Journal of Network and Information Security
11 (1) 2023, 01-07
http://www.publishingindia.com/jnis

Network Security Framework Based on an Intelligent Agent

Meena Sachdeva[1*] and Davinder Kumar[2]
[1]JIMS Engineering Management Technical Campus, Greater Noida, Uttar Pradesh, India.
Email: meena.sachdeva255@gmail.com
[2]Micron Electronics, Hyderabad, Telangana, India. Email: davinder991@gmail.com
*Corresponding Author

Abstract: In the growth and the development of technology security is a very important concept. Security properties are drawn in the implementation phase. But the integration of security properties can be implemented in all phases of software development. Agent is an autonomous entity and has the ability to act on behalf of others, can understand the changes in the environment and react according to environment with the help of features like mobility, learning ability etc [1]. So we conclude that an agent can be a person, a machine, a piece of software. Agents are autonomous, flexible and active according to the environment. Agents are smart and have flexible behaviour. In this paper we proposed information security framework with the help of an intelligent agents. Intelligent agents are designed with TOPSIS model. Model is based on multi-criteria decision analysis method.

Keywords: Agent, Information security, Intelligent agents, TOPSIS model.

I. Introduction

The distribution of information with the help distributed information systems is completely new characteristic of the most recent forms of multimedia communication. Computers become more obedient with the use of agents and Artificial Intelligence [2, 3]. Old computer systems needed to be planned in advance and to have rules that are not functioning well in unexpected situations. The basic concept of agents is very simple. Agents can be defined as an entity that has ability to do actions on behalf of his owner. Autonomy is the main concept of agents this means that an agent need not wait for the instructions about what to do in every moment of its life. But the programmer fix in the agent believes, desires, and intentions and the agents will guide their actions by these feelings. So the difference between the agent systems and the old programming paradigms is the emergence of the concept of an environment that interacts with and influences the agent actions and environment that did not exist in that old systems. Every agent is fixed in an environment in which the agent interacts through sensors and effectors [4]. The environment should be well known in which the agent lives and affect directly the success or failure of the agents. The decisions taken by the agent are taken from the environment that is interpreted by its environment [5]. So these decisions will be translated into actions performed in the same environment. Intelligent agents are very popular, but autonomy is not the only factor that affects their success. With the help of this autonomy agents can do anything to achieve their goals and this includes the ability to communicate and interact with other parties that make up the environment. These parties can be other agents, non-agent softwares and humans [6, 7, 8]. Social ability allows a problem that sometimes is beyond the individual capacities or knowledge to be distributed and solved by several entities. In a multi-agent system as several agents make up a virtual society and they uses the social ability, through cooperation, collaboration and negotiation, to achieve their particular objectives. Social ability also provides a way to model problems closer to the real world in which there is a division of labor and capabilities. Multi-Agent System (MAS) are currently been used in an increasingly wide variety of industrial, commercial, governmental, military and entertainment applications [11]. MAS can be found acting both small applications such as email filters, and personal assistants, as well as open, complex, mission critical systems, as air traffic control, military demining or logistic planning, financial portfolio management and among others.

II. Intelligent Agent and Security

Security is defined by given mentioned properties:

Confidentiality: In this property information is only accessible to authorized persons and inaccessible to others.

Authentification: With help of this property we can define the Identity of an entity.

Integrity: This property describing that the information can never be unmodified from source entity to destination entity.

Access Control: This property identifying the access rights an entity has over system resources.

Non-Repudiation: This property confirming the involvement of an entity in certain communication.

Availability: Availability provides accessibility and usability of information and given resources to authorized entities.

Secret Stream: This property preventing unauthorized users to be able to analyze the data flow.

Confinement: This property ensuring that a subject cannot voluntarily disclose contents of objects to which he has access to someone who doesn't have the right to access.

Security Threats in Intelligent Agent System

Intelligent agent technology faces the security problem which has not been met before. The agent interacts with other agents that can analyze or alter its content. Also visited host on which the agent runs has the ability to manipulate the agent or even destroying it.

Two types of attacks and five risk categories are defined.

Attacks: Attacks are active attack and passive attack.

Risk Categories:

- *Attacks between Two Agents:* In this an agent may suffer from another agent. There are basically four types of risks: attacks against authentication, attacks against confidentiality, attacks against availability and attacks against non-repudiation [9].
- *Attacks of the Host for Agents:* To run an agent, the host must have access to its code, data and state. Thus, an agent that runs on a site is exposed to security threats which are: attacks against authentication, attacks against confidentiality, attacks against availability and attacks against integrity.
- *Agent Attacks the Host:* In this class the problems include masquerading, denial of service, unauthorized access and repudiation.
- *Security between Agent and External Entities:* To migrate to another site, an agent must pass through a communications network on which the agent may suffer different types of attacks such as listening, alteration of its content or even its destruction.
- *In Addition, at the Target Platform:* Agent can be attacked by the user of the platform or by other agents.

III. Network Intrusion

All we are living in electronically interconnected world and information moves at the speed of light. This information is present in very large value. Network is very important media for getting information. E-commerce is caused due to the growth of Internet and WWW. Network intrusion increased with the growing population using public network [10, 11]. As described in the survey of Aberdeen Group, there were 100,000 network intrusion held in 2003, which effect company and personal loss of around USD 8.75 billion. Aberdeen Group completed his research and describes that

- Security based events from the Internet have average revenue losses amounting to almost $2 million per incident across all industries and firms.
- The median rate for revenue losses from Internet business disruptions is currently 0.067% of the revenue.

So that traditional information security methods uses passive mechanisms like encryption, authentication, firewall and uses system guards to protect information resources. As all these methods are "static", and hence information attacks cannot be detected in advance. They are used to filtering illegal network access. For example, firewalls do not inspect the contents of information packets. If a valid application contains viruses or worms, they will not be able to detect the attacks. Firewalls can not to stop hackers who use denial-of-service techniques to attack network. These two drawbacks of firewalls are not detecting internal attacks. So we take intrusion detection system (IDS) [12]. That is an IT technique can detect network intruders or crackers on its own initiative. Intrusion detection systems are developed from Denning's intrusion detection model (Denning, 1987), that audits records, network packets, or any other observable activities as the basis for detecting abnormalities in the system or checking them with traces and signals of known intrusion patterns. Intrusion detection divided into two categories.

- *Misuse Intrusion Detection:* In this technique intrusion patterns can be installed into the system in advance. This technique uses well-defined intrusion patterns and check if a user is hacker or cracker.
- *Anomaly Intrusion Detection:* In this network users activity records builds statistical profiles of the activities records. The user can be a hacker or cracker if the activities that differ remarkably from normal use as intrusions.

Both methods have its' own drawbacks. The misused intrusion detection method will not work when new or unknown forms of attack are found. The anomaly intrusion detection method is unable to detect inside attacks. So, any intrusion detection system uses any one of these methods will have a limited range of intrusions it can detect [13]. An intrusion detection system involves parallel employment of both techniques. But the system will become very large and operate slowly. To protect the intranet, intrusion detection system is usually installed in an intrusion server. This is called "Client-Server protection mechanism".

Keep these problems in mind we proposed in paper information security framework based on an intelligent agent that combines all distributed information security facilities to achieve

efficiently collaborative information security [14, 15]. In the framework, an allied member can still obtain information protection even it does not install any security devices or system. Moreover, it will use a warning mechanism for allied members to take action to protect their information resources before they suffer information attack. In order to let allied member choose an optimal action among alternatives to protect its information resources, the framework provides a decision model that enables its allied member's agent to choose among alternatives in an optimal fashion, taking into account the worth of acquiring prior information to reduce the uncertainty.

First, the model uses a group decision procedure to determine a global information threat level.

IV. Information Security Framework Based on an Intelligent Agent

Before describe the new framework first we describe the Characteristics of the agent. The agents are software entities that assist people and act on their behalf. Software agent system is combined of no of small agents that have different structures and they perform a job together [16]. It is a good technique to search and retrieve scattered data all over the world. On the basis of their properties, there are three types of agents: Intelligent agent, Mobile agent and Collaborative agent. Each has its own capabilities as follows:

- *Intelligent Agent:* Intelligent agents have the abilities of supervising, reasoning, and explaining and can observe and learn users' habits through its past experiences.
- *Mobile Agent:* Mobile agent can be transported from a server to another template of a different system structure.
- *Collaborative Agent:* An agent handles applications through cooperation that a single program cannot handle, such as job scheduling, mail managing, data mining, data searching, shopping on line, digital library, process managing.

ISFBA (Information security framework based agent) is composed of many organizations in to network systems. These network systems are known as "allied members" [17]. Each allied member is installed with two kinds of agents. They are inspection agent and mediating agent. The functions of each agent are described as follows:

A. Inspection Agent

The inspection agent is installed in a local allied member, always monitors possible information attack and evaluates the threat value according to the following criteria:

Let (M1, M2, . . . , Mn) be a set of profile and (S1, S2, . . . , Sn) be the respective deviations, then we define the threat value τ as:

$r_1S_1^2+r_2S_2^2+\ldots+r_nS_n^2$

$$\tau = \sqrt{\frac{r_1S_1^2+r_2S_2^2+\ldots+r_nS_n^2}{n}} \qquad \text{Eq. (1)}$$

Where $1 \geq r_i > 0$ is the reliability of i^{th} deviation (be adjustable).

It needs to note that the deviations are generated by a local allied member's information security system (IDS, firewall, system guards, etc.). The role of the inspection agent is to constantly collect the deviations and employ Eq. (1) to calculate a threat value τ.

B. Mediating Agent

The mediating agent is an intelligent agent installed in a local allied member. It plays two candidate roles, namely ISFBA "ordinary member" and "TOPSIS model".

C. Ordinary ISFBA Member

When the allied member is an ordinary ISFBA member, the mediating agent analyzes the inspection agent's information attack reports, delivers attack information (threat value s) to the TOPSIS model and takes corresponding actions according to the network system's security policy. For convenience of determining the information threat level and taking corresponding actions, the mediating agent uses (2) to define a local threat level:

$$\iota = \begin{cases} 1 & \text{if } 0.0 < \tau \leq 0.2 \\ 2 & \text{if } 0.2 < \tau \leq 0.4 \\ 3 & \text{if } 0.4 < \tau \leq 0.6 \\ 4 & \text{if } 0.6 < \tau \leq 0.8 \\ 5 & \text{if } 0.8 < \tau \leq 1.0 \end{cases} \qquad \text{Eq. (2)}$$

Then it uses the threat level to determine a corresponding action. For example, when it finds a level-1 information attack, it increases incident monitoring and looks for patterns across a wide range of variables, but does not stop any information activities. However, when it finds that a level-5 information attack has happened, it immediately stops all information activities (such as disconnects extranet and intranet service, stops application systems, implements information system damage assessment and damage systems repair/reload). The system's default threat level is zero (l = 0), meaning that no information attack has happened. Other attack threat levels and their corresponding actions are given in Table I. Note that the actions in Table I can vary from system to system.

Table I: The Threat Level and its Corresponding Actions

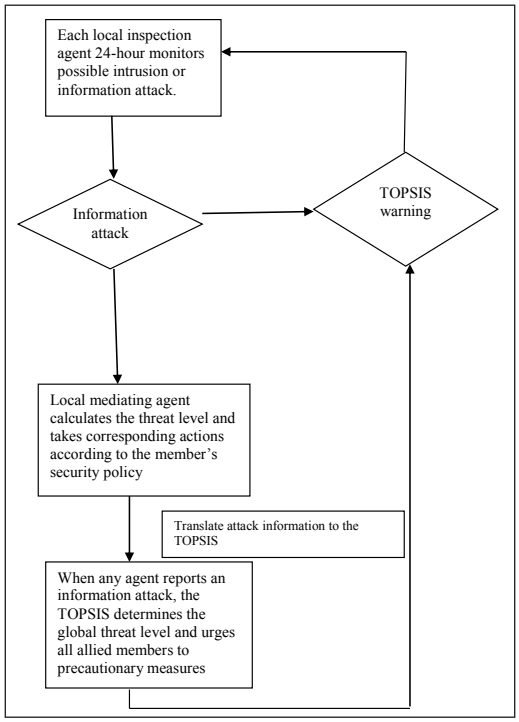
Threat Level	Action	Description
l = 0	a0	Do nothing
l = 1	a1	Increase incident monitoring and look for patterns across a wide range of variables
l = 2	a2	Disconnect extra network connection/ services
l = 3	a3	Disconnect extra network connection/ services, and stop database services
l = 4	a4	Disconnect extra network connections/ services, stop application systems, and disconnect partial intra network connection/services
l = 5	a5	Disconnect all information activities

From the above-described functions of different kinds of agent, we outline the ISFBA workflow below.

V. Workflow of ISFBA (Information Security Framework Based Agent)

Step 1: Local inspection agent collects constantly the deviations generated by the local allied member's information security system (IDS, firewall, system guards, etc.) [18]. Once it detects an information attack, it uses Eq. (1) to calculate the threat value of the attack.

Step 2: Following the inspection agent's action, the local mediating agent employs Eq. (2) to determine the threat level, and takes corresponding actions according to the allied member's security policy. Finally, it dispatches a report the attack to the TOPSIS model.



VI. TOPSIS Based Method

The Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS) method may work as the solution for routing decision making where *m* alternative routes exist. The chosen alternative should be nearest to the positive ideal solution (PIS) and farthest from the negative ideal solution (NIS). In this routing scheme e from the most trustworthy node and the longest distance from the no trustworthy node [19]. The method compares a set of options by assigning weights for each considered criterion. Weights are normalized for each criterion to prepare the decision table. Choices are compared with worst choice and the best choice to reach at an optimized solution [20]. A lot of tools are available to automate the TOPSIS method, and various performance evaluations are made on these tools.

VII. Intuitionistic Fuzzy TOPSIS

We assume that

A = {A1, A2, . . . , Am} be a set of alternatives and X = {X1, X2, . . . , Xn} be a set of criteria

The method for Intuitionistic Fuzzy TOPSIS as follows:

Step 1: We determine the weights of decision makers. Assume that decision group contains l decision makers. The importance of the decision makers are considered as linguistic terms expressed in intuitionistic fuzzy numbers.

Let Dk = [lk, mk, pk] be an intuitionistic fuzzy number for rating of k[th] decision maker. Then the weight of k[th] decision maker can be obtained as: $_{k}$

$$\lambda k = \frac{\left(\mu_k \pi_\kappa \left(\frac{\mu_\kappa}{\mu_\kappa + \nu_\kappa}\right)\right)}{\sum_{\kappa-1}^{l}\left(\mu_k \pi_\kappa \left(\frac{\mu_\kappa}{\mu_\kappa + \nu_\kappa}\right)\right)}$$

and $\sum_{\kappa-1}^{l} \lambda_\kappa = 1$ Eq. (3)

Step 2: Construct aggregated intuitionirstic fuzzy decision matrix based on the opinions of decision makers.

Let $R^{(K)} = (r_{ij}^{(K)})_{mxn}$ is an intuitionistic fuzzy decision matrix of each decision maker. $\{\lambda = \lambda_1, \lambda_2, \lambda_3 \ldots \lambda_l\}$ is the weight of each decision and $\sum_{\kappa=1}^{l} \lambda_\kappa = 1$, $\lambda_K \in [0,1]$.

In group decision-making process, all the individual decision opinions need to be fused into a group opinion to construct aggregated intuitionistic fuzzy decision matrix. In order to do that, IFWA operator proposed by Xu (2007d) is used. R= $(rij)_{mxn}$, where,

$$r_{ij} = \text{IFWA}_\lambda\left(r_{ij}^{(1)}, r_{ij}^{(2)}, \ldots, r_{ij}^{(l)}\right)$$

$$= \lambda_1 r_{ij}^{(1)} \oplus \lambda_2 r_{ij}^{(2)} \oplus \lambda_3 r_{ij}^{(3)} \oplus \cdots \oplus \lambda_l r_{ij}^{(l)}$$

$$= \left[1 - \prod_{k=1}^{l}\left(1 - \mu_j^{(k)}\right)^{\lambda_k}, \prod_{k=1}^{l}\left(v_j^{(k)}\right)^{\lambda_k}, \prod_{k=1}^{l}\left(1 - \mu_j^{(k)}\right)^{\lambda_k} - \prod_{k=1}^{l}\left(v_j^{(k)}\right)^{\lambda_k}\right]$$

Here, $r_{ij} = (\mu_{Ai}(x_j), v_{Ai}(x_j), \pi_{Ai}(xj))(i = 1, 2 \ldots, m\,; j = 1, 2, \ldots, n)$. Eq. (4)

The aggregated intuitionistic fuzzy decision matrix can be defined as follows:

$$R = \begin{bmatrix} \left(\mu_{A_1}(x_1), v_{A_1}(x_1), \pi_{A_1}(x_1)\right) & \left(\mu_{A_1}(x_2), v_{A_1}(x_2), \pi_{A_1}(x_2)\right) & \cdots & \left(\mu_{A_1}(x_n), v_{A_1}(x_n), \pi_{A_1}(x_n)\right) \\ \left(\mu_{A_2}(x_1), v_{A_2}(x_1), \pi_{A_2}(x_1)\right) & \left(\mu_{A_2}(x_2), v_{A_2}(x_2), \pi_{A_2}(x_2)\right) & \cdots & \left(\mu_{A_2}(x_n), v_{A_2}(x_n), \pi_{A_2}(x_n)\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(\mu_{A_m}(x_1), v_{A_m}(x_1), \pi_{A_m}(x_1)\right) & \left(\mu_{A_m}(x_2), v_{A_m}(x_2), \pi_{A_m}(x_2)\right) & \cdots & \left(\mu_{A_m}(x_n), v_{A_m}(x_n), \pi_{A_m}(x_n)\right) \end{bmatrix}$$

$$R = \begin{bmatrix} r_{11} & r_{12} & r_{13} & \ldots & r_{1m} \\ r_{21} & r_{22} & r_{23} & \ldots & r_{2m} \\ r_{31} & r_{32} & r_{33} & \ldots & r_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & r_{n3} & \ldots & r_{nm} \end{bmatrix}$$

Step 3: Determine the weights of criteria. All criteria may not be assumed to be equal importance. W represents a set of grades of importance. In order to obtain W, all the individual decision maker opinions for the importance of each criteria need to be fused.

Let $w_j^{(k)} = \{\mu_j^{(K)}, v_j^{(K)}, \pi_j^{(K)}\}$ be an intuitionistic fuzzy number assigned to criterion Xj by the k[th] decision maker. Then the weights of the criteria are calculated by using IFWA operator:

$$r_{ij} = IFWA\ r_{ij}^{1}, r_{ij}^{2}, \ldots \ldots r_{ij}^{l}$$

$$= \lambda_1 r_{ij}^{1} \oplus \lambda_2 r_{ij}^{2} \oplus \lambda_3 r_{ij}^{3} \oplus \ldots \oplus \lambda_l r_{ij}^{l}$$

$$= \left[1 - \prod_{k=1}^{l}\left(1 - \mu_j^{(k)}\right)^{\lambda_k}, \prod_{k=1}^{l}\left(v_j^{(k)}\right)^{\lambda_k}, \prod_{k=1}^{l}\left(1 - \mu_j^{(k)}\right)^{\lambda_k} - \prod_{k=1}^{l}\left(v_j^{(k)}\right)^{\lambda_k}\right]$$

$w = [w_1, w_2, w_3, \ldots w_j,]$ Eq. (5)

Step 4: Construct aggregated weighted intuitionistic fuzzy decision matrix. After the weights of criteria (W) and the aggregated intuitionistic fuzzy decision matrix are determined, the aggregated weighted intuitionistic fuzzy decision matrix is constructed according to the following definition (Atanassov, 1986)

$R \oplus W = \{x, \mu_{Ai}^{(x)}, \mu_w^{(x)}, v_w^{(x)} + v_w^{(x)} - v_{Ai}^{(x)}, v_w^{(x)} | x \epsilon X\}$

and

Then the aggregated weighted. Here, $r_{ij} = (\mu_{Ai}(x_i), r_{ij}, (v_{Ai}(x_i), r_{ij}, (\pi_{Ai}(x_i)$ (I = 1, 2.., m; j = 1, 2.., n).

The aggregated intuitionistic fuzzy decision matrix can be defined as follows:

$w = [w_1, w_2, w_3, \ldots w_j,]$

$$R' = \begin{bmatrix} r_{11} & r_{12} & r_{13} & \ldots & r_{1m} \\ r_{21} & r_{22} & r_{23} & \ldots & r_{2m} \\ r_{31} & r_{32} & r_{33} & \ldots & r_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & r_{n3} & \ldots & r_{nm} \end{bmatrix}$$ Eq. (6)

Step 5: Obtain intuitionistic fuzzy positive-ideal solution and intuitionistic fuzzy negative-ideal solution.

Let J1 and J2 be benefit criteria and cost criteria, respectively. A* is intuitionistic fuzzy positive-ideal solution and A is intuitionistic fuzzy negative-ideal solution.

Then A* and A[-] are obtained as:

$A^* = (\mu_{A^*W}(x_j), v_{A^*W}(x_j))$ and $(\mu_{A\text{-}W}(x_j), v_{A\text{-}W}(x_j))$ Eq. (7)

where,

$\mu_{A^*W}(x_j) = (\max i\ (\mu_{A^*W}(x_j) \mathrm{I} j \epsilon j_1), (\min i\ (\mu_{A^*W}(x_j) \mathrm{I} j \epsilon j_2)$

$v_{A^*W}(x_j) = (\max i\ (v_{A^*W}(x_j) \mathrm{I} j \epsilon j_1), (\min i\ (v_{A^*W}(x_j) \mathrm{I} j \epsilon j_2)$

$\mu_{A\text{-}W}(x_j) = (\max i\ (\mu_{A\text{-}W}(x_j) \mathrm{I} j \epsilon j_1), (\min i\ (\mu_{A\text{-}W}(x_j) \mathrm{I} j \epsilon j_2)$

$v_{A\text{-}W}(x_j) = (\max i\ (v_{A\text{-}W}(x_j) \mathrm{I} j \epsilon j_1), (\min i\ (v_{A\text{-}W}(x_j) \mathrm{I} j \epsilon j_2)$

Step 6: Calculate the separation measure:

$$S^* = \sqrt{\frac{1}{2n}\sum_{j=1}^{n}\left[\left(\mu_{A_iW}(x_j) - \mu_{A^*W}(x_j)\right)^2 + \left(v_{A_iW}(x_j) - v_{A^*W}(x_j)\right)^2 + \left(\pi_{A_iW}(x_j) - \pi_{A^*W}(x_j)\right)^2\right]}$$

$$S^- = \sqrt{\frac{1}{2n}\sum_{j=1}^{n}\left[\left(\mu_{A_iW}(x_j) - \mu_{A^-W}(x_j)\right)^2 + \left(v_{A_iW}(x_j) - v_{A^-W}(x_j)\right)^2 + \left(\pi_{A_iW}(x_j) - \pi_{A^-W}(x_j)\right)^2\right]} \quad \text{Eq. (8)}$$

Step 7: Calculate the relative closeness coefficient to the intuitionistic ideal solution.

$C_{i^*} = \frac{S_{\tilde{i}-}}{S_{\tilde{i}^*}+S_{\tilde{i}-}}$ where, $0 \le C_{i^*} \le 1$ Eq. (9)

Step 8: Rank the alternatives**.** After the alternative closeness coefficient of each alternative is determined, alternative are ranked according to descending order C_{i^*}'*S*.

VIII. Conclusion

In this paper we give the idea about environment of agents and information security framework based on an intelligent agent based on a intuitionistic fuzzy TOPSIS model. That combines all distributed information security facilities to achieve efficiently collaborative information security. In the framework, an allied member can still obtain information protection even it does not install any security devices or system. Moreover, it will use a warning mechanism for allied members to take action to protect their information resources before they suffer information attack.

References

[1] Mohd. Abomhara, and G. M. Koien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders, and attacks," *Journal of Cyber Security*, vol. 4, no. 1, pp. 65-88, 2015.

[2] K. F. Chiang, and S. W. Cheng, "Using analytic hierarchy process method and technique for order preference by similarity to ideal solution to evaluate curriculum in department of risk management and insurance," *Journal of Social Sciences*, vol. 19, no. 1, pp. 1-8, 2009.

[3] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, and A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," *Engineering Applications of Artificial Intelligence*, vol. 26, no. 9, pp. 2105-2127, 2013.

[4] J. L. Deng, "Introduction to grey system theory," *Journal of Grey Theory*, vol. 1, no. 1, pp. 1-24, 1988.

[5] Z. Hellwig, "Zastosowania metody taksonomicznej do typologicznego podziału krajów ze względu na poziom rozwoju i strukturę wykwalifikowanych kadr," *Przegląd Statystyczny*, no. 4, pp. 307-327, 1968.

[6] C. C. Hung, and L. H. Chen, "A fuzzy TOPSIS decision making model with entropy weight under intuitionistic fuzzy environment," *Proceedings of the International Multi-Conference of Engineers and Computer Scientists IMECS, Hong Kong*, 2009.

[7] G. R. Jahanshahloo, F. H. Lofti, and M. Izadikhah, "An algorithmic method to extend TOPSIS for decision-making problems with interval data," *Applied Mathematics and Computation*, vol. 175, pp. 1375-1384, 2006a.

[8] G. R. Jahanshahloo, F. H. Lofti, and M. Izadikhah, "Extension of the TOPSIS method for decision-making problems with fuzzy data," *Applied Mathematics and Computation*, vol. 181, pp. 1544-1551, 2006b.

[9] O. Jadidi, T. S. Hong, F. Firouzi, R. M. Yusuff, and N. Zulkifli, "TOPSIS and fuzzy multi-objective model integration for supplier selection problem," *Journal of Achievements in Materials and Manufacturing Engineering of Achievements in Materials and Manufacturing Engineering*, vol. 31, no. 2, pp. 762-769, 2008.

[10] O. Jadidi, T. S. Hong, F. Firouzi, and R. M. Yusuff, "An optimal grey based approach based on TOPSIS concept for supplier selection problem," *International Journal of Management Science and Engineering Management*, vol. 4, no. 2, pp. 104-117, 2008.

[11] C. Kahraman, "Fuzzy multi-criteria decision making theory and application with recent development," *Optimization and its Applications,* vol. 16, Springer, New York, 2008.

[12] C. Kahraman, G. Buyukozkan, and N. Y. Ates, "A two-phase multi-attribute decision making approach for new products introduction," *Information Sciences*, vol. 177, pp. 1567-1582, 2007. S. Liu, and Y. Lin, "Grey information," *Theory and Practical Applications*, 2006.

[13] X. Fuwen, "Optimal analysis of discontinuous data path mining in cloud computing environment [J]," *Computer Simulation*, vol. 35, no. 6, pp. 432-435, 2018.

[14] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing [J]," *Future Generation Computer Systems*, vol. 78, pp. 964-975, 2018.

[15] Z. S. Xu, "Models for multiple attribute decision making with intuitionistic fuzzy information," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 15, pp. 285-297, 2007c.

[16] M. E. Porter, and V. E. Millar, "How information gives you competitive advantage," *Harvard Business Review*, vol. 63, no. 4, pp. 149-160, 1985.

[17] Z. S. Xu, "Some similarity measures of intuitionistic fuzzy sets and their applications to multiple attribute decision making," *Fuzzy Optimization and Decision Making*, vol. 6, pp. 109-121, 2007b.

[18] P. Wang, "QoS-aware web services selection with intuitionistic fuzzy set under consumer's vague perception," *Expert Systems with Applications*, vol. 36, no. 3, pp. 4460-4466, 2009.

[19] W. Q. Wang, and X. L. Xin, "Distance measure between intuitionistic fuzzy sets," *Pattern Recognition Letters*, vol. 26, pp. 2063-2069, 2005.

[20] E. Szmidt, and J. Kacprzyk, "A similarity measure for intuitionistic fuzzy sets and its application in supporting medical diagnostic reasoning," *Lecture Notes in Computer Science*, vol. 3070, pp. 388-393, 2004.