International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:6, No:6, 2012

Graphical Password Security Evaluation by Fuzzy AHP

Arash Habibi Lashkari, Azizah Abdul Manaf, Maslin Masrom

***Abstract*—**In today's day and age, one of the important topics in information security is authentication. There are several alternatives to text-based authentication of which includes Graphical Password (GP) or Graphical User Authentication (GUA). These methods stems from the fact that humans recognized and remembers images better than alphanumerical text characters. This paper will focus on the security aspect of GP algorithms and what most researchers have been working on trying to define these security features and attributes. The goal of this study is to develop a fuzzy decision model that allows automatic selection of available GP algorithms by taking into considerations the subjective judgments of the decision makers who are more than 50 postgraduate students of computer science. The approach that is being proposed is based on the Fuzzy Analytic Hierarchy Process (FAHP) which determines the criteria weight as a linear formula.

***Keywords*—**Graphical Password, Authentication Security, Attack Patterns, Brute force attack, Dictionary attack, Guessing Attack, Spyware attack, Shoulder surfing attack, Social engineering Attack, Password Entropy, Password Space.

I. INTRODUCTION

IN describing Graphical Based Passwords, researchers coined the term "Picture Superiority Effect" which shows the effect of GBP being used as a solution for the conventional password techniques. It also underlines the impact of GBP and highlighting the fact that graphics and text are easier to commit to memory than those techniques.

Initially, the concept of Graphical User Authentication (GUA) (Graphical Password or Graphical Image Authentication (GIA)) described by Blonder (Blonder, 1996), one image would appear on the screen of whereupon the user would click on a few chosen regions on the image. Authentication is done when the user clicks on the correct regions. Security is one of the major issues in graphical passwords and should be evaluated and measured [1]-[3].

There are many researches on this area that shows the security of GP are related to the multiple factors such as entropy, password space and related attacks [1], [3]. These factors proved that it is not possible to simply find a formula that evaluates graphical password algorithms. Procedure for Paper Submission

Arash Habibi Lashkari is with Advanced Informatics School (AIS), University Technology Malaysia (UTM), Kuala Lumpur, Malaysia (e-mail: a_habibi_L@Hotmail.com).

Azizah Abdul Manaf is with Advanced Informatics School (AIS), University Technology Malaysia (UTM), Kuala Lumpur, Malaysia (e-mail: aazizah07@ic.utm.m).

Maslin Masrom is with Razak School of Engineering and Advanced Technology, University Technology Malaysia (UTM), Kuala Lumpur, Malaysia (e-mail: maslin@ic.utm.my).

So, till now, there isn't a complete evaluation model for evaluating the security of graphical password algorithms based on all the related aspects [3].

Meanwhile, there are many types of multi-criteria techniques for decision making like PROMETHEE, ELECTRE, and Analysis Hierarchy Process (AHP). These techniques use the best opinions from all possible alternatives using multiple, sometimes conflicting, decision criteria. The AHP technique investigated in the present study is a multi-criteria decision making technique developed by Saaty [4]. Although traditional AHP technique may display expert knowledge, it cannot reflect human thinking [4]. Therefore, FAHP technique was developed [4]. So, we will try to propose a complete security evaluation criterion for most graphical password (GP) algorithms including the related aspects in GP.

II. OUR PROPOSED FRAMEWORK

For the proposed Fuzzy AHP technique, five steps have been defined, as shown on fig. 1.

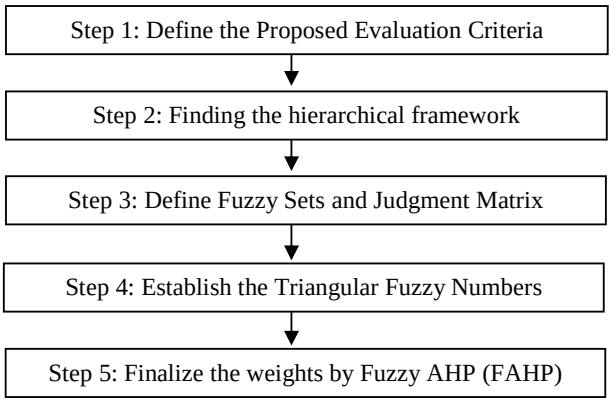

Fig. 1 The framework of proposed evaluation criteria

III. GRAPHICAL PASSWORD ALGORITHMS

In this section, we will present three major categories of graphical password techniques. In general, Most of articles from 1995 till 2011 show that Graphical passwords techniques are classified in three categories [1] which explain in continue sections (Please refer to "Graphical User Authentication (GUA)" book [1] for a comprehensive survey of the existing graphical password techniques since 1995 till 2010).

A. Pure Recall Based Techniques

Users reproduce their passwords, without having the chance to use the reminder marks of system. Although easy and convenient, it appears that users do not quite remember their passwords. Table I shows some of the algorithms which were created based on this technique.

TABLE I
PURE-RECALL BASED TECHNIQUES ORDERED BY DATE

Algorithm	Proposed Date	Created By
Draw a Secret (DAS)	1999	Jermyn Ian et al.
Passdoodle	1999	Christopher Varenhorst
Grid Selection	2004	Juaie Thorpe, P.C. Van Oorschot
Syukri	2005	Syukri, et al.
Qualitative DAS (QDAS)	2007	Di Lin, et al.

B. Cued Recall Based Techniques

Here, the system provides a framework of reminders, hints and gestures for the users to reproduce their passwords or make a reproduction that would be much more accurate. TABLE 2 lists some of the algorithms which were created based on this technique.

TABLE II
CUED-RECALL BASED TECHNIQUES ORDERED BY DATE

Algorithm	Proposed Date	Created By
Blonder	1996	Greg E. Blonder
Passlogix v-Go	2002	Passlogic Inc. Co.
VisKey SFR	2003	SFR Company
PassPoint	2005	Susan Wiedenbeck, et al.
Pass-Go	2006	-
Passmap	2006	Roman V. Vamponski
Background DAS (BDAS)	2007	Paul Duaphi

C. Recognition Based Techniques

Here, users select pictures, icons or symbols from a bank of images. During the authentication process, the users have to recognize their registration choice from a grid of image. Research has shown that "90% of users can remember their password after one or two months" [15]. Table-3 shows some of the algorithms which were created based on this technique.

TABLE III
RECOGNITION BASED TECHNIQUES ORDERED BY DATE

Algorithm	Proposed Date	Created By
Passface	2000	Sacha Brostoff , M. Angela Sasse
Déjà vu	2000	Rachna Dhamija, drian Perrig
Triangle	2002	Leonardo Sobrado , J-Canille Birget
Movable Frame	2002	Leonardo Sobrado , J-Canille Birget
Picture Password	2003	Wayne Jansen, et al.
WIW	2003	Shushuang Man, et al.
Story	2004	Darren Davies, et al.

Now, after a simple review on three categories of graphical password, next section tries to in the following section the GUA's algorithms will review and study.

IV. GRAPHICAL PASSWORDS' SECURITY ASPECTS

In regards to the Magic Triangle evaluation criteria [3], that we have proposed, we defined a triangular of attributes that can be used to test graphical password security, namely attack, password space and password entropy as shown in fig. 2. With reference to previous researches [3], it is possible to calculate the password space and entropy by using mathematical formulas. However in order to measure the attacks attribute, we must evaluate the attack resistance of each graphical password related attacks.

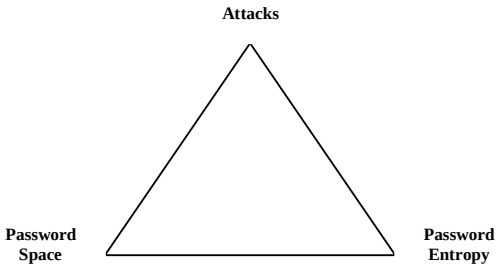

Fig. 2 Magic triangle evaluation for graphical passwords security

This also proves that we cannot use a general evaluation method to compare and test different algorithms. In the following section, we will try to explain the different attacks and the related formulas that will be used to calculate password space and entropy.

A. Graphical Passwords related Attacks

Based on the International Attacks Patterns Standard (CAPEC 2011) as well as related researches, at present there are seven common graphical password attacks, namely:

Brute Force Attack (BFA): The attack that tries to find every possible combination of password in order to break it (CAPEC-49).

Dictionary Attack: This method checks for words in a preset dictionary and test whether they are being used as a password or not (CAPEC-16).

Spyware Attack: Spyware installed themselves on a users' computer and records sensitive data for the attacker [3]

Shoulder Surfing Attack: Attackers will peer over a person's shoulder in order to find out their password [3]

Social Engineering Attack (Description Attack) (SEA): An attacker that impersonates an authorised employee by getting information through other employees in the organisation (CAPEC-403).

Guessing Attack: This type of attack guesses a user's password by using common personal information such as name of their pets, passport number, family name and so forth [1].

B. Password Space

The last resource on December 2010 defines the password spaces formula [1]:

PS= M^N

In this formula, M represents the number of images in each round while N represents the number of rounds. However, in regards to the triangle method and movable frame algorithms in this formula along with the process of finding and selecting the line and triangle values, it is not possible to calculate the accurate password space using this formula.

C. Password Entropy

In order to measure the security of passwords that has been generated, password entropy is used. It is a method of measuring the level of difficulty in guessing the password blindly. For example, let's assume that all passwords are distributed evenly; we can use the formula below to calculate the password entropy of the GP [1].

PE = N log2 (|L||O||C|)

Basically, graphical password entropy measures the probability of an attacker randomly guessing the correct password. In the formula, N represents the length or number of runs, L is the locus alphabet as the set of all loci, O represents and object alphabet and color is represent by C.

Although, it is possible to calculate the password entropy for some algorithms using this formula, it is not applicable to all algorithms [1].

V. Fuzzy Logic and Fuzzy Set

Fuzzy numbers are the special classes of the fuzzy quantities. It is a fuzzy quantity M that represents the generalization of r, a real number. Intuitively, M(x) should be a measure of how well M(x) approximates "r" [5].

The convex normalized fuzzy set is the fuzzy number f. It characterized the given interval if real numbers, with a grade between 0 and 1 for each membership. Of course, it is possible to use different fuzzy number for different conditions. Generally in practice triangular and trapezoidal fuzzy numbers are used [6].

Typically, it is more convenient to work with triangular fuzzy numbers (TFNs) in applications because it is computationally simpler. Also, they are more useful when promoting the representation and information processing in a fuzzy environment.

Fig. 3 below shows the triangular fuzzy number, M:

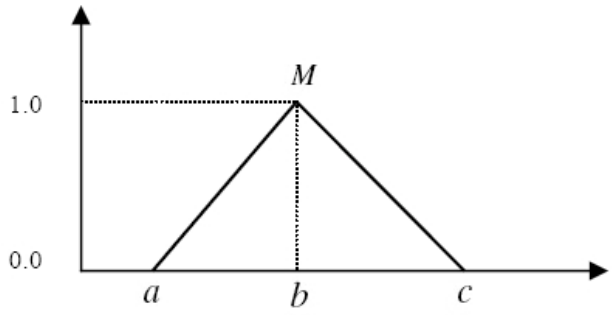

Fig. 3 A triangular fuzzy number, M

Three real number, expressed as a, b and c, are defined in TFNs. These parameters respectively represent the smallest value possible, followed by the most promising value and finally the largest possible value that describes the fuzzy event. The function of the membership can be described as;

$$\mu(x/M) = \begin{cases} 0, & x < l \\ \frac{x-a}{b-a} & a \le x \le b \\ \frac{c-x}{c-b} & b \le x \le c \\ 0, & x > u \end{cases} \quad (1)$$

The different operations can be defined by the triangular fuzzy numbers. However, there are three important operations being used in this study. For example, if we define two positive fuzzy numbers of x= (xa, xb, xc) and y= (ya, yb, yc) then it would be:

x+y= (xa, xb, xc)+ (ya, yb, yc) = (xa +ya, xb +yb, xc +yc) (2)

x*y= (xa, xb, xc)* (ya, yb, yc) = (xa ya, xb yb, xc yc) (3)

x -1= (xa, xb, xc)-1 = (1/xa, 1/xb, 1/xc) (4)

z*x=z*(xa, xb, xc)= (zxa, zxb, zxc) (5)

Other algebraic fuzzy numbers operations can be found in [7, 8].

VI. AHP and Fuzzy-AHP (FAHP)

There are several fuzzy AHP methods, but the authors of this paper prefer Chang's extent analysis method since the steps of this approach is relatively easier compare to the other methods. In the following, the outlines of the extent analysis method on fuzzy AHP are given as: Let X = (x1, x2, . . . ,xn) be an object set, and U = (u1,u2, . . . ,um) be a goal set. Based on Chang's extent analysis [9], each object is taken and extent analysis for each goal, gi, is performed respectively. Therefore, m extent analysis values for each object can be obtained, with the following signs:

$M_{gi}^1, M_{gi}^2, \ldots, M_{gi}^m \qquad i = 1,2,\ldots,n$

Where all the $M_{gi}^j \ (i = 1,2,\ldots,n)$ are triangular fuzzy numbers (TFNs). Respectively, they are the lowest possible value, most possible value and largest possible value.

Fig. 6 illustrates a TFN that is represented as a, b, and c.

The steps of Chang's extent analysis can be given as follows:

Step1:

The value of the fuzzy synthetic extent with respect to the ith object is defined as:

$$S_i = \sum_{j=1}^{m} M^j{}_{gi} * \left[\sum_{i=1}^{n}\sum_{j=1}^{m} M^j{}_{gi}\right]^{-1} \quad (6)$$

To obtain $\sum_{j=1}^{m} M^j{}_{gi}$ perform the fuzzy addition operation of m extent analysis values for a particular matrix as:

$$\sum_{j=1}^{m} M^j{}_{gi} = \left(\sum_{j=1}^{m} a_{ij}, \sum_{j=1}^{m} b_{ij}, \sum_{j=1}^{m} c_{ij}\right),\ i = 1,2,\dots,n \quad (7)$$

Regarding to the fuzzy addition operation such as Equation 5, it is possible to define:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} M^j{}_{gi} = \left(\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}, \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}, \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}\right) \quad (8)$$

And then compute the inverse of the vector in Equation. such that:

$$\left[\sum_{i=1}^{n}\sum_{j=1}^{m} M^j{}_{gi}\right]^{-1} = \left(\frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}}\right) \quad (9)$$

So it is possible to compute S_i such that:

$$S_i = \left(\sum_{j=1}^{m} a_{ij}, \sum_{j=1}^{m} b_{ij}, \sum_{j=1}^{m} c_{ij}\right) * \left(\frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}}\right) \quad i = 1,2,\dots,n \quad (10)$$

Step2:

The degree of possibility of $M_2 = (a_2, b_2, c_2) \geq M_1 = (a_1, b_1, c_1)$ is defined as:

$$V(M_2 \geq M_1) = \mathrm{Sup}_{Y \geq x}[\min(\mu_{M1}(X),\ \mu_{M2}(y))] \quad (11)$$

And can be equivalently expressed as below:

$$V(M_2 \geq M_1) = hip(M_1 \cap M_2) = \mu_{M2}(d) = \begin{cases} 1, & if\ b_2 \geq b_1 \\ 0, & if\ a_1 \geq c_2 \\ \frac{a_1 - c_2}{(b_2 - c_2) - (b_1 - a_1)}, & Otherwise \end{cases} \quad (12)$$

Where d is the ordinate of the highest intersection point D between μ_{M1} and μ_{M2} (Fig. 4).

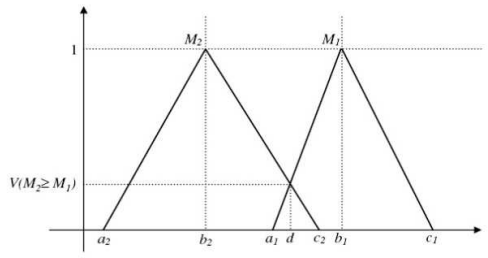

Fig. 4 the intersection between $M_1 and\ M_2$

For comparing M_1 and M_2, we need both the value of $V(M_2 \geq M_1)$ and $V(M_1 \geq M_2)$.

Step3:

The degree of possibility for a convex fuzzy number to be greater than K convex fuzzy number $M_i(i = 1,2,\dots,k)$ can be defined by:

$$V(M \geq M_1, M_2, \dots, M_K) = V[(M \geq M_1) and (M \geq M_2) and \dots and\ (M \geq M_k)] = \min V(M \geq M_i),\ i = 1,2,3\dots,k \quad (13)$$

Assume that:

$$d(A_i) = \min V(S_i \geq S_k)\ \ K = 1,2,\dots,n;\ k \neq i \quad (14)$$

Then the weight vector is given by:

$$W' = (d'(A_1), d'(A_2), \dots, d'(A_n))^T \quad (15)$$

That $A_i(i = 1,2,\dots,n)$ has n elements

Step 4:

Via, normalization, the normalized weight vectors are:

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T \quad (16)$$

That W is a non-fuzzy number.

It is impossible to create mathematical operations directly using security evaluation values especially the common attack values. The best way is to convert the attack scale into a fuzzy scale. There is a variety of different fuzzy scales [10-13], The triangular fuzzy conversion scale in this paper - shown in table 4 below, is used in the evaluation model founded by Gumus (2009) [8].

TABLE IV
TRIANGULAR FUZZY CONVERSION SCALE

Row	Security	Triangular	Triangular
1	Just equal	(1,1,1)	(1,1,1)
2	Moderate	(1,3,5)	(1/5,1/3,1)
3	Weakly more	(3,5,7)	(1/7,1/5,1/3)
4	Strong	(5,7,9)	(1/9,1/7,1/5)
5	Very strong	(7,9,11)	(1/11,1/9,1/7)

VII. PROPOSED SYSTEM AND HIERARCHICAL DIAGRAM

We would like to propose an evaluation methodology to examine the security strength of graphical password algorithms. In order to yield the proper result, the method that was chosen - fuzzy AHP, requires a hierarchical structure. Referring to the last security evaluation criteria which is the magic rectangle discovered by Lashkari (2011) [3], The main variables for security evaluation in graphical passwords are C1: Password Space (PS), C2: Password Entropy (PE) and Common Attacks namely C3: Brute Force Attack (BTA), C4: Dictionary Attack (DA), C5: Spyware Attack (SA), C6: Shoulder Surfing Attack (SSA), C7: Social Engineering Attack (Description Attack) (SEA), C8: Guessing Attack (GA). Fig. 6 shows the hierarchical structure that is considered for this proposed system. It is based on a graphical password technique (GPT) and will be evaluated by the system (Fig. 5).

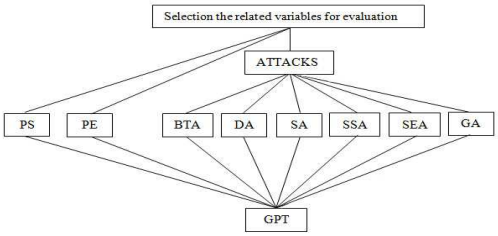

Fig. 5 The hierarchy to security evaluation of graphical passwords

More than fifty postgraduate computer security students have worked to build pair-wise comparison matrixes for the attributes. Figure 6 below shows an example of a questionnaire that is provided to retrieve the first numerical evaluation matrix. The geometrical mean of individual evaluations is taken and calculated to get the accurate result.

This questionnaire submitted to more than fifty postgraduate students which studied and worked in computer security area. The average of the participants' answers, as pair-wise comparison values are converted into TFN values, as shown in the table matrix where the main attribute is being built (Table V).

Once the fuzzy pair-wise comparison matrix has been formed, the weights of all criteria can be determined with the help of FAHP. The first synthesis value should be calculated according to the FAHP method.

Q.	Attributes	Fuzzy Scale					Reciprocal Scale					Attributes
		1	2	3	4	5	1	2	3	4	5	
Q1	Password Space (PS)											Password Entropy (PE)
Q2												Brute Force Attack (BTA)
Q3												Dictionary Attack (DA)
Q4												Spyware Attack (SA)
Q5												Shoulder Surfing Attack (SSA)
Q6												Social Engineering Attack (Description Attack) (SEA)
Q7												Guessing Attack (GA)
Q9	Password Entropy (PE)											Brute Force Attack (BTA)
Q10												Dictionary Attack (DA)
Q11												Spyware Attack (SA)
Q12												Shoulder Surfing Attack (SSA)
Q13												Social Engineering Attack (Description Attack) (SEA)
Q14												Guessing Attack (GA)
Q16	Brute Force Attack (BTA)											Dictionary Attack (DA)
Q17												Spyware Attack (SA)
Q18												Shoulder Surfing Attack (SSA)
Q19												Social Engineering Attack (Description Attack) (SEA)
Q20												Guessing Attack (GA)
Q22	Dictionary Attack (DA)											Spyware Attack (SA)
Q23												Shoulder Surfing Attack (SSA)
Q24												Social Engineering Attack (Description Attack) (SEA)
Q25												Guessing Attack (GA)
Q27	Spyware Attack (SA)											Shoulder Surfing Attack (SSA)
Q28												Social Engineering Attack (Description Attack) (SEA)
Q29												Guessing Attack (GA)
Q31	Shoulder Surfing Attack (SSA)											Social Engineering Attack (Description Attack) (SEA)
Q32												Guessing Attack (GA)
Q34	Social Engineering Attack (SEA)											Guessing Attack (GA)

Fig. 6 questionnaire for collect the evaluators' feedbacks

TABLE V
FUZZY PAIRWISE COMPARISON MATRIX

Criteria	**C1:** (PS)	**C2:** (PE)	**C3:** (BTA)	**C4:** (DA)	**C5:** (SA)	**C6:** (SSA)	**C7:**(SEA)	**C8:**(GA)
C1	1,1,1	3,5,7	3,5,7	1,3,5	1,3,5	1,3,5	1,3,5	1,3,5
C2	1/7,1/5,1/3	1,1,1	3,5,7	3,5,7	3,5,7	1,3,5	3,5,7	3,5,7
C3	1/7,1/5,1/3	1/7,1/5,1/3	1,1,1	1,3,5	1,3,5	3,5,7	1,3,5	1,1,1
C4	1/5,1/3,1	1/5,1/3,1	1/5,1/3,1	1,1,1	1,3,5	1,1,1	1,1,1	1,3,5
C5	1/5,1/3,1	1/7,1/5,1/3	1/5,1/3,1	1/5,1/3,1	1,1,1	1,1,1	1,1,1	3,5,7
C6	1/5,1/3,1	1/5,1/3,1	1/7,1/5,1/3	1,1,1	1,1,1	1,1,1	1,3,5	1,3,5
C7	1/5,1/3,1	1/7,1/5,1/3	1/5,1/3,1	1,1,1	1,1,1	1/5,1/3,1	1,1,1	1,1,1
C8	1/5,1/3,1	1/7,1/5,1/3	1,1,1	1/5,1/3,1	1/7,1/5,1/3	1/5,1/3,1	1,1,1	1,1,1

By calculating the same way as in Equation (6) using operation based on Eq. (3), we can find the synthesis values namely Sc1, Sc2, Sc3, Sc4, Sc5, Sc6, Sc7, Sc8. After this we need to calculate the V matrix which has 64 cells (8*8) namely V(Sc1≥Sc2), based on Eq. (12). Finally based on Eq. (14), it is possible to calculate the d'(c1)…d'(c8) which are the weights of our attributes. Based on this research and data collection the result of attributes were w'= (0.808, 0.890, 0.370, 0.470, 0.110, 0.509, 0.080, 0.187, 0.288).

VIII. CONCLUSION

User authentication is the most important and critical elements in Information Security. Regarding to the weaknesses of textual passwords, graphical Passwords (GP) are the most desirable alternative to textual passwords.

In order to select the best GP algorithms based on issues related to security, some arguments should be consider such as password spaces, password entropies and the strength or weakness to common attacks. To select the best GUA, this paper suggests the integration of Fuzzy AHP. Fuzzy AHP can be used to determine the criteria weights and priority values of the GP algorithms using the nine common security related attributes and issues. This method is very useful when evaluating complex multiple criteria alternatives that includes subjective and uncertain judgments. For collecting the basic pair-wise matrix, a questionnaire has submitted to more than fifty postgraduate computer security students. Finally a linear formula has generated for selecting the best GUA algorithm that covered suits security purposes and requirements.

ACKNOWLEDGMENT

This paper is supported by project UTM-J-13-01/25.10/3/02H07 (1) from Research University Grant (RUG) of University Technology Malaysia (UTM).

REFERENCES

[1] Lashkari, A.H. and F. Towhidi, *Graphical User Authentication (GUA)*. 2010: Lambert Academic Publisher.
[2] Lashkari, A.H., et al., Shoulder Surfing attack in graphical password authentication. 2009, International Journal of Computer Science and Information Security (IJCSIS).
[3] Lashkari, A.H., et al., Security Evaluation for Graphical Password, in The International Conference on Digital Information and Communication Technology and its Applications (DICTAP2011). 2011, Communications in Computer and Information Science (CCIS) Series of Springer LNCS: Université de Bourgogne, France.
[4] Saaty, T.L., How to make a decision: The Analytic Hierarchy Process. European Journal of Operational Research 1990. 48 p. 9-26.
[5] Nguyen, H.T. and E.A. Walker, A First Course in Fuzzy Logic. 1997: CRC Press.
[6] Klir, G.J. and B. Yuan, Fuzzy Sets and Fuzzy Logic Theory and Applications. 1995, New Jersey: Prentice Hall.
[7] Zimmermann, H.-J., Fuzzy Set Theory and its Applications. Third Edition ed. 1996: Kluwer Academic Publishers.
[8] Ballı, S. and S. Korukoğlu, Operating System Selection using Fuzzy AHP and Topsis Methods. Mathematical and Computational Applications, 2009. 14(2): p. 119-130.
[9] Wang, Y.-M. and T.M.S. Elhag, Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment. Expert Systems with Applications, 2006. 31.
[10] Kreng, V.B. and C.Y. Wu, Evaluation of knowledge portal development tools using a fuzzy AHP approach: The case of Taiwanese stone industry. European Journal of Operational Research, 2005.
[11] Erensala, Y.C., T. Öncanb, and M.L. Demircan, Determining key capabilities in technology management using fuzzy analytic hierarchy process: A case study of Turkey. Information Sciences, 2006. 176(18): p. 2755-2770
[12] Kahraman, C., U. Cebeci, and D. Ruan, Multi-attribute comparison of catering service companies using fuzzy AHP: The case of Turkey. International Journal of Production Economics, 2004. 87.
[13] Leung, L.C. and D. Cao, On consistency and ranking of alternatives in fuzzy AHP. European Journal of Operational Research, 2000. 124: p. 102-113.