Fuzzy logic methodology for cyber security risk mitigation approach

Mansour Al-Ali, Ahmad AlMogren
King Saud University
Saudi Arabia
ahalmogren@ksu.edu.sa
ahalmogren@ksu.edu.sa

ABSTRACT: *This paper describes the impacts of criminal activates based on the nature of the crime, the victim, and the basis (whether short-term or longrange) of the impacts of cybercrime. Saudi Arabia faces numerous cyber threats including DoS (and DDoS), malware, website defamation, and spam and phishing email attacks. Although recent findings highlight the poor state of Saudi Arabia's information security system, it is within the current premise's suggestion that the development of a special cyber security risk assessment. Using Fuzzy Logic (FL) theory, we propose Fuzzy Inference Model (FIS) to produce risk mitigation and try to solve such issues to proposed entities.*

Keywords: Fuzzy Logic, Cyber Security, Fuzzy Inference System, Risk Assessment, Vulnerability, Threat, Mitigation, MOFA

Received: 19 April 2017, Revised 30 May 2017, Accepted 7 June 2017

1. Related Work

The primary purpose of identifying risk and analyzing the same risk gets done in preparation for mitigation of risk. Mitigation involves minimization of the possibility of occurrence of risk and also the reduction of the aftermath of the risk in question if, that risk happens. Several ways apply in the successful mitigation of risk [1].

Risk acceptance gets used after running the analysis of cost-benefit which makes the determination of whether the mitigating risk is more expensive, compared to the cost of bearing the same risk. In that case, the most appropriate response becomes accepting the risk while also having continued risk monitoring. Avoidance of risk gets applied as a mitigation approach when the activities involved have a significant possibility of a significant adverse financial blow or any other kind of loss. In such an instance, avoiding the whole activity which has the potential of great adversity becomes the only alternative.

Risk limitation gets applied as a strategy that minimizes risk to an acceptable level that makes sure that a firm gets part cover from the occurrence of the risk. For instance, a company will apply risk limitation against the occurrence of floods by accepting the fact that a tsunami may happen and also avoid the possibility of loss of its assets by having an insurance cover against floods. Risk transference also called risk contracting refers to the allocation of risks to entities that are best placed to handle and manage the risks. The challenge occurs however when there is the absence of quantitative measurement of the risk which could cause lack of accountable responsibility in looking for mutual threats that have optimal allocation. Quantifying risk is, therefore, necessary.

Planning for risk mitigation helps in settling on the best approach to curbing the potential in question, based on its efficiency and effectiveness [2]. There are several applicable methods of reducing risk based on the perspective of systems engineering in the order of intensity of risk. They include In-depth reviews of the process of engineering both technically and management wise; peculiar supervision of the allocated engineering parameters and different testing and analysis of important objects of design. Also, quick prototype formation and feedback from tests; making consideration to make a relief of relevant requirements of design and lastly, starting backup parallel developments.

The management and mitigation of risk do not happen at free cost regardless of whether one is handling lowprobability or high impact hazards. It becomes necessary to identify unusual activities involved in mitigation of risk. Notably, a plan of risk management defines the framework of managing the risk of a project while a program of risk reduction describes the wholesome risk and the plan of action response. For instance, implementing the reduction of parallel developments could assist the government in calculating the possibility of the cost involved being twice as much. On the other hand, putting into consideration fast prototyping or making alterations to the operational needs could spark the idea of making a projection of the likely time and cost to get incurred during risk mitigation [3].

2. Implementation of Risk Mitigation

In this section, we will propose our model for mitigation risk and will simulate the result using MATLAB. The proposed model consists of resulting risk assessment and another attribute that resulting from behavioral of human intervention. The human intervention is a major key indicator to mitigate the risk since most mitigation results should come after intensive discussion between stockholder. The human intervention behavioral could be the mentioned “Reviewer” which act as key responsible for decision making.

In figure 1, we proposed the mitigation risk which consists of two blocks of models binding with each other through FIS as follows:

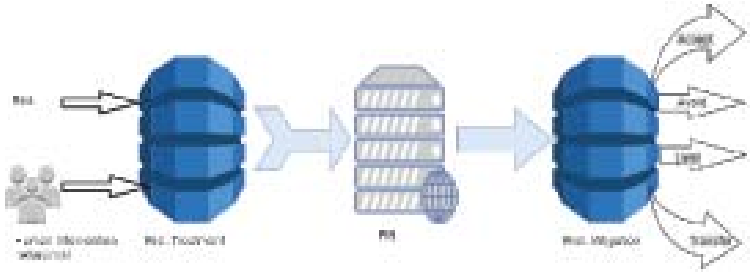

Figure 1. Proposed Mitigation Risk Model

As seen in above figure, we can have five variables for the Risk input as we extracted from previous risk assessment model which have the following analysis results (VERY HIGH, HIGH, MEDIUM, LOW, VERY LOW), however the human intervention behavior has only four inputs(AGREE, NEUTRAL,DISAGREE,STRONGLY DISAGREE). the input values ranging from 0-1. The result can be described in figure 2.

The result of our Mitigation Risk shown below in figure 5,6 respectively, which include all the situation of risk estimation starting from very low until Very high risk situation and the human intervention where can divide Transfer value between (0.00-0.25) , Limit(0.26-0.50),Avoid(0.51-0.75) and Accept(0.76- 1.00) as follows:

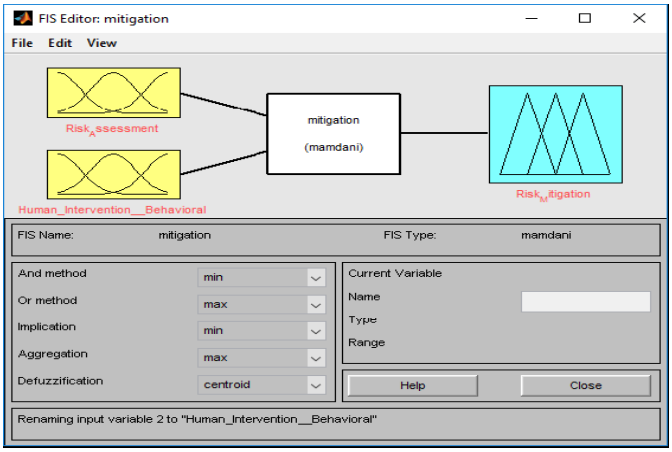

Figure 2. FIS Mitigation Risk Parameters and Settings

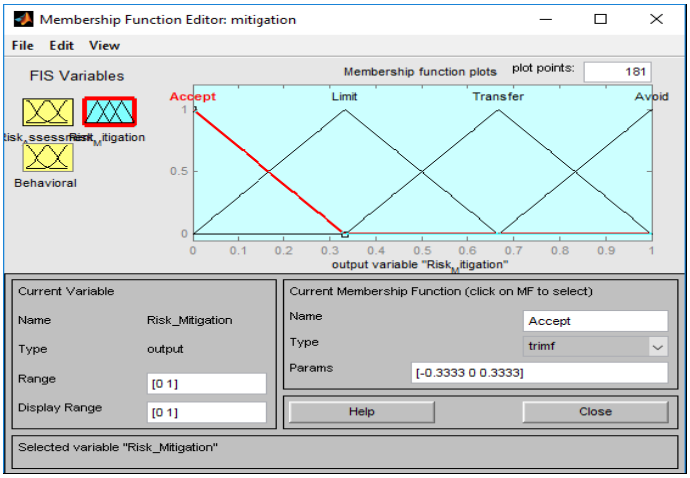

Figure 3. Membership Function of FIS

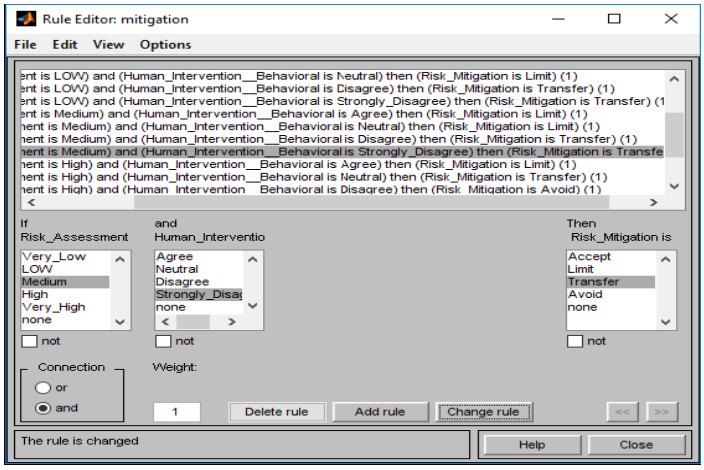

Figure 4. Mitigation Risk Rules

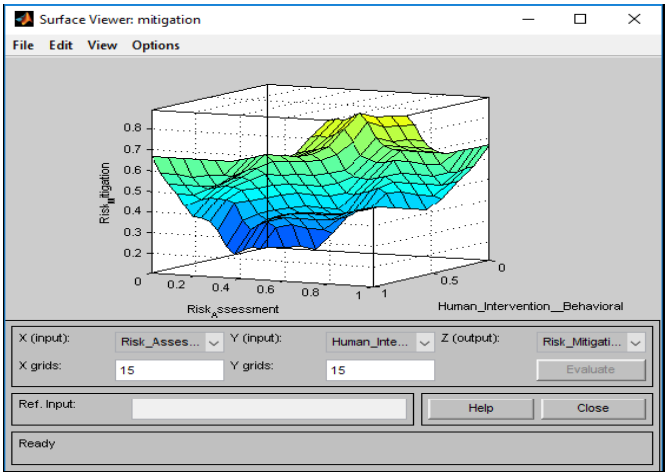

Figure 5. Mitigation Risk Surface View Result

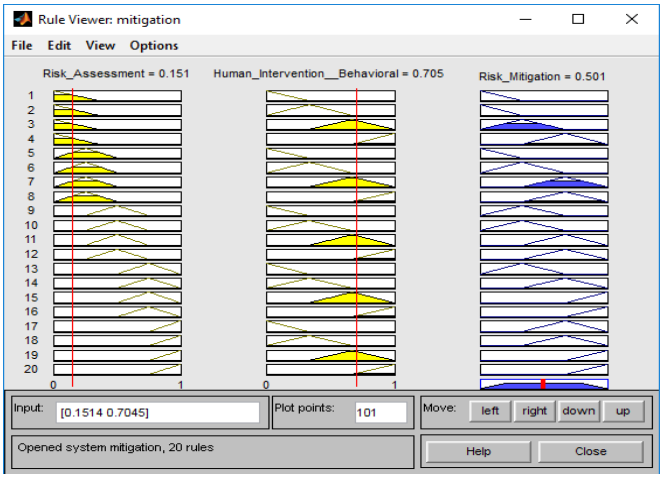

Figure 6. Mitigation Risk Rule View Result

Figure 7. Risk Mitigation chart

As we seen from above figure 6, we have seen 20 conditions to satisfy mitigation risk model. From above result we gained that risk assessment result is the primary key and more power than human intervention behavioral playing the potential result affect. This result comes as result of human intervention should come as support not as make decision for such a case. The following chart describes the percentage of risk mitigation model.

The formula to produce risk mitigation approach is as follows:
F=**Mitigation Risk** = (Risk Assessment, Human behavioral)

Which can be represented as combination of all possibility of Risk assessment and Human behavioral for all sets of membership n=1 to n=n
$\mathbf{F} = \Sigma_1^n$ (*Risk Assessment X Human behavioral*)
The algorithmic formula to mitigate risk is as follows:

```
variable=i
        for(each
Membership=1&&Membership<=n)
                do (insert F[M]=i)
                increment (i)
        end if
return F
```

Case 2: Lets represents the following memberships for risk assessment result:
A= :{0.00 ≤ Very Low ≤ 0.20}
B= :{0.21 ≤ Low ≤ 0.40}
C= :{0.41 ≤ Medium ≤ 0.60}
D= :{0.61 ≤ High ≤ 0.80}
E= :{0.81 ≤ Very High ≤ 1.00}-
and we have the following memberships for human behavioral:
A^- = :{0.00 ≤ Agree ≤ 0.25}
B^- = :{0.26 ≤ Neutral ≤ 0.50}
C^- = :{0.51 ≤ Disagree ≤ 0.75}
D= :{0.0.76 ≤ Strongly Disagree ≤ 1.00}
Assume the following values, risk assessment= .0.53 and human behavioral =.60. Find the risk assessment result?
The result of F=0.53*.60=.0..318
So the risk assessment result is 31.8% which is located in avoid status, so the organization should have action plan to limit this type of risk.

Chapter 10. Evaluation
Our model consists of two parts; the first part is evaluating the risk to produce risk assessment values. The second part is treating the risk using our risk mitigation approach. To measure above models for such an organization that facing major vulnerabilities that raised to become a potential risk. We can implement our models for Ministry of Foreign Affairs in Saudi Arabia as good practice. We should declare the risk factors as input used for our models which are:

1. Intent; which are the probability of stolen or corrupted resource systems.

2. Targeting; is the goal resource systems for hackers or intruders.

3. Capabilities; which is the technical skills and knowledge of the intruders.

4. Vulnerabilities; is the weak measurement of the controls, like firewalls, gateway,...etc.

5. And Impact; which is the damage of resource for certain time mainly shortly.

Wiki Leaks published leaking confidential information to correspondence by incident and said it between the Saudi Ministry of Foreign Affairs and diplomatic missions around the world starting from June 19, 2015 until November 2015 which was published 61,195 documents out of 500 thousand documents intends to publish in the coming weeks in the Saudi Cables site. The organization said it received an e-mail correspondence between the Saudi Ministry of Foreign Affairs and other countries in

addition to the confidential reports from Saudi Arabia and other ministries. “WikiLeaks” did not mention the source of the documents, but it said that hackers calling themselves “the Yemeni military mail” infiltrated the network of the Saudi Ministry of Foreign Affairs in May 2015 and leaked thousands of documents.

The Foreign Ministry said Saudi Arabia that the documents recently published across the site “Wikileaks” linked to the process of piracy suffered by the former ministry, warning of circulation considering that some of them “have been staged”, the ministry said it would prosecute legal for all those who stood behind this breakthrough in the frame existing electronic warfare between countries, whether companies or governments, under international laws and regulations, and reduced the ministry would hack it said that what has been leaked documents do not deviate from the framework of the stated policy of the Foreign Ministry in their statements and various data about the various regional and international issues. The compromise has been conducted when a Philippine employ has published a personal resume for him through Linkedin. This employ received many invites and offers to join other job vacancies. The hacker sent to him a batch file with job offer under email phishing attack (described in chapter 2) . This employ is a master key in IT within MOFA considering the long time experience and administrator of network.We apply the above data illustrated above to our formula, consider the following variables;intent, targeting, capabilities, overall_capabilities,vulnerabilities, overall_liklihood and impact represented as follows:

V_0, V_1, V_2, V_3, V_4, V_5 and V_6 respectfully and the membership of each variables divided into 5 categories starting from Very Low until Very High; M_0, M_1, M_2, M_3 and M_4.

we can describe the variables in the following statement:

V_0 = 1 which is 100% of success stolen information $\in M_4$

V_1 = 61195/500000= 0.154 which is 15% of resource system has been compromised $\in M_0$

V_2 =1 which is 100% that the intruders have the powerful capabilities $\in M_4$

V_3 = (1+0.15+1)/3=.716 which is more than 71.6% $\in M_3$

V_4 =1 which is 100%, that means all system controls failed to defeat such attack

V_5 = (1+.716)/2=0.85 which is 85% which $\in M_4$

V_6 = 0.9 the impact was $\in M_4$ since it was large scale attack over short time.

F=(.9+.85)/2=.88 which is 88% $\in M_4$

The table 7 below described the risk factors values.

Factor	**Value**
intent	100
targeting	15
capabilities	100
overall_capabilities	71.6
vulnerabilities	100
overall_liklihood	85
impact	90
Risk assessment	88

Table 7. Values of risk factors

From above table, we found that risk assessment values exceed the expectation and tend to be Very High, those results should maintain risk treatment approach which most enter the risk mitigation model.

We apply the above result to our mitigation risk model considering the following variables; risk assessment and human intervention as V_0 and V_1 with four memberships between $M_0 ... M_3$;

V_0 = .88 which was obtained previously from risk assessment result $\in M_3$

V_1 =.85 $\in M_3$

F = V_0 * V_1 =.88*.875=.75 which is M_2 which is AVOID risk that must have action plan immediately to overcome the risk. Table 8 shows the risk mitigation factors.

Factor	Value
Risk assessment	88
Human intervention behavioral	85
Risk mitigation	75

Table 8. Risk mitigation factors

So what we learned from above example as the source of the risk and how we recover the risk are as follows:

1. Leakage information always started from inside.

2. The users ignore storing credential safely or changing it periodically.

3. The administrators should keep their passwords complex, lengthy and not using it always.

4. The organization should hold always awareness session for security and hackers' deceivable approaches.

5. The organization should maintain affordable budget for security purposes whenever cut off exist in resource, may the security get breached.

6. It is essential to recourse for well security global solution company to assist the organizational resource to protect them from potential risk.

So, it is obvious that attacks start from insides whenever there are employees that open every e-mail or attachment or accepting any invite through the internet or downloading non-secure attachment or neglecting establishing a secure infrastructure such as implementing firewall ,IDS, IPS,AMP,…etc to protect them from such attacks like DDOS or website attacks.

8. Conclusion

Technological advancement and its relation with cyber wellness can be expressed as a metaphoric two-edged sword, one providing new insight into the vulnerabilities of the global cyber network, and another seeking way to redress the possibilities of successive cyber attacks. Amidst this complexity come numerous attempts, both at sate and global levels, to combat cybercrime and reduce the risk of cyber attacks both in the private and public realms. It is inevitable to conceptualize the hiring additional cyber security specialist as the principal strategy to displace cyber insecurity from the top three security threats. However using Fuzzy logic can give abroad vision to the organizations to estimate risk and evaluate risk factors and can end up with evaluation of most important security measures.

Reference

[1] Ming-Chang, Lee. (2014) Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method, *International Journal of Computer Science & Information Technology* (IJCSIT) 6 (1) p. 29-45.

[2] Sjoberg, Lennart. (1999). Consequences of perceived risk: Demand for mitigation. *Journal of Risk Research* 2.2.

[3] National Research Council of the National Academies. (2005).The Owner's Role in Project Risk Management. Available in: (https://www.nap.edu/read/11183/chapter/7). p. 41.

[4] Hany, Sallam. (2015). Cyber Security Risk Assessment Using Multi Fuzzy Inference System, *International Journal of Engineering and Innovative Technology* (IJEIT) 4, 8.

[5] Martin McNeill, F., Ellen, Thro. (1994). FUZZY LOGIC A PRACTICAL APPROACH" by Academic Press Professional. San Diego, CA, USA.

[6] Bajpai, Shailendra, et al. (2010). Security Risk Assessment: Applying the Concepts of Fuzzy Logic, *Journal of Hazardous Materials*, 173 (1-3) 258-264.

[7] International Council on Systems Engineering (INCOSE), (2010). INCOSE Systems Engineering Handbook, Version 3.2, INCOSE-TP-2003-002-03.2, p. 213-225.

[8] U.S. Department of Energy, Electricity Subsector Cyber security Risk Management Process, DOE/OE-0003 (2012).

[9] Sonia., Singhal, A., Banati, H. (2011). Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD model, *IJCSI International Journal of Computer Science Issues*, 8 (4) 1.