

Selecting Adequate Security Mechanisms in E-Business Processes Using Fuzzy TOPSIS

Shahriar Mohammadi, K. N. Toosi University of Technology, Iran

Sina Golara, K. N. Toosi University of Technology, Iran

Nasim Mousavi, K. N. Toosi University of Technology, Iran

ABSTRACT

Security mechanisms are substantial to an e-business environment. While many security mechanisms have been developed to secure e-business processes (EBP) and networks, little attention is given to actual process of a systematic decision making. In most cases strongest security level available is selected. In many cases there are low risks and threats associated with the processes and the use of strong security wastes the available resources. In this paper the authors developed a practical multiple criteria decision making model based on the group fuzzy technique for order preference by similarity to ideal solution (GFTOPSIS) for choosing adequate security mechanism for e-business processes and making a trade-off between security and other important factors in the enterprise. Data was acquired from experts and implemented fuzzy approach. The authors differentiated four phases in the EBP. Each phase of the process which has specific security requirements thus we suggested the use of specified security mechanisms for each phase which improves the efficiency of the system.

Keywords: *Analytic Hierarchy Process, E-Business Process, E-Commerce, Fuzzy TOPSIS, Multiple Criteria Decision Making, Security*

INTRODUCTION

E-business security is a fast-growing field. Network communications play an essential role in e-business environment. While the internet as a global network provides new opportunities such as interconnecting millions of networks, countless resources and different services for users, it also brings new threats and security risks such as worms, viruses, denial of service

(DOS) attacks etc. Because of the significant increase in computers speed and complexity of applications, making quick and adequate decisions about security mechanisms is very difficult. As a consequence usually strongest security level available is selected. However this approach is not efficient and brings additional costs and resources consumption. Besides, the usage of strong security mechanisms under the insufficient availability of resources can serve as a base for DOS attacks (Smirnov, 2007). In e-business processes (EBP), we differentiate four

DOI: 10.4018/ijfsa.2012010103

phases. Each phase of the process has specific security requirements. Thus we suggest the use of specified security mechanisms for each phase which improves the efficiency of the system. Decision making to find the adequate security mechanism with regard to the required security level is the problem for which we are seeking a solution in this paper.

While many security mechanisms has been introduced to secure devices and networks, too little attention is given to actual decision making process about the security level with respect to predefined requirements (Williams, 2003; Anderson, 2001).

Networks and e-business platforms are often faced with a wide spectrum of different security mechanisms e.g., block ciphers, virtual private networks (VPNs), secure socket layer and transport secure layer (SSL/TSL) protocols (Smirnov, 2007).

These security mechanisms have different features such as the security level the can provide, costs, implementation ease and complexity, processing speed and computational efficiency, required resources etc. The e-business must decide which security solution to choose in order to satisfy the business needs and policies.

In this work we are seeking to make a trade-off between security level and other important factors in the e-business environment, instead of the “always highest security” approach. The new approach is more efficient and better suites the requirements of the e-business. We develop our framework under the notion of “always best security (ABS)” first introduced by Johnson (2005). According to this approach the strongest security level is not necessarily what we need. Instead we should search for the “best” security level which makes a trade-off between the criteria to achieve the optimal solution. Decision making under this approach is a complex multiple criteria decision making process. To accomplish the objective of this paper, we modeled the decision making process as a multiple criteria decision making

(MCDM) problem which adopts group fuzzy technique for order preference by similarity to ideal solution (GFTOPSIS). The data required to make the decision is obtained from experts and transformed into fuzzy numbers.

PRELIMINARIES

In this section we introduce some basic notions essential to understanding of the proposed approach. Instead of crisp numbers, this paper uses fuzzy numbers in decision making process. Moreover technique for order preference by similarity to ideal solution (TOPSIS) is adopted for ranking the alternatives final decision. The combination of the two notions is called fuzzy technique for order preference by similarity to ideal solution (FTOPSIS). We have also adopted group decision making approach in FTOPSIS procedures. The resulting technique can be referred to as GFTOPSIS, the elements of which are introduced.

Fuzzy Set and Fuzzy Number

In this section we review some basic notions of fuzzy sets, as follows:

Definition 1. A fuzzy set $\tilde{A}$ in a universe of discourse X is characterized by a membership function $\mu_{\tilde{A}}(x)$ that associates each element x in X a real number in the interval $[0, 1]$. The function value $\mu_{\tilde{A}}(x)$ is termed the grade of membership of x in $\tilde{A}$.

Definition 2. A positive triangular fuzzy number (PTFN) $\tilde{n}$ can be defined as (n_1, n_2, n_3) illustrated in Figure 1. The membership function $\mu_{\tilde{n}}(x)$ is defined as shown in Figure 1 (Kaufmann & Gupta, 1991).

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/selecting-adequate-security-mechanisms-business/63354

Related Content

Nelder-Mead Evolutionary Hybrid Algorithms

Sanjoy Das (2009). *Encyclopedia of Artificial Intelligence* (pp. 1191-1196).

www.igi-global.com/chapter/nelder-mead-evolutionary-hybrid-algorithms/10391

A Fuzzy-Neural Approach with Collaboration Mechanisms for Semiconductor Yield Forecasting

Toly Chen (2010). *International Journal of Intelligent Information Technologies* (pp. 17-33).

www.igi-global.com/article/fuzzy-neural-approach-collaboration-mechanisms/45154

Effective Use of Information Systems/Technologies in the Mergers and Acquisitions Environment: A Resource-Based Theory Perspective

Hung W. Chu and Minh Q. Huynh (2012). *Insights into Advancements in Intelligent Information Technologies: Discoveries* (pp. 140-160).

www.igi-global.com/chapter/effective-use-information-systems-technologies/64374

A Low-Cost Multi-Touch Surface Device Supporting Effective Ergonomic Cognitive Training for the Elderly

Vasiliki Theodoreli, Theodore Petsatodis, John Soldatos, Fotios Talantzis and Aristodemos Pnevmatikakis (2010). *International Journal of Ambient Computing and Intelligence* (pp. 50-62).

www.igi-global.com/article/low-cost-multi-touch-surface/46023