International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 85-98
http://dx.doi.org/10.14257/ijsia.2015.9.3.09

A New Bionic Architecture of Information System Security Based on Data Envelopment Analysis

Jianrong Yao and Minxue Wei

School of Information
Zhejiang University of Finance and Economics
Hang Zhou, China
y6310@163.com, wmx901231@163.com

Abstract

With the extensively use of information system, the security issue of the system increasingly becomes a problem. With the defense structure, biological immune system can efficiently defense and obliterate the foreign pathogens. Based on the current research of biological immune system and information system security architecture, this paper comes up with a feasible method to apply the defense structure of biological immune system to information system security architecture. Summarizing common characteristics between the two systems, which proves the possibility of realizing the defense structure in the information system security architecture and come up with an achievable method to construct the three defensive lines. The realization of risk identification in the information system security architecture is analyzed with DEA which is used to identify the risk in the information system security architecture through the establishment of the 'production frontiers'. A mathematical model of DEA is also developed using MATLAB to accomplish the risk analysis based on a set of real data from a company. Afterwards, this paper solves the problem that the previous studies are largely relying on the traditional safety analysis methods or the common risk assessment tools, which is lacking of effective protection technology to cope with the risk in the external environment and lay a foundation for achieving the bionic function of the information system security architecture.

Keywords: *biological immune system, information system security, data envelopment analysis, MATLAB, risk*

1. INTRODUCTION

With information technology advances in recent years, almost all sectors of society are increasingly dependent on the information system which is running normally and effectively, including industrial manufacturing, agricultural production, transportation, financial services and so on. Without the information system, many enterprises and institutions will not be able to function well. Just like other advanced technology in the human history, the information system also has two sides. On one hand, information system security has become the strong driving force to promote the development of the information society. In the information system, the information spreads to all aspects of the world at the speed of light through optical fiber, which makes the enterprise can get information rapidly and inexpensively. It is helpful to realize the resource sharing and improve the working efficiency. At the same time, it can enhance the core competencies of the enterprises to meet the challenges that brought by joining the WTO. Also, the enterprise can cope with the more intense situation of international competition well. On the other hand, with the extensive use of information system, there are increasing companies that have a strong dependency on it. This is followed by a higher requirement of accuracy and

ISSN: 1738-9976 IJSIA

security of the information. But the information system has brought about some safety issues, involving the political stability, economic development and cultural prosperity. Examples include information leakage, information theft, network worm attacks, hacker attacks, hardware damaged, data tampering, data deletion, the viruses and Trojans threaten the safety of the users.

It's well known that biological immune system is a layered architecture. Its three defensive lines through immune defense function, immune surveillance function and immune self-stable function are able to obliterate the foreign pathogens, and then to achieve the purpose of maintaining organism's physiological balance. Through introducing the similarities between the immune system and the information system security architecture from distributivity, adaptability, diversity and dynamic balance, this paper reveals the feasibility of setting up a bionic architecture of information system security. We describe the information system security architecture by copying the biological immune system. Inspired from three defensive lines in the biological immune system, we can establish the corresponding lines in information system security architecture by taking advantage of the protection technology now available. It is noted that a safe and effective information system is the combination of multi-level and multi-functional components. This paper maps the role of immune system in organism into information system security architecture and regards the 'risk' in the information system security architecture as the antigen. So the problem of distinguishing the 'risk' from 'safe' should be solved immediately. By using the method of DEA (Data Envelopment Analysis), this paper can recognize the 'risk' in the information system security architecture, which lay a foundation for the realization of its bionic functions. And the realization of DEA in the information system security architecture is done with mathematical modeling software MATLAB. Also, in order to validate the feasibility of using DEA to identify the 'risk' in the information system security architecture, this paper analysis the data from a company and the data is the four results of inventory management.

2. RELATED WORK

With the rapid development and the wide use of information technology, these types of problems have drawn significant attention to information system security. Various related theories and technologies have emerged in large numbers. The safety analysis methods put forward in the early stages, such as fault/event tree analysis, are the static description of the system from the standpoint of hardware structure and system function initially. Most of them, which emphasize on safety and reliability analysis, are used for transportation, water conservation, ore mining and other traditional industries. However, the conventional fault/event tree analysis is often very difficult to estimate precise failure rates or failure probabilities of individual components or failure events [1]. Cepin and Marko [2] have developed an improved method for classic fault tree analysis, and presented a dynamic fault tree to reduce the system unavailability, which extends the static fault tree with the time requirements. Subsequent research published by Boudali and Crouzen has shown that a number of issues still remain when using dynamic fault tree, despite of the fact that dynamic fault tree is experiencing a growing success among reliability engineers [3]. Besides, regarding the dynamic performance presented from modem information system, which is the technology of dynamic fault tree and dynamic event tree, the description is still insufficiently obvious and strongly relies on the engineering experience of analysts. The most common assessment tools are: COBRA (Consultative, Objective and Bi-functional Risk Analysis), which is a set of risk analysis software launched by system security company C&A in UK; CRAMM (CCRA Risk Analysis and Management Method), which is used by central computers of UK government and the telecommunications office to assess the vulnerability; ASSET (Automated Security Self- evaluation Tool), an automatic tools of automated security risk self-assessment, which is developed by NIST

(National Institute of Standards and Technology); CORA (Cost of Risk Analysis) and CORAS (Platform for Risk Analysis of Security Critical systems), which is designed by International Security Technology Company. Unfortunately, previous work has shown that the consideration of information system security no matter on the base of traditional safety analysis methods or the common risk assessment tools is far from complete.

Plenty of researches have revealed a truth that '100% information system security' is an ideal state, as most of the existing protective techniques for information system security have not taken the complexity of information system into account. Numerous successful risk invasions have shaken the information system security architecture that relies on the simple static defense technology or simple dynamic intrusion detection technology [4, 5]. Hence we devote to establish information system security architecture with the function emphasizing on "defense in depth" and seek out a new method to evaluate the information system security effectively. On the basis of three defensive lines in the biological immune system, we can establish the corresponding lines in information system security architecture by taking advantage of the protection technology now available. Noting that a safe and effective information system is the combination of multi-level and multi-functional components, we can also map the role of immune system in organism into information system by regarding the 'risk' in the information system as the antigen.

3. THE FEASIBILITY OF CONSTRUCTING BIONIC ARCHITECTURE OF IN FORMATION SYSTEM SECURITY

3.1. THE COMMON CHARACTERISTICS BETWEEN BIOLOGICAL IMMUNE SYSTEM AND INFORMATION SYSTEM SECURITY ARCHITECTURE

Biological immune system is a system with biological structures that can safeguard organism and protect against disease, while information system security architecture defend the information system from invasion, unauthorized use, and disruption. These two systems are in two completely different areas. However, for the purpose of the structure improvement of information system security architecture, the summarization of common characteristics between biological immune system and information system is necessary. There are four common characteristics that can be summed up: distributivity, adaptivity, diversity and dynamic balance.

3.1.1. DISTRIBUTIVITY

This feature of the biological immune system first depends on the distributed characteristics of the pathogen, namely pathogens scattered over the organism [6]. Secondly, the immune system consists of cells, lymph nodes, tissues and organs that are distributed over all parts of the organism. These lymphocytes are generally independent of each other, thus there is no need for the centralized control and coordination. Meanwhile, the biological immune system can amplify lymphocytes as needed, hence the increased lymphocytes will not consume too many system resources and also won't make control complicated.

The distributed information system is different from the centralized network. Its workloads spread over multiple units of work, and can effectively improve the working efficiency. Furthermore, the distributed feature can reduce the adverse effects of local work unit failure or malfunction on the overall system security.

3.1.2. ADAPTIVITY

The antigen types in the natural world are far more than the antibody types existing in the organism, therefore, we could not predict which antigen will invade the organism. The lymphocytes that are distributed over all parts of the organism can recognize the specific antigen by means of 'learning'. After antigen recognition, the mutation probability of antibodies will soar to 10 times more than that of normal cell. As a result, its affinity will be enhanced and the suitable antibodies to eliminate the invaded antigens are generated. The whole process adapt to the changes in the external dynamically.

The information system should have artificial intelligence, fault tolerance at some level to ensure its security. This means that the information system ought to extend its protective capability by means of self-learning.

3.1.3. DIVERSITY

Different organisms share the same immune mechanism, while the individuals have different immune ability. This feature is influenced and determined by the evolutional ability of immune system. What's more, each lymphocyte can detect several pathogens, but the pathogen types detected by different lymphocyte are not the same. As far as we know, the collections of lymphocytes among various organisms are also different, and the weakness of one immune system does not mean the same to another. For these reasons, a germ may be able to break through the safeguard of one immune system, nevertheless, it's highly unlike to infringe the other immune systems. It is precisely because the diversity of immune system, the organism as a whole can protect itself from the infection of external virus very well.

At present, the security defending systems are similar. Once vulnerability is found in an information system, the invasion will tread to all the systems using the same security defending system. Despite the similarity of the system can bring many benefits, the security risks caused by the lack of diversity are ignored. According to this, different means and focus of the protection should be used in computer immune system, so that the diversity can guarantee the entire network with the protection on the basis of individual safety.

3.1.4. DYNAMIC BALANCE

There are about 108 lymphoid detectors for human, but about 1016 kinds of pathogens should be identified and the cells will replace about every 10 days to adapt to the current substance to be detected, which form an interacted homeostasis network system. The method used by biological immune system is actually a time-cost for space approach.

If an information security system is to test all the possible intrusions to the detector set, the cost of the system will be considerably high, which has a serious impact on the system performance. At a time, the detection system can just contain a necessary subset of intrusion detectors which detect all the invasions. And the set of detectors can change dynamically over time, so that all the possible intrusions can be detected within a period of time.

3.2. THE CONSTRUCTION OF THE INFORMATION SYSTEM SECURITY ARCHITECTURE WITH BIONIC DEFENSIVE LINES

The biological immune system has the similar survival environment with the information system security architecture. Immune system is in face of the circumstance that is full of diverse pathogens such as viruses, bacteria, parasites. The known or unknown pathogens realize the evolution during the procedure of being eliminated. And meanwhile, the immune system will continue to evolve to adapt to it. The information system is working with kinds of computer viruses or attacks which are known or unknown to us. The computer viruses or attacks are

constantly changing with the improvement of safety technology in order to achieve the purpose of invasion. Furthermore, the role of information system security architecture is the same with the immune system in organism. The vital function of the immune system is to discriminate the 'self' from the 'non-self' [7]. At this point, the 'self' is cellular or molecular of the organism and the 'non-self' refers to viruses, parasites, bacteria and other foreign substances. Risk identification function of the information system security can match the essential feature of immune system. Here, the 'self' represents legitimate users or health data that are under protection and the 'non-self' represents computer viruses, unauthorized users, destroyed data and other malicious attacks. In addition, the 'self' can be seen as 'safe' and the 'non-self' can be seen as 'risk'.

The biological immune system is a layered architecture, which can rapidly detect and clear away the pathogens without the intervention by any outside force. The biological immune system provides protection to organism at different levels. The first defensive line is the skin, which can act as a physical barrier for the organism. And the skin can resist all kinds of harmful substances from invasion. The second defensive line is the physiological conditions, it provides a chemical barrier for the organism. Skin and mucous membranes will secrete a variety of sterilization, antibacterial substances, such as acid, saliva. And humidity and blood PH can kill foreign pathogens that could not adapt to the circumstance. The third defensive line is the immune line, which is composed of B-lymphocyte and T- lymphocyte. It is the cell barrier that can protect against the pathogen through the competition with it. The other way to resist disease is to eliminate pathogens by means of uniting with them.

In information security system, the technology like firewall can be used as the first defensive line, whose function is mainly controlling the connection between inner and outer net to prevent the illegal access and use the password technology to further ensure the security of the system. Firewall can controls the incoming and outgoing network traffic and check the data package and links in two or more networks based on applied rule set. It establishes a barrier to monitor the network so that the connection will not be allowed to make unless it is trusted. The second defensive line is using the tools to analyze the weakness and the safety of the system, such as port scan and vulnerability analysis. Instead of the situation that taking an action after the invasion, the vulnerability scanning of the information system makes it possible for the companies to repair the faults before it happens. The technology of information steganography and trap, which is the third defensive line, can be adopted to cheat and catch the invader. Intrusion detection and warning systems also can be used to monitor the protected system in real time, which can respond from the beginning of the invasion accordingly and prevent it from continuing. Intrusion detection and warning systems can monitor and take a quick response to the invasion that bypass firewall constraints, the intranet attacks and the misoperation. The system backup method should be used to make the system reduce loss to minimum after the invasion.

4. BIONIC FUNCTION OF THE INFORMATION SYSTEM SECURITY ARCHITECTURE

4.1. AN OVERVIEW OF BIOLOGICAL IMMUNE SYSTEM

The biological immune system has a storied structure [8], which is the basis of the immune mechanism, and it can have protective effects in multi-level. The biological immune system is mainly composed of skin, body fluids and lymph. It is of crucial importance that immune system can protect the organism from exotic germs invasion or infection. Hence, without the immune system, the organism will not be able to survive in the circumstance full of bacteria and viruses.

And the mechanism of biological immune system is shown in Figure 1. There are two types of lymphocytes in the immune system, named lymphocyte B and lymphocyte T.

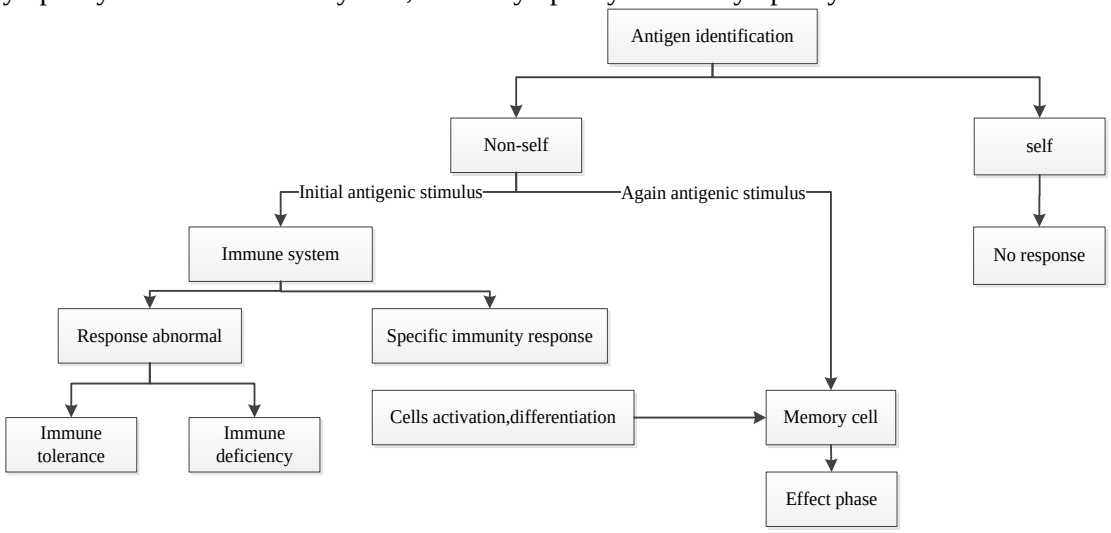

Figure 1. Mechanism of Biological Immune System

What we now appreciate is that the B-cells are continually coming into being from the bone marrow throughout life, and these naive B-cells can undergo a process of cell division and maturation [9], then the mature B-cells will leave the bone marrow to enter the peripheral lymphoid organs. In the peripheral lymphoid organs, the mature B-cells will become plasma cells that produce antibodies under the stimulus of foreign antigens. The B-cells are involved in specific humoral immunity. Data show that the ETPs (Earliest Thymic progenitors) give rise to T-cells in thymus, and the T-cells are responsible for specific cellular immunity and immunoregulation. When invaded by the external viruses, germs or parasites, the immune system will recognize the invaders first by combining the 'self' recognition function of T-cell with the 'non-self' recognition function of B-cell. And then the macrophages will wipe out the invaders that dare to intrude the organism in collaboration with other corresponding cells.

The primary function of Immune system is to maintain the physiological equilibrium of the organism. The function of immune system is the diverse biological effects in identifying and eliminating 'non-self' antigens, which includes:

- Immunologic defense: an immune protection with the role of anti-infections immunity. It protects the organism from the antigen and prevents the pathogen from invading, and can also clear away the invaded pathogens.
- Immunologic surveillance: a physiological protective effect that can promptly identify and remove the body cells which are mutated, distorted and virus interfered, and can prevent tumor from happening.
- Immunologic homeostasis: a physiological function that can maintain the internal stable environment by keeping immune tolerance to the 'self'. Normally, the organism can eliminate the internal cells that are damaged, aging or degenerate in time.

4.2. REALIZATION OF RISK IDENTIFICATION BASED ON DEA

4.2.1. INTRODUCTION OF DEA

DEA is an efficiency evaluation method that is originally formulated by Charnes, Cooper and Rhodes in 1978 [10]. It is a new cross-subject that covers economics, mathematics, operational

research as well as management science. DEA has been successfully employed in many cases, such as measure performance among schools, hospitals, sales department, and branch structures of the bank. DEA uses the mathematical programming model to measure the relative efficiencies among the Decision Making Units (DMU) [11], especially with multiple inputs and multiple outputs. We can estimate whether a decision making unit is efficient from the observed historical samples. Then on this basis, we make full use of the observed historical samples to construct the production possibility set, T= {(X, Y), the output Y can be produced by the input X} [7]. As shown in the Figure 2, the 'production frontiers' and the shaded area form the production possibility set. Effectively what we're talking about is to judge a DMU whether it is on the 'production frontiers' of production possibility set or not [12]. We regard the DMUs lying on the 'production frontiers' as efficient ones while the DMUs in the shaded area are not.

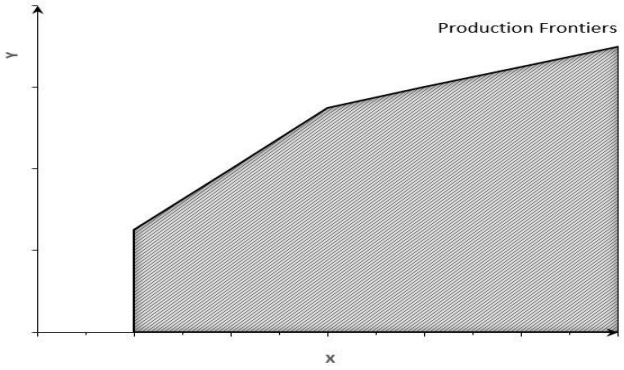

Figure 2. Line Graph of DEA

4.2.2. REALIZATION OF RISK IDENTIFICATION IN INFORMATION SYSTEM

DEA method provides a new approach for risk identification through the establishment of the 'production frontiers'. Combined with DEA theory, the DMUs lying on the 'production frontiers' are regarded as 'the safe set' and the DMUs below the 'production frontiers' are regarded as 'the risk set' here. As is known to all, a fundamental theorem gives that if DMU_1, $DMU_2 \in$'the risk set' then $DMU_1 + (1-\lambda) DMU_2$ also belongs to 'the risk set' ($0 \leq \lambda \leq 1$) [13].

We set up the 'production frontiers' with n DMUs (*i.e.*, history samples selected by audit experts) (j = 1,…,n) to identify 'the safe set' and 'the risk set' in the information system security architecture. Assuming that each DMU has the same inputs (i = 1,…,m) and the same outputs (1,…,s). X_{ij} denotes the i_{th} input of the j_{th} DMU and Y_{rj} denotes the r_{th} output of the j_{th} DMU [14]. The relationships between inputs and outputs are shown vividly in the Figure 3.

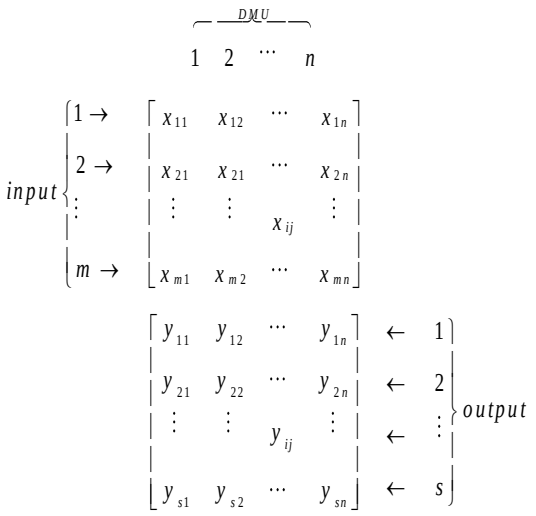

Figure 3. Relationships between Inputs and Outputs

We introduce the following model to identify any DMU_{j0} that is either at risk or not. The inputs of DMU_{j0} are $x=(x_{1j},x_{2j},x_{3j},x_{4j},\ldots,x_{mj})$ and the outputs of DMU_{j0} are $y=(y_{1j},y_{2j},y_{3j},\ldots,y_{sj})$.

Min E

$$s.t.\begin{cases}\sum_{j=1}^{n}\lambda_i y_{rj}\geq y_{rj0}\,(r=1,2,\cdots,s)\\ \sum_{j=1}^{n}\lambda_j x_{ij}\leq E x_{ij0}\,(i=1,2,\cdots,\mathrm{m})\\ \sum_{j=1}^{n}\lambda_j=1,\lambda_j\geq 0\,(j=1,2,\cdots,\mathrm{n})\end{cases} \quad (1)$$

If $E< 1$ in the mathematical model (1) above, (i.e., the DMU_{j0} is inefficient, then it means risks exist in the DMU_{j0}). If $E\geq 1$, we believe the DMU_{j0} is located on the 'production frontiers', which means the DMU_{j0} is efficient and it belongs to 'the safe set'.

4.3. DATA ANALYSIS

In data analysis, DEA is the method that we apply to the information system security architecture and the software we used to realize the algorithm is MATLAB.MATLAB is a mathematical modeling software that developed by Math works in 1982 [15]. It becomes one of the most popular and basic software in diversity of fields. MATLAB is of high intelligence, easy to use, easy to communication and visual for programing. Most important, it has powerful computing capability and it makes calculation of massive matrixes easier. These are the reasons that we use MATLAB to realize the DEA. The program is to analysis the data which is from the actual company and to certificate the correctness of the mathematical model. The basic idea to realize the reusability of different actual projects is to use a reusable function which has the inputs and outputs.

In the input X and output Y, we can simply let $X=[x_1, x_2, \ldots, x_n]$ and $Y=[y_1, y_2, \ldots, y_n]$ which x_n and y_n is an array, which means $x_i=(x_{1i}, x_{2i},\ldots,x_{mi})T$ and $y_i=(y_{1i}, y_{2i},\ldots,y_{mi})T$. In this paper, we set v and u as the input and output weight vector separately. I_i and O_i refer to the sum of inputs and outputs and we can get the value through (2).

$$\left.\begin{array}{l} I_i = x_i^T v (v \geq 0) \\ O_i = y_i^T u (u \geq 0) \end{array}\right\} \tag{2}$$

From (3) we get E, which is the efficiency evaluation index, and it is used to evaluate the efficiency of DMU_i. And to each DMU_i we try to make the weight vector to be max so that the inputs and outputs are in the safe set.

$$E_n = \frac{O_i}{I_i} = \frac{y_i^T u}{x_i^T v} \tag{3}$$

By using the model of C2R, we can get (4), which needs the max of E. Transferring it in to a linear programming problem which can solve the equation.

$$\left.\begin{array}{l} \max \dfrac{y_i^T u}{x_i^T v} = E_{ii} \\ s.t. \dfrac{y_j^T u}{x_j^T v} \leq 1 (1 \leq j \leq n), u \geq 0, v \geq 0 \end{array}\right\} \tag{4}$$

(5) is the linear programming equation and the solution to this equation, which we can make them as ω_i^*,μ_i^*, are the best weight vectors. With the value of ω_i^*,μ_i^*, the most efficient weight vector can be calculated.

$$\left.\begin{array}{l} \max y_i^T \mu = E_{ii} \\ s.t. y_j^T \mu \leq x_j^T \omega (1 \leq j \leq n), x_i^T \omega = 1, \omega \geq 0, \mu \geq 0 \end{array}\right\} \tag{5}$$

According to the algorithm mentioned above, the equation that need to be solve is (5) and LB and UB refers to the lower bound and upper bound, which is the range for w. and the main build-in function that we used is the linear programming function which is LINPTOG to get the solution for the equation. Here is the main code to realize the mathematical model [16]:

```
Clear
X=[…]
Y=[…]
function  E  = result( x,y )
n=size(x',1);
m=size(x,1);
s=size(y,1);
A=[-x' y'];
b=zeros(n,1);
LB=(zeros(m+s,1));
UB=[];
for i=1:n
   f=[zeros(1,m)-y(:,i)'];
   aeq=[X(:,i)' zeros(1,s)];
   beq=1;
   w(:,i)=LINPROG(f,A,b,aeq,beq,LB,UB);
   E(i,i)=y(:,i)'*w(m+1:m+s,i);
end

end
```

Based on the program, we can directly use the function and use multiple inputs which are matrix X and matrix Y as the parameters to accomplish the calculation. The result can be get in the command window. In the actual example, we use the data of material management from a company. Totally there are four types of materials and for each of them, the attributes for the X are: the number of people, the expense of the management, the quantity of materials; the

attributes for the Y are: the quantity of dumped materials, low-turnover rate materials, shortage of materials. According to the algorithm that we mentioned above, we can know the risk of the material management of this company by calculating the E. If E<1, the risk exists and DMU is inefficient. If E>1, then the set of the material management is safe and the DMU is efficient. Table.1 is the data of DMU_i (1<i<4) of the inventory management for four times:

Table 1. The Inputs and the Outputs of the Actual Company

		DMU_1	DMU_2	DMU_3	DMU_4
In-puts	People	20	30	25	18
	Expense(K)	4	5	5	2
	Quantity	1000	1300	1200	700
out-puts	Dumped	20	31	20	15
	Low-turnover	30	45	32	20
	Shortage	35	20	18	13

Based on the result of the program as shown in Figure 4 and the mathematical modeling mentioned in (1), E_{11} for the first inventory management DMU_1, E_{22} for the second inventory management DMU_2 and E_{44} for the fourth inventory management DMU_4 are all equal to 1, which means that the first, the second and the fourth inventory management are all lying on the 'production frontiers'. In other words, they are all efficient and they belong to 'the safe set'. Whereas E_{33} for the third inventory management DMU_3 is 0.8533, that is less than 1. According to that, we can draw a conclusion that the third inventory management is not lying on the 'production frontiers', which means the third inventory management is inefficient and it belongs to 'the risk set'.

4.4. THE BIONIC FUNCTION OF INFORMATION SYSTEM SECURITY ARCHITECTURE

The immune reaction in the organism is contributed by the foreign pathogens. We regard the 'risk' in the information system as the antigen, and the information system can make the corresponding reaction if there exist the risk. The mechanism of information system security bionic architecture is shown in Figure 5.

The protection of information system security architecture is similar to the function of immunologic defense in the biological immune system. Immunologic defense protects the organism from the antigen and prevents the pathogen from invading, and can also clear away the invaded pathogens. The protection of information system security architecture is to prevent the risk in advance, such as the illegal access. It reduces the damage of information system caused by risk, which is of great importance to ensure the normal operation of the information system.

The detection of information system security architecture is similar to the function of immunologic surveillance in the biological immune system. Immunologic surveillance can promptly identify and remove the body cells which are mutated, distorted and virus interfered, and can prevent tumors from happening. The detection of information system security architecture can be used to monitor the protected system in real time, which can respond from the beginning of the invasion accordingly and prevent it from continuing.


```
Command Window
>> a=[20 30 25 18;4 5 5 2;1000 1300 1200 700];
>> b=[20 31 20 15;30 45 32 20;35 20 18 13];
>> c=result(a,b)
Optimization terminated.
Optimization terminated.
Optimization terminated.
Optimization terminated.

c =

    1.0000         0         0         0
         0    1.0000         0         0
         0         0    0.8533         0
         0         0         0    1.0000

fx >>
```

Figure 1. The Result of Program

The repair function of information system security architecture is similar to the function of immunologic homeostasis in the biological immune system. Immunologic homeostasis can maintain the internal stable environment by keeping immune tolerance to the 'self'. Normally, the organism can eliminate the internal cells that are damaged, aging, or degenerate in time. The repair function of information system security architecture can make a related suggestion of modification and analyze the causes of the defect when the defect of the information system is found. It can be used to improve the level of information system security by preventing the same defect from coming into being again.

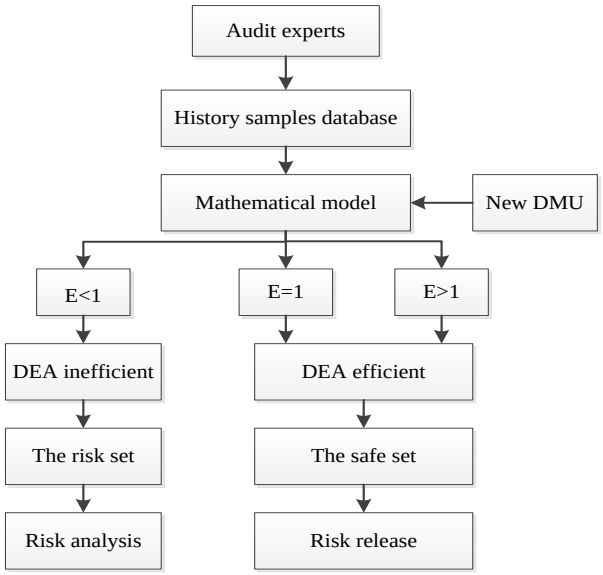

Figure 2. Mechanism of Information System Security Bionic based on Architecture DEA

5. CONCLUSION

With information technology becoming extensively used by companies in any areas, the security issue is increasingly significant. Biological immune system is a biological system with capability to protect the organism and fight against disease while the information system security architecture is to safeguard the information. Although these two systems are in different area, there are plenty of similarities so that we can improve the security level of information system based on the theory of biological system. The similarities can be summarized as distributivity, adaptivity, diversity, and dynamic balance. Furthermore, this paper makes an intensive study of the bionic mechanism of the information system security architecture. In order to distinguish 'the safe set' and 'the risk set' and apply the immune architecture to the information system, DEA, which is an efficiency evaluation method, is used to estimate the 'production frontiers' of information system security architecture. The main concept of DEA is $E< 1$ means the DMU_{j0} is located in the shaded area and it belongs to 'the risk set'; $E \geq 1$means the DMU_{j0} is located on the 'production frontiers' and it belongs to 'the safe set'. This paper use MATLAB to solve the in-equation and implement the mathematic model of DEA that can be used to identify the risk of the real data from the information system of a company in real time. Based on the analysis of the data, the correctness of the mathematical model is proved to be feasible. The risk can be regarded as the antigen of the information system and it can be monitored by DEA using the mathematic model. As long as the $E<1$, the risk will be promptly identified in real time and the relative actions will be taken to protect the information system. Also, the repair function of information system security architecture will be activated to give a suggestion of modification and find the root of the defection.

The immune system contains some characteristics which is similar to most of the complex systems. Both in the aspects of engineering applications and technologies, these characteristics have significant and far-reaching effects. However, due to the complexity of the biological immune system, it is still a long way to imitate its full potential. Future research should gear towards integrating other functions of the biological immune system into the information system security architecture by studying more mathematical models.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Minxue Wei, an intellectual and responsible student, who has provided me with valuable ideas in every part of my thesis. She is a talented, hard-working student and has a strong background of English. Without her great efforts, I could not have completed my thesis smoothly. I believe her keen academic observation will keep her making progress in the future.

I shall extend my heartfelt gratitude to Professor Liu for his kindness and patience to examine the thesis. I would also like to thank all the teachers in the school of information. They have helped me a lot in the past several years.

Last but not least, I would like give my gratitude to my family who are the strongest supports for me. They are the source power for me to keep myself motivated. Without them, I would not have come so far in my research.

REFERENCES

[1] P. V. Suresh and A. K. Babar, "Uncertainty in fault tree analysis: A fuzzy approach," Fuzzy Sets and Systems, vol. 83, **(1996)**, pp. 135-141.
[2] M. Cepin and B. Mavko, "A dynamic fault tree. Reliability Engineering and System Safety," vol. 75, **(2002)**, pp. 83-91.
[3] H. Boudali, P. Crouzen and M. Stoelinga, "Dynamic Fault Tree Analysis Using Input/Output Interactive Markov Chains," Dependable Systems and Networks, vol. 37, **(2007)**, pp. 708-717.
[4] P. Garcia-Teodoro, J. Diaz-Verdejo and G. Macia-Fernandez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computer & Security, vol. 28, **(2009)**, pp. 18-28.

[5] S. Zanero and S. M. Savaresi, "Unsupervised learning techniques for an intrusion detection system," Proceedings of the 2004 ACM symposium on Applied computing, **(2004)** April, pp. 412-419.
[6] Z. Shi, "Artificial Immune System," Intelligence Science, **(2012)** February, pp. 521-550.
[7] J. Huang, Y. Huang and L. Dou, "The risk warning model of auditing immune system: Based on Data Envelopment Analysis," In proceedings of 2012 International Conference on Management Science & Engineering, Dallas, USA, **(2002)** September, pp. 1478-1483.
[8] U. Aickelin and D. Dasgupta, "Artificial Immune Systems," Search Methodologies, **(2014)**, pp. 187-211.
[9] E. Vivier, D. H. Raulet and A. Moretta, "Innate or Adaptive Immunity? The Example of Natural Killer Cells," Science, vol. 331, **(2011)**, pp. 44-49.
[10] T. J. Coelli and D. S. P. Rao, "Data Envelopment Analysis," An Introduction to Efficiency and Productivity Analysis, **(2005)**, pp. 161-181.
[11] Y. Cui and L. Ma, "A New Procedure for Determining Super-Most Productive Scale Size," 2008 Fourth International Conference on Natural Computation, **(2008)** January, pp. 141-144.
[12] Q. Wei and H. Yan , "The data envelopment analysis model with intersection form production possibility set," Journal of Systems Science and Complexity, vol. 23, **(2010)**, pp. 1086-1101.
[13] Y. Hu, "Data Envelopment Analysis," Tutorial of Operations Research, vol. 3, **(2007)**, pp. 37-39.
[14] M. R. Alirezaee and M. Khalili, "Recognizing the efficiency, weak efficiency and inefficiency of DMUs with an epsilon independent linear program," Applied Mathematics and Computation, vol. 183, **(2006)**, pp. 1323-1327.
[15] P. Zhang, "Research on primary mathematics teaching based on MATLAB, " Hunan Normal University, **(2011)**, pp. 14-15.
[16] Y. W. Xu, X. S. Xu and S. X. Wu, "The application of MATLAB in data envelopment analysis," Journal of Southwest University for Nationalities, vol. 28, **(2002)**, pp. 139-143.