributes is applied in order to obtain the global optimum.

In order to obtain an optimum hardware and software infrastructure able to acquire and process the information related to anthropic computer incidents *[Resteanu et al., 2015]*, using this methodology is useful and strictly to apply.

DECISION THEORY MODEL

A first model for optimum choice is the classic Decision Theory model. This proposes the interaction of two actors: the man endowed with logical judgment and the nature with probabilistic behavior. The man is named here decision-maker and his job is to perform calculations and analyze on the basis of which he can decide on the action that will bring him the greatest profit.

Nature cannot achieve anything from what man can do, it selects probabilistic states. Consequently, there are two fundamental concepts in this theory, namely the actions and the states of nature.

The actions are under the control of the decision-maker; any available action can be selected by the decision-maker. The states of nature are under the control of nature, they are probably selected by nature, but they cannot be under the control of the decision-maker. In this context, a decision problem is represented by a pair $<S, A>$ composed of a lot of states of nature S and a lot of actions A. Thus defined, the pair $<S, A>$ is a decision model under conditions of uncertainty. If the states of nature have a system of probabilities associated, then $<S, A>$ is a decision model under risk conditions.

The decision theory postulates that the human decision-maker brings in modeling his own beliefs and preferences. Specifically, the theory assumes that decision-maker has a probability system, which surprises its beliefs concerning the choice of the states of nature, a system of confidence regarding the results obtained by performing actions in different states of the nature and a structure of preferences over the results. Thus, the decision-maker is the triplet $<P, G, U>$ composed of a measure of probability P, a function of the gains G and a utility function U.

The probability measure P is defined over the states of nature set, and it captures the decision-makers' opinion in the process through which the states of nature are naturally selected. G is defined on the Cartesian product of the states of nature and actions and presents the results obtained from performing each action in each state of nature. Thus, G generates a new set O of the results. The utility function is defined on the set O of the results and represents the decision-makers' preference over the results, that is, $F:O \rightarrow R+$. Function F acts through the principles of optimality or may have an analytical expression according to the needs of the decision-maker. Usually, the standard working form of these models is used, that is given by the so-called decision matrix (***Table 1***), in case of opt_1, ..., opt_i options and c_1, ..., c_j criteria. A problem consists of a model defined above, essentially the decision matrix, and the function F, most often an optimal principle chosen from a lot of such principles validated over time in an impressive set of practical cases. The decision rules consist of two commands. The first command tells the user how to assign winnings to the actions; the second order tells the user how to choose between the gains assigned by the first order. Decision rules are designed to reflect people's attitude to the decision making process.

	c_1	c_2	c_3	…	c_j
opt_1	c_{11}	c_{12}	c_{13}	…	c_{1j}
opt_2	c_{21}	c_{22}	c_{23}	…	c_{2j}
opt_3	c_{31}	c_{32}	c_{33}	…	c_{3j}
⋮	⋮	⋮	⋮		⋮
opt_i	c_{i1}	c_{i2}	c_{i3}	…	c_{ij}
	p_1	p_2	p_3	…	p_{1j}

Table 1*. Decision Matrix - Model of Decision Theory*

The Expected Value Principle (Realistic)

This method appeals to the probabilities of the states of nature. As a result, we can say that it is a method of risk-solving. The expected value is calculated, for each action, by multiplying the winnings with the corresponding probabilities and summing the results of the multiplication, along the states of nature. The optimal action is the one for which the highest value is obtained. The criterion of expected value is also called the Bayesian principle.

The Maximax principle (Optimistic)

This principle states that, in Step 1, in turn, for all the states of nature, the action with the highest gain is chosen. In Step 2, one chooses the action that has the highest value obtained in Step 1. This principle is also called the best of the best.

The Maximin principle (Pessimistic)

This principle states that, in Step 1, in turn, for all the states of nature, the action with the least gain is chosen. In Step 2, one chooses the action that has the highest value obtained in Step 1. This principle is also called the weakest of the weakest.

The Minimax Principle (Loss of Opportunity)

This principle states that, in Step 1, in turn, for all the states of nature, the action with the highest gain is chosen. In Step 2, one chooses the action that has the lowest value obtained in Step 1. This principle is also called the principle of loss of opportunity or regret.

As a consequence, both the decision making process under uncertain conditions and at risk conditions were taken into consideration.

A second model for optimal choice is the Multi-Attribute Decision Theory model that is presented below.

OPTIMAL CHOICE MODEL. SOLVING METHODS OF MADM PROBLEM

The assessment and optimal choice model belongs to the Multi-Attribute Decision Making (MADM) domain. This is a multiple decision-makers one. The entities involved in modele defining are:

1) Decision-makers set $D = \{d(k) | 1 \leq k \leq K\}$, that is discrete and finite, with at least three elements.

The decision-makers are specialists having the task to choose the optimum hardware - software pair. Every element $d(k)$ is characterized by: $d\_code(k)$ – code; $d\_name(k)$ – name; $d\_description(k)$ – short description; $d\_weight(k)$ – weight; $WD=\{d\_weight(k) | 1 \leq k \leq K\}$ represents the vector of experts' weights.

2) Objects set $O = \{o(i) | 1 \leq i \leq I\}$, that is discrete and finite, with at least one element.

The objects are hardware - software pairs to be assessed and submitted to optimal choice.

Every element $o(i)$ is characterized by: $o\_code(i)$ – code; $o\_name(i)$ – name; $o\_$

$description(i)$ – description; $o\_eval(i)$ - object's evaluation computed.

3) Attributes set $A = \{a(j) \mid 1 \le j \le J\}$, that is discrete and finite, with at least one element.

The attributes are software products' characteristics and they are taken as discriminators.

Every element $a(j)$ is characterized by: $a\_code(j)$ – code; $a\_name(j)$ – name; $a\_description(j)$ – description; $a\_expression(j)$ – mode of expressing (cardinal / ordinal / Boolean / fuzzy / random variables); ($a\_low(j)$, $a\_upper(j)$)

– variation ranges; $a\_sense(j)$ – sense, that can be ascending (A), if $a(j)$ is considered the better for the largest values, or descending (D), if $a(j)$ is considered the better for the smallest values; $a\_weight(j)$ – absolute weight that is characterised by properties:

$$0 < a\_weight(j) \le 1, \ (\forall) 1 \le j \le J \quad \sum_{j=1}^{J} a\_weight(j) = 1$$

$AW = \{a\_weight(j) \mid 1 \le j \le J\}$ represents the vector of attributes' absolute weights;

$$a^{l}_{j_1 j_2} \quad 1 \le l \le L, \ \ 1 \le j_1, j_2 \le J$$

- one to one attributes' influences in the opinion of $e(l)$ expert.

$$A^{l} = \{a^{l}_{j_1 j_2} \mid 1 \le l \le L, 1 \le j_1, j_2 \le J\}$$

represents the 3-dimension massive containing the influences.

4) Decision matrix $OA = \{oa(i, j) \mid 1 \le i \le I, 1 \le j \le J\}$ is a 2-dimension ($I \ x \ J$) matrix, that reffers the relation between the objects and the attributes sets, where every $oa(i,j)$ is the j attribute's value corresponding to the i object.

5) Matrix of relativ importances of the attributes $AA = \{irel\_aa(j_{1,} j_2), 1 \le j_{1,} j_2 \le J\}$ is a 2-dimension ($J \ x \ J$). The relative importance of the attribute related to the attribute is a positive real number that expresses how many times the attribute is more important than the attribute $a(j_2)$.

6) Evaluation matrix $Eval\_od = \{eval\_o(i) \mid 1 \le i \le I\}$, each element $eval\_o(i)$ represents the place that the object $o(i)$ occupies in a hierarchy given by a method of solving. This set has the significance of the image of function $E{:}O \to R^{+}$ and represents the problem solving.

Thus, the MADM model is entirely defined. This model is referred by all the solving methods existing in the specialized literature *[Resteanu et al., 2007]*. Solving the problems that are generated over this model leads, depending on the purpose pursued, to determine an optimal or pessim object or to achieve a hierarchy of the objects or to carry out an evaluation of each object.

The MADM problem can have a high degree of complexity even if only a few attributes are considered. The increase in complexity is due to the fact that in real problems, the attributes are conflicting. An object can be rank on a very good position in relation to one of the attributes and on a very bad position in relation to another attribute. It verifies:

- the syntactic correctness (the good organization of the data in the massifs defined by the theoretical model);
- the semantic correctness (the data in the model reflects the reality one by one);
- the completeness (all the massive ones in the model are dense);
- the credibility (the values of the attributes can be associated in reality model objects).

Solving a multi-attribute decision problem supposes its normalization. This means that the data will be in the range [0, 1]. The normalization method von von Neumann - Morgenstern is given below.

The linear function $y=ax+b$ is determined so that we have the linear system:

$$\begin{cases} 0 = a \cdot pesim\_a(j) + b \\ 1 = a \cdot optim\_a(j) + b \end{cases} \qquad (1)$$

with a,b unknown.

By solving it, we obtain the linear transformation:

$$y = \frac{x - pesim\_a(j)}{optim\_a(j) - pesim\_a(j)} \qquad (2)$$

The principle of the method consists in the interpolation through this linear function of the attribute levels for each object. By interpolation, it is obtained for the worst value $pesim\_a(j)$, the normalized value 0 and for the optimal value $optim\_a(j)$, the normalized value 1. This is the most used method of normalization.

Solving methods

There are classes of mathematical tools with which, from case to case, MADM problems can be solved. These include: the calculation of dominance, evaluation functions, the calculation of distance in various norms, the allocation of scores or scores, etc. In any case, the decision-maker must orient himself towards one of these classes of methods.

The analysis of the mathematical solving techniques of the optimal choice problem highlights two distinct classes of solving methods:

- methods of objects evaluation;
- methods of characterization of objects.

The methods of objects evaluation explicitly express, in relation to the purpose of the problem, each object or only part of the objects set. Effectively, these methods determine the optimal solution of the problem. These methods can be of compensatory or non-compensatory type, they can calculate the utility of each object in the von Neumann - Morgenstern sense, they can provide an object hierarchy, or they can choose an optimal object/class of objects without providing information concerning the other objects.

Evaluation methods: MAXIMIN, MAXIMAX, Pareto, TOPSIS, Onicescu, TODIM, scores, diameters, linear utility function method *[Yoon & Hwang, 1995; Onicescu, 1970]*.

Objects characterization methods do not provide explicit appreciation according to the purpose of the problem. They provide, for each object, information that outlines an image about its characteristics.

Applying of these methods allows to reduce the dimensions of the problem and to establish the relations of dominance and of good / weak appreciation by each attribute on the set of objects. Characterization methods allow discrimination in the set of optimal solutions and discrimination between optimal solutions determined by applying a set of evaluation methods to the given problem. Based on this information, the merit of the classes resulting from the application of the knowledge-based simulation techniques is determined, leading to the acceleration of the procedure for determining the global optimality of the problem.

Characterization methods: the number of objects dominated by each object, the number of dominant objects for each object, the minimum number of characteristics by which the objects are best evaluated, the maximum number of characteristics by which the objects are best evaluated, the minimum number of characteristics by which the objects are worst rated, maximum number of features by which objects are worst rated method.

If, using several solving methods, different solutions have been obtained, the global optimum is built.

Solving the multiple optimum

In the case of a Decision Theory problem as well in the case of a Multi-Attribute Decision Theory problem, a multiple optimum can be obtained. In this case, the decision making context is similar. This means that more states of nature and more attributes are added to the decision matrix and the problem is solved. If the obtained optimum is a multiple one, the procedure is repeated.

Next, the Onicescu method *[Onicescu, 1970]* and an amended version of it are presented.

Onicescu method

The method uses the function $loc\_oa:\{1,...,\mathbf{i}\}\ x\ 1,...,\mathbf{j}\} - N$, $loc\_oa(i,j) =$ the place ocupied by the object $o(i)$ in the hierarchy induced by the the attribute $a(j)$ (in relation to its sense) for any $i=1,I$, $j=1,J$. If two or more objects occupy the same place in relation to a given attribute, the immediate next place is not left vacant but is assigned in the order to the following objects.

The method starts both directly from the matrix of consequences and from its normalized form.

The algorithm is presented below:

The matrix $nap\_o: = (nap\_o(i,\acute{a})\ _{\substack{i=\overline{1,\mathbf{i}} \\ \acute{a}=\overline{1,\mathbf{i}}}}$ is determined starting from the matrix loc_oa.

The algorithm starts with this null matrix and, going through its elements loc_oa for each $loc\_oa(i,\ )=t$ calculates $nap\_o(i,\ ):=nap\_o(i,\ t)+1$

Step 1: The places matrix is built loc_oa.

Step 2: The elements are calculated.
Step 3: STOP.

Onicescu amended method

For the case where the coefficients of importance

$$eval\_o(i) = \sum_{j=1}^{\mathbf{i}} \frac{a\_weight(j)}{2^{loc\_o(i,j)}}, \quad \forall i = \overline{1,\mathbf{i}} \qquad (3)$$

were provided, Onicescu proposed that the elements of the weights vector be calculated using the formula,

$$a\_weight(j) = \frac{1}{2^j}, j=1,J$$

So, the method relates to the fact that instead of the string

$\frac{1}{2^1}, \frac{1}{2^2}, \ldots, \frac{1}{2^{\mathbf{i}}}$ it is used the string *1, 2, ..., **i**.*

The method checks the third axiom of Arrow and, in addition, raises no problems in memorizing the numbers. form $1/2^i$ where $i > 32 / 64 / etc.$ The quoted axiom refers to the fact that if the objects are sorted against each other in a certain way according to a method and if an object or more is removed from the set of objects a new ordering by the same method will give the same relative ordering for the remaining objects.

For each attribute A, $A=1,AA$, the line vector *WNValue(A,OO)* is considered. This vector is ordered decreasing by the values of that attribute. Thus, there are AA orderings of the objects. Based on them, a vector is calculated. The vector elements show how many times an object occupies the 1, 2, 3, ..., OO places. The vector thus obtained is scalarly multiplied by the vector of attributes *WNImportance (AA)* and each component is divided by its rank. Obviously, we work in complementarity with 1 so that the optimal object has an evaluation as close to 1. This fact is really possible if at the end of each evaluation of *WNValue(0,O)*, *O=1,OO*, is divided by the maximum after *O* of these evaluations.

In the following is presented the pseudocode for this method.

```
PROCEDURE (AA, OO, WNImportance(AA), WNValue(AA, OO))
INTEGER  A, O, I, Sigma(OO)
REAL Max, WNImportance(AA), WNValue(AA, OO)
Max=0
DO FOR O=1,OO
    WNValue(0,O)=0
ENDDO
DO FOR A=1,AA
    SORT DESCENDING WNValue(A, OO) GIVING Sigma(OO)
    DO FOR O=1,OO
        DO FOR I=1,OO
            IF Sigma(O)=I  THEN
                WNValue(0,O)=WNValue(0,O)+ WNImportance(A)*(OO-I)/I
            ENDIF
        ENDDO
    ENDDO
ENDDO
DO FOR O=1,OO
    IF WNValue(0,O)> Max
       Max= WNValue(0,O)
    ENDIF
ENDDO
DO FOR O=1,OO
    WNValue(0,O)=WNValue(0,O)/Max
```

```
ENDDO
ENDPROCEDURE

//Onicescu amended
void subrutine (int AA,int OO,float WNValue[25][25],float WNImportance[25])
{int a,o, q[25],ii,jj,poz=0;
float max;
max=0;
for(o=1; o<=OO; o++)
WNValue[0][o]=0;
for(a=1; a<=AA; a++)
 {
           for(ii=1; ii<=OO;ii++)
           {  poz=0;
                     for(jj=1; jj<=OO; jj++)
                if(WNValue[ii][a]>WNValue[jj][a]) poz++;
      if(poz==0) q[ii]=1;
             else q[ii]=OO-poz+1;
           }
 for(o=1; o<=OO; o++)
 {WNValue[0][o]=WNValue[0][o]+WNImportance[c]*(OO-q[o])/q[o];
   }
}
for(o=1; o<=OO; o++)
if(o==1) max=WNValue[0][o];
else if(max<WNValue[0][o]) max=WNValue[0][o];
for(o=1; o<=OO; o++)
 WNValue[0][o]=WNValue[0][o]/max;
for(o=1; o<=OO; o++)
cout<<WNValue[0][o]<<” “;
cout<<endl;
}
```

EXAMPLE OF USING THE MADM MODEL TO SELECT AN INFRASTRUCTURE FOR ACQUISITION OF INFORMATION RELATED TO COMPUTER INCIDENTS

Computer security means the methods and mechanisms intended to prevent the unauthorized destruction / modification / use of software and data of a computer system. To accomplish this task, an appropriate infrastructure is mandatory for each company.

This exemple consists of:

The company has the possibility to use the following three DBMSs for the acquisition of information on computer incidents; were chosen as appropriate: DBMS1, DBMS2 and DBMS3.

DBMS1 = MySQL *[Carter, 2019; Schwartz, 2008; Thompson & Welling, 2008; Fairuzullah, 2019]*;

DBMS2 = ORACLE *[Kyte, 2010; Maftei & Maftei, 2009; Maftei & Maftei, 2010; Mustafa & Lockard, 2019]*;

DBMS3 = DB2 *[Chong & Liu, 2013; Mullins, 2012]*.

They generate the first component of the software – hardware infrastructure couple.

The company has the possibility to use the following support infrastructures: INF1 and INF2 for the generation and operation of the databases.

INF1 = classic architecture;

INF2 = cloud architecture.

They generate the second component of the software – hardware infrastructure couple.

As a result, there will be 6 pairs of databases - support infrastructure DBMSi, $i=1,3$; INFj, $j=1,2$. In the theory of the Multi-Attribute Decision, the set of these couples is called the set of objects and the decision-maker's task is to determine the optimal object. This is possible if we highlight, for all objects, a lot of independent, observable or calculable characteristics, in relation to which the optimum is determined. In Multi-Attribute Decision Theory, these characteristics are called attributes. The model analyst must think about how to properly evaluate these eight attributes for each object. Scores are assigned to each object for each attribute and the lines and columns of the decision matrix are determined (***Table 2***).

The objects are: $o1$ = DBMS1-INF1, $o2$ = DBMS1-INF2, $o3$ = DBMS2-INF1, $o4$ = DBMS2-INF2, $o5$ = DBMS3-INF1, $o6$ = DBMS3-INF2.

The attributes are: $a1$ – hardware infrastructure, $a2$ – distribution, $a3$ – structuring, $a4$ – number of users, $a5$ – size, $a6$ – dynamics, $a7$ – memory, $a8$ – content.

The vector of importances (weights) assigned by the experts is: (0.17, 0.17, 0.10, 0.09, 0.17, 0.12, 0.08, 0.10), the places vector is: p = (1, 1, 3, 4, 1, 2, 5, 3). Lower and upper limit of the attributes are: 1≤$a1$≤10, 1≤$a2$≤10, 1≤$a3$≤10,..., 1≤$a8$≤10.

The vector of senses is: (max, max, max, max, max, max, max, max).

	$o1$	$o2$	$o3$	$o4$	$o5$	$o6$
$a1$	8	10	8	10	8	10
$a2$	7	10	8	9	7	9
$a3$	10	9	9	10	8	10
$a4$	8	9	7	10	10	9
$a5$	8	8	9	9	10	10
$a6$	9	8	9	10	8	10
$a7$	8	9	8	10	9	8
$a8$	7	9	8	9	10	9
	0.300781	0.679688	0.734375	0.765625	0.492188	0.863281

Table 2*.*
The decision matrix

In this case of producing and managing performant database from the exploitation point of view in the context of using the two chosen supporting infrastructures INF1 and INF2, the following procedures are performed:

- any database hosted by infrastructure INF1 is awarded 8 points;
- any database hosted by infrastructure INF2 is awarded 10 points.

$p(j)$ = the coefficient of importance for the criterion j which is calculated by the relation: $p(1)=\frac{1}{2^1}$, the first criterion is considered as the most important, $p(3)=\frac{1}{2^3}$, the third criterion is considered as the third as importance level, etc. So, corresponding to the vector p the vector

$$\left(\frac{1}{2^1},\frac{1}{2^1},\frac{1}{2^3},\frac{1}{2^4},\frac{1}{2^1},\frac{1}{2^2},\frac{1}{2^5},\frac{1}{2^3}\right)$$

Next, the place occupied by each object is calclated:

$loc(oa_{11}, a_1)=3$; (8 is the third value, criterion of maximum),

$loc(oa_{11}, a_2)=1$; (10 is the first value, criterion of maximum), etc.

Thus, the places matrix is:

$$\begin{pmatrix} 3 & 1 & 2 & 1 & 3 & 1 \\ 4 & 1 & 2 & 2 & 4 & 2 \\ 1 & 2 & 1 & 1 & 3 & 1 \\ 3 & 2 & 3 & 1 & 1 & 2 \\ 3 & 3 & 1 & 2 & 1 & 1 \\ 2 & 3 & 1 & 1 & 3 & 1 \\ 3 & 2 & 2 & 1 & 2 & 3 \\ 4 & 2 & 2 & 2 & 1 & 3 \end{pmatrix}$$

For each object, the following calculations were obtained:

$$o\_eval(o1) = \sum_{j=1}^{8} p[j] \cdot 2^{-loc(oa_{1j},c_j)} = 0.300781;$$

$$o\_eval\,(o2) = \sum_{j=1}^{8} p[j] \cdot 2^{-loc(oa_{2j},c_j)} = 0.679688;$$

$$o\_eval\,(o3) = \sum_{j=1}^{8} p[j] \cdot 2^{-loc(oa_{3j},c_j)} = 0.734375;$$

$$o\_eval\,(o4) = \sum_{j=1}^{8} p[j] \cdot 2^{-loc(oa_{4j},c_j)} = 0.765625;$$

$$o\_eval\,(o5) = \sum_{j=1}^{8} p[j] \cdot 2^{-loc(oa_{5j},c_j)} = 0.492188;$$

$$o\_eval\,(o6) = \sum_{j=1}^{8} p[j] \cdot 2^{-loc(oa_{6j},c_j)} = 0.863281.$$

A higher value of *eval_o(oi)* shows that the corresponding object i is better. After calculating *eval_o(oi)*, the objects are sorted by descending order. The order of the alternatives is therefore o6,o4,o3,o2,o5, o1. The best alternative is o6,so the pair DBMS3-INF2 is the solution of the problem. The database developed on DBMS3 and run on INF2 is the wanted optimal solution.

CONCLUSIONS

The 21st Century is the century of Communications and Video Accessibility. New requirements in continuous evolution ensure that everyone has access to communications as well as the ability to send and receive emergency information and services. In this circumstances the threats are increasing rapidly, so it is necessary to think about the solutions that have more complex measures. In the interconnected world, cyber security is changing second by second: organisations need to be prepared and the technology used must protect themselves from cyber vulnerabilities that can be rendered obsolete tomorrow. Cyber security management process is very dynamic and organisations must face situations that are not in their plans and that need to be covered in the future.

The paper presented an example of effective use and suitability of a MADM model for choosing optimal infrastructure (hardware and software) for acquisition and processing of the information related to computer security incidents. Making use of mathematical methods (that combine multidisciplinary research: Computer Science (hardware and databases, computer security), Operational Research (Multi-Attribute Decision Theory), etc.), the selection process can become faster and more accurate. The technological aspects that are used to protect critical infrastructure from cyber security attacks and vulnerabilities must be subject for future research interests.

REFERENCE LIST

Bulakh, A., Tuohy, E., Pernik, P., (2016). Estonia's Developing Level Playing Field for Critical Energy Infrastructure Protectors - a Model for Broader Scale Platforms, Energy Security: Operational Highlights 10: 4-10, Available on the Internet: https://www.icds.ee/fileadmin/media/ icds.ee/failid/no_10_20160410.pdf

Carter, P.A, (2019). SQL Server Security Model, In: Pro SQL Server 2019 Administration. Apress, Berkeley, CA, ISBN: 978-1-4842-5088-4, 978-1-4842-5089-1, DOI https://doi.org/10.1007/978-1-4842-5089-1_10

Chong, R.F. and Liu, C., (2013). DB2 Essentials: Understanding DB2 in a Big Data World (3rd Edition), Indianapolis: IBM Press

Fairuzullah, A., Noraziah, A., Mohd, W.M.W., Herawan, T., (2019). A New Approach to Secure and Manage Load Balancing of the Distributed Database Using SQL Firewall, In: Proceedings of the International Conference on Data Engineering 2015 (DaEng-2015). Lecture Notes in Electrical Engineering, vol 520. Eds: Springer, Singapore, ISBN 978-981-13-1797-2, 978-981-13-1799-6, DOI https://doi.org/10.1007/978-981-13-1799-6_1

Kyte, T. (2010). Expert Oracle Database Architecture: Oracle Database 9i, 10g, and 11g Programming Techniques and Solutions ISBN-10: 1430229462, ISBN 13: 978-1430229469

Maftei, E. and Maftei, C. (2009). ORACLE de la 9i la 11g pentru dezvoltatorii de aplicaţii - Vol. 1, ISBN 978-973-650-267-5

Maftei, E. and Maftei, C. (2010). ORACLE de la 9i la 11g pentru dezvoltatorii de aplicaţii - Vol. 2, ISBN 978-973-650-270-5

Maniatakos, M., (2017). Hardware-based solutions for critical infrastructure security, New York University Abu Dhabi Center for Cyber Security, sites.nyuad.nyu.edu/ccs-ad/

Mullins, C.S. (2012). DB2 Developer's Guide: A Solutions-Oriented Approach to Learning the Foundation and Capabilities of DB2 for z/OS, Indianapolis: IBM Press

Mustafa O., Lockard R.P., (2019). Oracle Database Threats. In: Oracle Database Application Security. Apress, Berkeley, CA, ISBN 978-1-4842-5366-3, 978-1-4842-5367-0, DOI https://doi.org/10.1007/978-1-4842-5367-0_4

Onicescu, O., (1970). Comparative Estimation Methods for multi-characteristic objects, In: Review of Statistic, Bucharest, Romania, No. 4, pp. 18-28

Resteanu, C., Şomodi, M., Andreica, M., Mitan, E., (2007). Distributed and parallel computing in MADM domain using the OPTCHOICE software. Wisconsin, USA: In: Proceedings of the 7th WSEAS International Conference on Applied Computer Science (ACS'07), pp. 376-384

Resteanu, C., Mitan, E., Andreica, M., Păcurar, G., (2015). Optimal Infrastructure for Acquiring and Processing of Data related to Anthropic Computer Incidents, Studies in Informatics and Control, ISSN 1220-1766, vol. 24 (1), pp. 51-60. https://doi.org/10.24846/v24i1y201506

Schwartz, B., Zaitsev, .P, Tkachenko, V., Zawodny, J.D., Lentz, A., Balling, D.J., (2008). High Performance MySQL: Optimization, Backups, and Replication, O'Reilly Media, ISBN-10: 0596101716, ISBN-13: 978-0596101718

Thompson, L., Welling, L., (2008). PHP and MySQL Web Development. The definitive guide to building database-drive Web applications with PHP and MySQL, ISBN-10: 9780672329166, ISBN-13: 978-0672329166

Tzeng, G.H., Huang, J.J. (2011). Multiple-Attribute Decision Making: Methods and Applications, Chapman & Hall, CRC Press, ISBN 1439861579, 9781439861578

Yoon, K.P., Hwang, C.L. (1995). Multiple-Attribute Decision Making: An Introduction, SAGE Publications

https://www.cert.ro/

https://www.edu.ro/search/node/arniec

https://www.enisa.europa.eu

https://www.fcc.gov/annual-reports

https://www.geant.org

https://www.nortonsecurityonline.com

http://orniss.ro

https://www.security-database.com