SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Authentication Methods Selection in Information Security through Hybrid AHP and EGT

Bee Wah Loo[1,*], Pei Ling Tan[1], Siew Kian Tey[1], Wan Yoke Chin[1]

[1] Department of Mathematical and Data Science, Faculty of Computing and Information Technology, Tunku Abdul Rahman University of Management and Technology, Setapak, 53300 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 11 December 2023
Received in revised form 23 January 2024
Accepted 19 July 2024
Available online 20 August 2024

Keywords:

MCDM; AHP; EGT; Authentication; Information security

ABSTRACT

The information security leader frequently encounters the challenge of choosing the appropriate defence strategy. Effective multi-criteria decision-making (MCDM) is essential in the field of information security for determining the optimal strategies that involve more than one party. To address this challenge, we propose a hybrid model that combines the strengths of the Analytic Hierarchy Process (AHP) with Evolutionary Game Theory (EGT). The hybrid model helps the information security leader assess the criteria for security controls and make the optimal decisions to protect the organization's data. Initially, the AHP is utilized to assess the criteria of information security control. Subsequently, the priority of the alternatives is established through evaluating these criteria. Furthermore, we will construct a defence-attack circumstance using the EGT framework, which involves formulating strategies and determining payoffs for both the information security leaders and attackers involved. We utilize the replicator dynamic to examine the process of evolution in the game, resulting in the determination of the optimal strategy. A case study is conducted to determine the optimal strategy for information security leaders and attackers. The result indicates that the best defence strategy is password protection, followed by token-based and biometric-based protections. On the other hand, the optimal strategy for attackers is no attack, followed by attack and moderate attack. This study contributes to the multi-criteria decision-making (MCDM) problem's solving by considering the dynamic aspect between both defender and attacker in the context of information security.

1. Introduction

Enterprises face significant challenges related to information security in the rapidly changing technological environment of nowadays, necessitating effective decision-making processes that take into account a range of viewpoints, multifaceted criteria, and dynamic interactions. As industries depend more and more on digital solutions to promote efficiency, innovation, and competitive advantage, making optimal decisions in information security issues becomes essential [1].

* *Corresponding author.*
E-mail address: loobw@tarc.edu.my

https://doi.org/10.37934/araset.50.2.171185

In the complex web of digital systems, where decision-makers must deal with issues from software selection and resource allocation to strategic planning and risk management, is the framework in which information security problem-solving takes place [2]. Information security issues can be seen in a variety of industries, including business, healthcare, finance, and government, all of which have specific technology requirements and complexities. Information security leaders in organizations frequently struggle to select appropriate authentication control alternatives. Advanced decision support approaches that can accommodate the complexities of the information security ecosystem are required due to the complex interaction of agents and the rapid pace of technological change [3].

This research holds significant importance for a multitude of stakeholders. Organizations stand to benefit from more efficient and effective information security decision-making, which can lead to enhanced system performance, and improved overall outcomes [4]. Practitioners, information security leaders, and decision-makers will gain a comprehensive toolkit to navigate the complexities of information security problem-solving, ultimately contributing to improved business performance and innovation [5]. Additionally, academia and the broader research community will gain insights into the application of interdisciplinary approaches in addressing real-world information security challenges.

The priority ranking of information security authentication methods is determined by various criteria, making this a MCDM problem. MCDM methods are widely applied to properly formulate and evaluate the multi-criteria problem in a systematic manner. Numerous techniques have been constructed for their application in a range of fields, where the most popular MCDM method is AHP, ranging from financial [6], business [7], and courier service [8] to the fuel industry [9], and energy resources [10]. Some researchers integrated AHP with other techniques to solve MCDM problems. Lam *et al*., [11] applied the AHP-TOPSIS method to select mobile phones among undergraduate students. Rizam *et al.*, [12] analysed the HVAC semi-hermetic compressor maintenance strategy by AHP-FMEA. Integration of AHP-SOM-CGT was implemented by Zhao *et al*., [13] in ecosystem health risk assessment. Nevertheless, most of the MCDM approaches do not take the dynamic aspect of decision-making into account.

In this study, we aim to integrate two mathematical approaches, namely the AHP and EGT, in an effort to effectively prioritize rankings of security authentication criteria and identify optimal strategies based on the dynamic progress of the players in the game. The AHP was initially developed by Thomas L. Saaty in the 1970s and has been subject to numerous enhancements and investigations ever since. It serves as a powerful tool for making complex decisions by assisting decision-makers in determining priorities and selecting the most suitable course of action from a range of alternatives. Various fields utilize the AHP method, such as networking [14-17] and information analysis [1,2,5], for solving relevant problems. Furthermore, the AHP offers a mathematical approach to evaluate decision-makers validity and mitigate biases. It considers all assessment criteria and alternatives to assist decision-makers in selecting optimal features. In terms of information security, the AHP can be used to prioritize security authentication attributes.

Despite the improvements in decision support systems, there remains a gap in our knowledge regarding a comprehensive methodology that seamlessly incorporates both the systematic evaluation of alternatives and the modelling of strategic interactions within information security problem-solving contexts. In a real-world environment of information security, there exists an ongoing interplay between attackers seeking unauthorized access to systems and security leaders striving to protect organizational data. According to Said [18] and Viveros *et al.*, [19], AHP may overlook the dynamic nature of information security environments and the competitive interactions among stakeholders. Therefore, it is crucial to consider the interaction that occurs between these

two parties. Game theory is a systematic method that studies the interaction strategies among rational participants. It has gained popularity in analysing the goals and tactics of all participants involved in information security warfare, including the interaction between attackers and security leaders. Its application in solving network security issues and simulating attack-defence behaviours has drawn significant attention [20]. Nevertheless, creating a payoff matrix using game theory alone is exceedingly difficult; a systematic approach is needed to overcome the problem. Some researchers applied AHP to accommodate constructing the payoff matrix.

Using the AHP approach in the initial phase, Rajbhandari and Snekkenes [21] assessed the efficacy of the characteristic controls related to information security. In the second phase, the authors deploy game theory and risk analysis to make decisions. Chowdhury, Tashikur Rahman, and Jang [14] developed a combined model of AHP and game theory to address interface selection in 5G heterogeneous networks. The AHP is used to establish a hierarchy among the criteria for evaluating network services. By integrating the network hierarchy with game theory, the optimal network selection can be determined. The dynamic part, however, was disregarded because players' preferences and their approaches to how they value their outcomes might vary with each repetition. Furthermore, we may face the assailants with limited rationale under real-world conditions. To overcome this issue, some scholars expanded their investigation from classical game theory to EGT. The EGT was used by many researchers [22-25] to address this shortcoming, especially in the area of network analysis.

It is important to consider the dynamic nature of players in this game, as participants may alter their strategies after each play. Meenakshi and Singh [16] employed the AHP method to determine the weights of network attributes in a heterogeneous wireless network selection problem. They utilized both EGT and bankruptcy game theory to rank the networks. The bankruptcy game was used as a cooperative game strategy to achieve mutual benefit among players, while the evolutionary game focused on examining the evolution of individual actions within a non-cooperative framework.

Using AHP alone, we are able to prioritize the control's criteria and alternatives, but we are unable to account for the dynamic specification. Since the defenders and attackers in the information security context will constantly alter their strategies after each play to obtain the best payoff, the dynamic element is essential in this case. EGT is an effective method in examining the dynamic process of players in a game because different individuals are likely to have possibly different strategies due to the variance that is always present in a population. Although EGT provides a systematic framework for determining players' best options in an information security setting, game theory by itself is unable to produce a payoff matrix. Therefore, the motivation of the study aims to analyse the information security control problem using the hybrid AHP-EGT model. Firstly, decision-makers will determine comparable weights for different control criteria and alternatives through AHP. Secondly, we will form a payoff matrix by applying the results obtained from AHP. Lastly, to determine the evolutionary progression of the information security state, EGT is utilized to examine the dynamic variation in attack-defence strategy-selection likelihood based on replicator dynamics.

The summary of the current literature review that relates to MCDM, ICT, and technology in this paper is shown in Table 1. The network selection problem has been studied in various research contributions by combining the AHP and game theory. However, pertaining to our understanding, there has been no comprehensive research done on the evaluation and selection of information security authentication methods with the AHP-EGT model.

Table 1
Summary table of literature review

Year	Reference Id	Contribution in Problem Type	Application Field	MCDM Technique
2001	[18]	Selection	Technology development	AHP-GT
2011	[20]	Risk assessment	ICT	AHP-GT
2014	[19]	Adaption to environment change	Maintenance	DAHP
2016	[16]	Selection	Networking	Cooperative and non-cooperative GT
2018	[15]	Selection	Networking	Markov differential game
2019	[1]	Risk assessment	Information security	AHP
2019	[17]	Decision making	Networking	EGT
2019	[22]	Defence decision	Network security	EGT
2020	[14]	Selection	Networking	AHP-GT
2020	[2]	Risk assessment	Information security	AHP
2021	[7]	Selection	Supplier development practices	AHP, FAHP
2022	[9]	Selection	Fuel industry	AHP
2022	[10]	Selection	Renewable energy resources	AHP
2022	[21]	Threat assessment	Network security	Qualitive Differential and EGT
2023	[11]	Selection	Mobile phones	AHP-TOPSIS
2023	[12]	Prioritize ranking	Technology	AHP-FMEA
2023	[13]	Risk assessment	Ecosystem	AHP-SOM-CGT
2023	[23]	Decision making	Network security	EGT
2023	[24]	Defence decision	Network security	EGT

In making the decision about information security authentication alternatives, there is not only the selection of multiple options, but there is also the interactive aspect between the defender and attacker that needs to be considered. Therefore, this motivates us to simulate a real-world situation in information security circumstances within a mathematical framework. Additionally, the other motivation of the study is to determine the attributes of information security authentication control. The novelty of the study presented in this paper aims to bridge a notable void in the interactive aspect of defenders and attackers in information security disciplines. We enhance the MCDM's performance by integrating AHP and EGT in selecting the optimal information security strategy. The amalgamation of three distinct information security authentication attributes, namely password, token, and biometric protections, is accomplished through AHP. The AHP is employed to extract distinctive weights from each attribute. Then the utilization of EGT in optimizing the defence-attack process, which involves the amalgamation of authentication attributes scores derived from the AHP, constitutes a pivotal novelty in this study. The findings demonstrate the efficacy of this approach, underscoring the significance of choosing the optimal authentication strategies according to the hybrid model.

This paper is structured into 4 sections. The proposed methodology of the hybrid model is introduced in Section 2. In section 3, we present a result discussion about the hybrid model. Lastly, the conclusion is presented in section 4.

2. Methodology

2.1 Hybrid Model of AHP and EGT

In this study, we propose the utilization of an integrated AHP and EGT model for the purpose of solving information security's problem. The AHP model offers the distinct advantage of establishing the priority of decision criteria and alternatives through the acquisition of input from the expert. Furthermore, the optimal decision is ascertained by employing the EGT. The research's proposed framework, as illustrated in Figure 1, is composed of four stages, which are delineated as follows:

i. In the step of decision-making analysis, firstly, the MCDM problem is established, followed by identifying the criteria and alternatives.
ii. The utilization of the AHP methodology is employed to determine the weight of each criterion, followed by the computation of alternative priorities. We construct a utility function for every player, i.e., the defender and attacker, from the results of alternative priorities.
iii. The interactive condition between the players is examined. Primarily, the utilities of each player's strategies are computed based on the utility functions stipulated in Stage 2. Subsequently, the payoff matrix is developed.
iv. The optimal strategy will be determined based on the equilibrium values of the game, by replicator dynamic method from EGT.

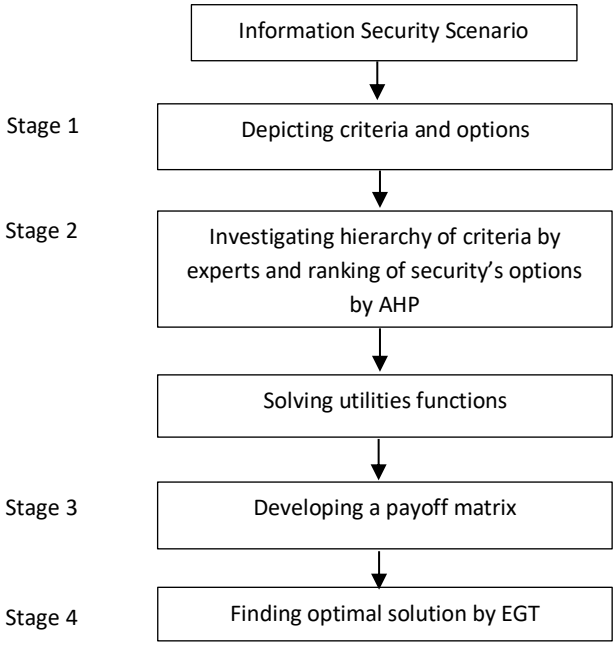

Fig. 1. The composition of the hybrid model

2.2 AHP

In the 1970s, Thomas L. Saaty [26-28] introduced the AHP approach as a means to aid decision-makers in the establishment of priorities and the selection of the most optimal course of action from a multitude of alternatives. Subsequently, the AHP underwent extensive investigation and application in various fields to resolve MCDM problems. When assessing the alternatives of multiple criteria, the AHP method encompasses both qualitative and quantitative elements. It entails the creation of a hierarchy among multiple decision criteria and the subsequent ranking of the different

alternatives. Consequently, AHP determines the optimal alternative based on the multiple input criteria. Fundamentally, the AHP hierarchy consists of three primary levels, with the goal occupying the highest level, the alternatives situated at the lowest level, and the criteria positioned between these two levels [28].

Table 2 presents the proposed hierarchical framework for assessing information security authentication attributes employing the AHP-EGT model. The first level indicates the goal of the investigation, while the second tier entails the four decision criteria. The third tier showcases a total of three decision alternatives.

Table 2
Hierarchical framework of AHP for the ranking of security authentication attributes

Level 1: Goal	Level 2: Decision criteria	Level 3: Decision alternative
Prioritize the ranking of security authentication attributes	1) Applicability 2) Effectiveness 3) Cost 4) Time	1) Biometric-based protection 2) Password protection 3) Token-based protection

After constructing the hierarchy in the assessment of security authentication attributes, the decision-makers compare the criteria based on their relative importance according to the goal, using the value of relative importance as presented in Table 3 [26]. Additionally, it is possible to assign intermediate values such as 2, 4, 6, and 8.

Table 3
AHP fundamental scale of pairwise comparison

Definition of relative importance	Value of relative importance
Two criteria are equally important	1
Criterion *a* is weakly more important than criterion *b*	3
Criterion *a* is strongly more important than criterion *b*	5
Criterion *a* is very strongly more important than criterion *b*	7
Criterion *a* is absolutely more important than criterion *b*	9

In our information security context, there are a total of six pairs of criteria that will be compared: applicability (A) and effectiveness (E), applicability (A) and cost (C), applicability (A) and time (T), effectiveness (E) and cost (C), effectiveness (E) and time (T), cost (C) and time (T). The outcomes derived from this valuation process will elucidate the ranking of each criterion concerning the others, as presented in Table 4.

Table 4
Pairwise comparison matrix of criteria

	A	E	C	T
A	1	0.5	0.3333	2
E	2	1	2	3
C	3	0.5	1	2
T	0.5	0.3333	0.5	1

The eigenvector that has been normalized for Table 4 serves as a representation of the relative weights assigned to each criterion. The following step is to perform pairwise comparisons of the existing alternatives: Token-based (TB), Biometric-based (BB), and Password-based (PB) protections, based on multiple criteria. The comparison matrices of the security authentication alternative for the criteria of applicability, effectiveness, cost, and time are presented in Tables 5 to Table 8 respectively.

Table 5
Pairwise comparison matrix of alternative for applicability

	TB	BB	PB
TB	1	3	0.2
BB	0.3333	1	0.1429
PB	5	7	1

Table 6
Pairwise comparison matrix of alternative for effectiveness

	TB	BB	PB
TB	1	0.5	3
BB	2	1	3
PB	0.3333	0.3333	1

Table 7
Pairwise comparison matrix of alternative for cost

	TB	BB	PB
TB	1	0.5	3
BB	2	1	3
PB	0.3333	0.3333	1

Table 8
Pairwise comparison matrix of alternative for time

	TB	BB	PB
TB	1	2	0.2
BB	0.5	1	0.1667
PB	5	6	1

Subsequently, we calculate the normalized eigenvectors to obtain the relative importance of each alternative. The alternatives are prioritized, to obtain the weights of the alternatives.

Lastly, using the consistency ratio (*CR*) Eq. (1) to assess the consistency of the pairwise matrix. The decision-maker needs to reassess the relative importance of the elements if the *CR* is more than 0.10 [2,27,29].

$$CR = \frac{CI}{RI} \tag{1}$$

where *RI* represent the random index and CI is the consistency index as shown in Eq. (2) [26].

$$CI = \frac{\lambda_{max} - n}{n-1} \tag{2}$$

where λ_{max} denotes the principal eigenvalue and *n* is the size of the matrix.

2.3 EGT

Each player's objective in an evolutionary game with a set of offensive and defensive strategies is to maximize profit during the game's progression. Based on the outcomes of past games, players

who select unsatisfactory strategies typically select better ones. Until every player in the game chooses the optimal course of action, this procedure is repeated. To be more precise, the repetitive procedure is stopped when an equilibrium state is attained. Players no longer unilaterally alter their plans at this moment [30]. Evolutionary equilibrium describes the state of equilibrium at this point.

Assuming that the attacker and the defender are the two players in an information security game. We define $B = \{\beta_1, \beta_2, \beta_3, \cdots \beta_L\}$ as the set of defender's strategies and $K = \{\alpha_1, \alpha_2, \alpha_3, \cdots \alpha_L\}$ as the set of attacker's strategies. To identify the optimal strategy, we determine the defence efficiency of control σ_i against an attack τ_j by $y(\sigma_i, \tau_j) = \sum_{i=1}^{L} v_i A_i$, where v_i denotes the *i*th attribute's value, A_i is the *i*th attribute's weight from the normalized matrix and *L* is the total number of alternatives. This defence efficiency shows how effective the defender's strategy (β) is against the attacker's (α) strategy. If $y(\sigma_i, \tau_j) = 0$ indicates the defence strategy is ineffective, while $y(\sigma_i, \tau_j) = 1$ indicates the attacker's strategy can be obstructed. Defence efficiency has a finite value that ranges from zero to one, or $0 \leq y(\sigma_i, \tau_j) \leq 1$. Second, using the formula $u_{\beta_i,\alpha_i} = U(y_i, c_i)$, where c_i is the *i*th strategy's cost, one can determine the utilities of each player. In line with Yang *et al*., [31], the cost of defence, or c_i, comprises manpower, money, time, and resources like software and hardware tools. In the next step, each player's utility function is used to build a payoff matrix, $M_{L\times L}$, as illustrated in Eq. (3).

$$M_{L\times L} = \begin{bmatrix} u_{\beta_1,\alpha_1} & u_{\beta_1,\alpha_2} & \cdots & u_{\beta_1,\alpha_L} \\ u_{\beta_2,\alpha_1} & u_{\beta_2,\alpha_2} & \cdots & u_{\beta_2,\alpha_L} \\ \vdots & \vdots & \cdots & \vdots \\ u_{\beta_L,\alpha_1} & u_{\beta_L,\alpha_2} & \cdots & u_{\beta_L,\alpha_L} \end{bmatrix} \quad (3)$$

Next, we determine the game's participants' utilities [20]. The security leader's utility is Eq. (4),

$$U_{\beta_i} = \sum_{i=1}^{m} \sum_{j=1}^{n} \left[g_e y(\sigma_i, \tau_j) - (g_c c_i) \right] \quad (4)$$

and the attacker's utility is Eq. (5).

$$U_{\alpha_i} = \sum_{i=1}^{m} \sum_{j=1}^{n} \left[g_e \left(1 - y(\sigma_i, \tau_j) \right) - (g_c c_j) \right] \quad (5)$$

where
c_i represents the defender's cost,
c_j represents the attacker's cost,
g_e represents the weights of inducements,
g_c represents the weights of cost,
m represents the number of controls, and
n represents the number of attacks.
AHP's pairwise comparison method yields the values of g_e and g [20].

Assumed to be the odds of implementing strategy *i* in attack and defence are x_{β_i} and x_{α_i}. Next step is to apply Eq. (6) and Eq. (7) to calculate the fitness of the attacker's and security leader's strategies, respectively.

$$f_{\alpha_{i,j}} = \sum_{i=1}^{m} \sum_{j=1}^{n} (U_{\alpha_i} x_{\alpha_i}) \quad (6)$$

$$f_{\beta_{i,j}} = \sum_{i=1}^{m} \sum_{j=1}^{n} \left(U_{\beta_i} x_{\beta_i} \right) \quad (7)$$

Using Eq. (8) and Eq. (9), we proceed with determining the average fitness of attacker's and security leader's strategies.

$$\bar{f}_{\alpha_{i,j}} = \sum_{i=1}^{m} \sum_{j=1}^{n} \left(x_{\alpha_i} f_{\alpha_{i,j}} \right) \quad (8)$$

$$\bar{f}_{\beta_{i,j}} = \sum_{i=1}^{m} \sum_{j=1}^{n} \left(x_{\beta_i} f_{\beta_{i,j}} \right) \quad (9)$$

Replicator dynamics describes the evolution of frequencies for each proportion of strategies by taking into account the fitness and interdependence of each strategy. The replicator dynamics equation is a differential equation that expresses the frequency of strategy application in a population. Finally, the replicator dynamic formulas for the attacker and security leader, represented by Eq. (10) and Eq. (11), respectively, are applied to identify the best player strategies.

$$\frac{dx_{\alpha_i}}{dt} = x_{\alpha_i} \left(f_{\alpha_{i,j}} - \bar{f}_{\alpha_{i,j}} \right) \quad (10)$$

$$\frac{dx_{\beta_i}}{dt} = x_{\beta_i} \left(f_{\beta_{i,j}} - \bar{f}_{\beta_{i,j}} \right) \quad (11)$$

The replicator dynamic's findings converge at a stable state (ESS), which is reached by repeating the above evolutionary process until a stable equilibrium is reached.

3. Result

We now consider a MCDM problem that concerns information security authentication methods. Based on the second stage of the proposed hybrid model, firstly, experts completed the pairwise comparison judgements of security authentication criteria and alternatives. The result of the pairwise comparison matrix of criteria is shown in Table 4. Following the determination of this decision, the matrix is then normalized, which entails calculating the average weight, as presented in Table 9. The arithmetic mean approach is used to determine the weight.

Table 9
Weighted normalized decision matrix for security authentication criteria

Security authentication criteria	A	E	C	T
A	0.1538	0.2143	0.0870	0.2500
E	0.3077	0.4286	0.5217	0.3750
C	0.4615	0.2143	0.2609	0.2500
T	0.0769	0.1429	0.1304	0.1250

The weights of the security criteria are displayed in Figure 2. Figure 2 summarizes the priority weights of the AHP analysis on the criteria for the selection of security authentication methods. The analysis of the criteria has found that effectiveness, with a weight of 0.4083, is the most important criterion in information security authentication, followed by the second important criterion which is cost, with a weight of 0.2967. Applicability ranks third in terms of importance among the decision criteria, followed by time attributes, which have weights of 0.1763 and 0.1188, respectively.

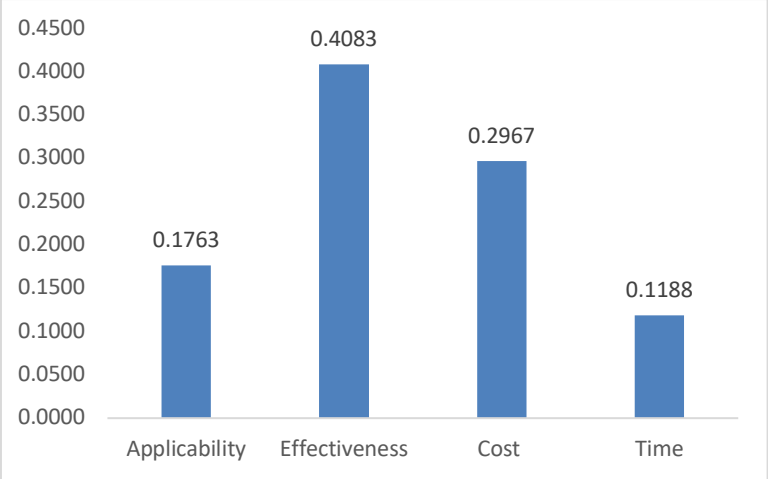

Fig. 2. Weights of the security control criteria

Subsequently, from the pairwise comparison matrices, namely Table 5 to Table 8, we normalized the weights of security authentication alternatives for different criteria, and the results are presented in Table 10 to Table 13.

Table 10
Weighted normalized decision matrix of security authentication alternatives for applicability

Security authentication alternative	TB	BB	PB
TB	0.1579	0.2727	0.1489
BB	0.0526	0.0909	0.1064
PB	0.7895	0.6364	0.7447

Table 11
Weighted normalized decision matrix of security authentication alternatives for effectiveness

Security authentication alternative	TB	BB	PB
TB	0.3000	0.2727	0.4286
BB	0.6000	0.5455	0.4286
PB	0.1000	0.1818	0.1429

Table 12
Weighted normalized decision matrix of security authentication alternatives for cost

Security authentication alternative	TB	BB	PB
TB	0.2381	0.3846	0.2258
BB	0.0476	0.0769	0.0968
PB	0.7143	0.5385	0.6774

Table 13
Weighted normalized decision matrix of security authentication alternatives for time

Security authentication alternative	TB	BB	PB
TB	0.1538	0.2222	0.1463
BB	0.0769	0.1111	0.1220
PB	0.7692	0.6667	0.7317

In consequence of the normalization matrix calculation, we compute the local priority for each alternative. The preference for alternative security authentication based on each selection criterion is shown in Figure 3 to Figure 6.

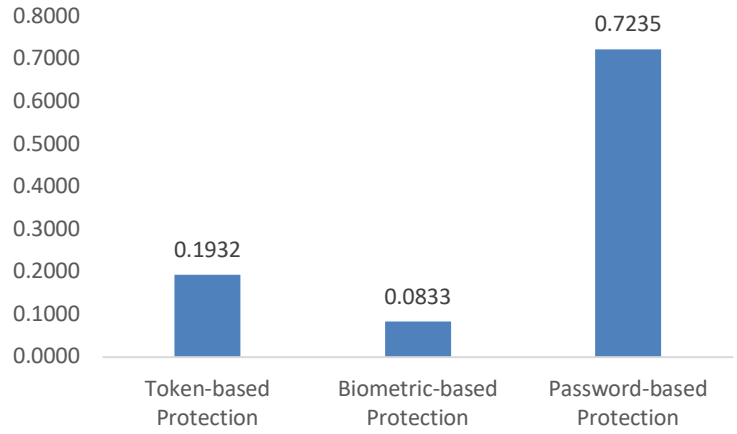

Fig. 3. Weight of security authentication alternative based on applicability

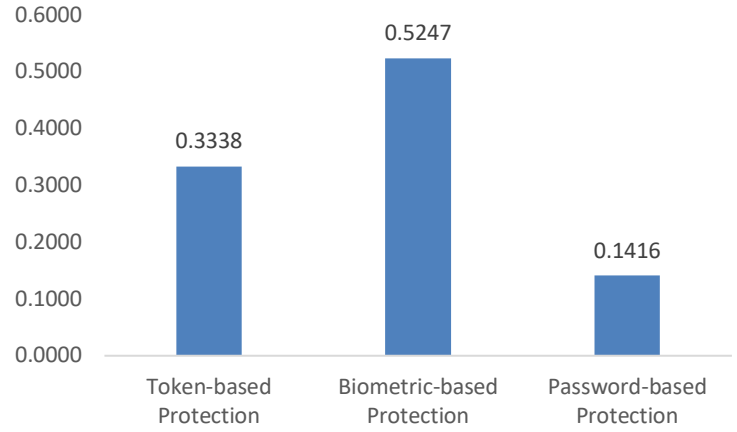

Fig. 4. Weight of security authentication alternative based on effectiveness

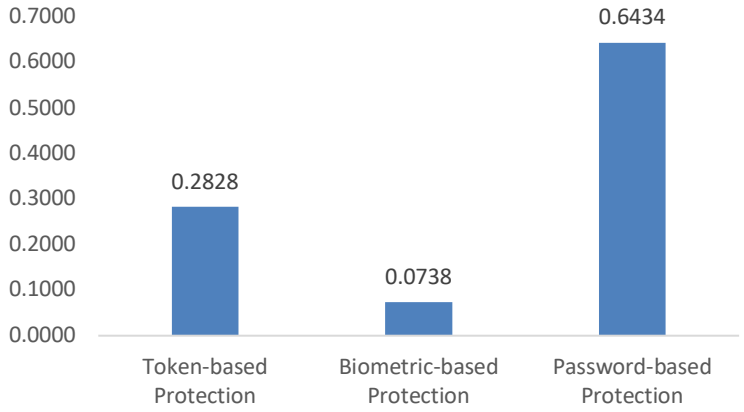

Fig. 5. Weight of security authentication alternative based on cost

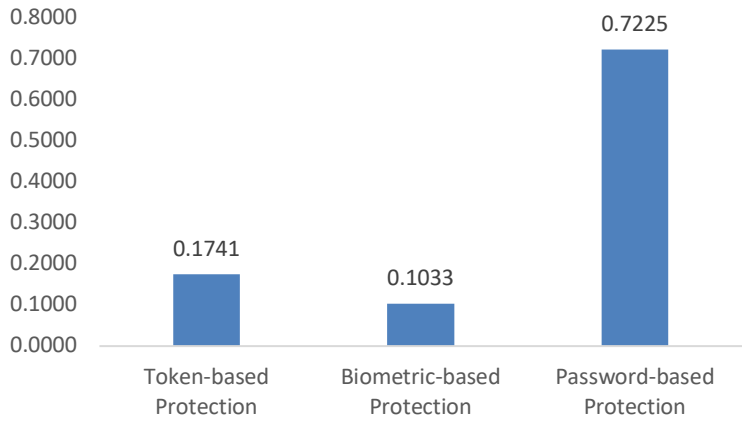

Fig. 6. Weight of security authentication alternative based on time

The overall priority for each alternative is determined after the local priorities, which indicate the preferable alternative in relation to each criterion, have been calculated. Table 14 displays the overall priority matrix that was produced during this process.

Table 14
Overall weight of the alternatives for the criteria

Criterion/ Alternative	A	E	C	T	Overall weight of alternative
Criteria weight	0.1763	0.4083	0.2967	0.1188	
TB	0.1932	0.3338	0.2828	0.1741	0.2749
BB	0.0833	0.5247	0.0738	0.1033	0.2630
PB	0.7235	0.1416	0.6434	0.7225	0.4620

Consequently, we check the consistency of the judgements. Table 15 shows that all the CR of alternatives based on criteria are less than 0.1, indicating the pairwise comparison decisions are consistent.

Table 15
CR of alternatives based on criteria

Criteria	CR
A	0.0560
E	0.0462
C	0.0559
T	0.0257

The following step is to rank the priority of alternatives; the result is tabulated in Table 16. It showcases that password-based protection and token-based protection are the top two security authentication methods, based on applicability, effectiveness, cost, and time.

Table 16
Priority ranking of security authentication alternatives based on criteria

Alternatives	Weights	Ranking
TB	0.2749	2
BB	0.2630	3
PB	0.4620	1

We simulate this information security scenario as a game that involves two players: the security leaders and the attackers. The security leaders have three options for safeguarding the organization's data: password-based, token-based, or biometric-based protection. There are three options available to the attackers: attacking the organization's data system, moderately attacking the organization's data system, or not attacking at all. We assume that the probability distribution of the tactics used by the attackers and security leaders is equal at the initial stage. We applied the equations in Section 2 and simulated with Python. The evolution outcomes for both players to the number of iterations are shown in Figure 7 and Figure 8.

According to Figure 7, there is a 72.56% chance that the security leaders will decide to use password-based protection, 15.43% of the time to use token-based protection, and the lowest chance is using biometric-based protection, with a probability of 8.97%. Password protection is preferred by most organizations, most likely because it saves time and resources. We notice from Figure 8 that the highest likelihood of an attacker's strategy is too select not attacking, with a probability of 45.97%, if the defender applies for security protection, whereas the likelihood of attacking is 35.46%.

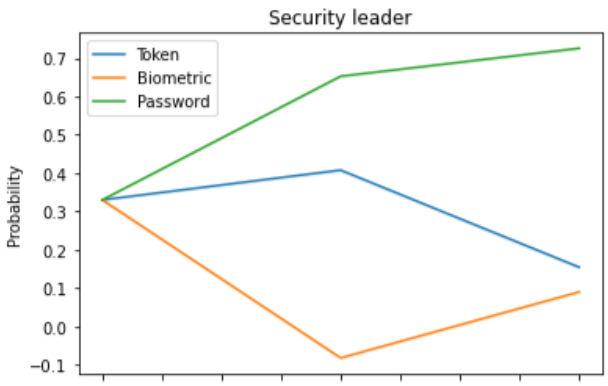

Fig. 7. The evolution of security leader's strategy

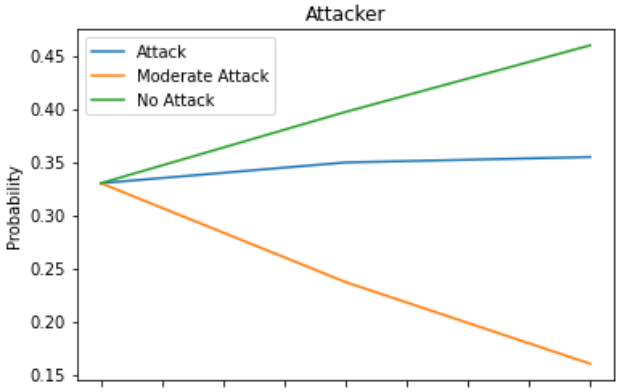

Fig. 8. The evolution of attacker's strategy

4. Conclusion

Information security scenario can be simulated as a MCDM problem as it requires careful examination of several different criteria. We applied the AHP-EGT model to determine which choice criteria should be prioritized when choosing an optimal security control, among token-based, biometric-based, and password-based protections. First, we use the AHP to evaluate the criteria and options that are related to information security. Next, using the utilities functions determined by employing the AHP result, we construct a payoff matrix. The replicator dynamic technique is used to help players in the security game to make the optimal strategies. The findings of this study show that password-based protection is the most preferable protection method, followed by token-based and biometric-based protections. In addition, effectiveness and cost are the top two weighty criteria in determining security control, while applicability and time are ranked as the third and fourth weighty criteria, respectively.

The contribution of this work is the proposal of an MCDM model for information security control assessment and evaluation. The formation of a payoff matrix for two conflicting players is one of the problems in game theory [32]. This drawback can be compensated for by computing each player's payoff within the game model using the AHP's priority assessment of the criteria. However, the interaction perspective between two players is neglected when utilizing the AHP approach alone. As a result, we illustrate and resolve the information security issue in this paper using the hybrid AHP

and EGT model, which will assist the security leader in selecting the best course of action, with the consideration of interactive and dynamic aspects from EGT. We will expand the study in future work to include other information security control characteristic criteria and options. In order to address the scale issue, machine learning methods will be incorporated.

Acknowledgment
This research is supported by the Tunku Abdul Rahman University of Management and Technology, Malaysia.

References

[1] Zaburko, J., and J. Szulżyk-Cieplak. "Information security risk assessment using the AHP method." In *IOP conference series: materials science and engineering*, vol. 710, no. 1, p. 012036. IOP Publishing, 2019. https://doi.org/10.1088/1757-899X/710/1/012036

[2] Kahraman, K. Goztepe C. "A New Approach to Military Decision Making Process: Suggestions from MCDM Point of View."

[3] van der Kleij, Rick, Jan Maarten Schraagen, Beatrice Cadet, and Heather Young. "Developing decision support for cybersecurity threat and incident managers." *Computers & Security* 113 (2022): 102535. https://doi.org/10.1016/j.cose.2021.102535

[4] Ahmad, Atif, Kevin C. Desouza, Sean B. Maynard, Humza Naseer, and Richard L. Baskerville. "How integration of cyber security management and incident response enables organizational learning." *Journal of the Association for Information Science and Technology* 71, no. 8 (2020): 939-953. https://doi.org/10.1002/asi.24311

[5] Naseer, Ayesha, Humza Naseer, Atif Ahmad, Sean B. Maynard, and Adil Masood Siddiqui. "Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis." *International Journal of Information Management* 59 (2021): 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334

[6] Abadi, Satria, Muhamad Hariz Muhamad Adnan, Sri Redjeki, and Citrawati Jatiningrum. "Using Analytical Hierarchy Process for Double Auction to Optimize Financial Performance of Private Higher Education Institutions." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 31, no. 3 (2023): 13-24. https://doi.org/10.37934/araset.31.3.1324

[7] Tukimin, Rahayu, Wan Hasrulnizzam Wan Mahmood, Maimunah Mohd Nordin, Mohd Razali Muhamad, and Numfor Solange Ayuni. "Application of AHP and FAHP algorithm for supplier development evaluation." *Malaysian Journal on Composites Science and Manufacturing* 5, no. 1 (2021): 21-30. https://doi.org/10.37934/mjcsm.5.1.2130

[8] Lee, Pei Fun, Weng Siew Lam, Weng Hoe Lam, and Wein Kei Muck. "Multi-Criteria Decision Analysis on the Preference of Courier Service Providers with Analytic Hierarchy Process Model." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 35, no. 2 (2024): 94-103. https://doi.org/10.37934/araset.35.2.94103

[9] Zaidi, Mohamad Faizal Ahmad, Shafini Mohd Shafie, and Mohd Kamarul Irwan Abdul Rahim. "AHP Analysis on the criteria and sub-criteria for the selection of fuel cell power generation in Malaysia." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 98, no. 2 (2022): 1-14. https://doi.org/10.37934/arfmts.98.2.114

[10] Ilham, Zul. "Multi-criteria decision analysis for evaluation of potential renewable energy resources in Malaysia." *Progress in Energy and Environment* 21 (2022): 8-18. https://doi.org/10.37934/progee.21.1.818

[11] Lam, Weng Siew, Weng Hoe Lam, Kah Fai Liew, Mohd Abidin Bakar, and Chooi Peng Lai. "Evaluation and selection of mobile phones using integrated AHP-TOPSIS model." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 33, no. 2 (2023): 25-39. https://doi.org/10.37934/araset.33.2.2539

[12] Ab Ghani, Ahmad Fuad, Mohd Azhar Shah Rizam, Jeefferie Abd Razak, Mohd Syaiful Rizal Abdul Hamid, Raja Nor Firdaus Kashfi Raja Othman, and Rahifa Ranom. "Analytical Hierarchy Process and Failure Mode and Effect Analysis on HVAC Semi-Hermetic Compressor Maintenance Strategy." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 3 (2023): 256-272. https://doi.org/10.37934/araset.32.3.256272

[13] Zhao, Lefan, Rong Ma, Zhenjing Yang, Kai Ning, Peng Chen, and Jun Wu. "Ecosystem health risk assessment of lakes in the Inner Mongolian Plateau based on the coupled AHP-SOM-CGT model." *Ecological Indicators* 156 (2023): 111168. https://doi.org/10.1016/j.ecolind.2023.111168

[14] Chowdhury, Mostafa Zaman, Md Tashikur Rahman, and Yeong Min Jang. "An analytical hierarchy process combined with game theory for interface selection in 5G heterogeneous networks." *KSII Transactions on Internet and Information Systems (TIIS)* 14, no. 4 (2020): 1817-1836. https://doi.org/10.3837/tiis.2020.04.022

[15] Huang, Shirui, Hengwei Zhang, Jindong Wang, and Jianming Huang. "Markov differential game for network defense decision-making method." *IEEE Access* 6 (2018): 39621-39634. https://doi.org/10.1109/ACCESS.2018.2848242
[16] Singh, N. P. "A comparative study of cooperative and non-cooperative game theory in network selection." In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, pp. 612-617. IEEE, 2016.
[17] Yi, Zhuo, Delong Jiang, Lifeng Cao, and Xuehui Du. "A handover decision algorithm based on evolutionary game theory for space-ground integrated network." In *2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019)*, pp. 143-146. Atlantis Press, 2019. https://doi.org/10.2991/wcnme-19.2019.34
[18] Said, Ilham. "Combine game theory and AHP to choose strategic orientation in technology development-Indonesian case." *Jurnal Teknik Industri: Jurnal Keilmuan dan Aplikasi Teknik Industri* 4, no. 2 (2002): 45-57. https://doi.org/10.9744/jti.4.2.45-57
[19] González-Prida, Vicente, Pablo Viveros, Luis Barberá, and Adolfo Crespo Márquez. "Dynamic analytic hierarchy process: AHP method adapted to a changing environment." *Journal of Manufacturing Technology Management* 25, no. 4 (2014): 457-475. https://doi.org/10.1108/JMTM-03-2013-0030
[20] Rajbhandari, Lisa, and Einar Arthur Snekkenes. "An approach to measure effectiveness of control for risk analysis with game theory." In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pp. 24-29. IEEE, 2011. https://doi.org/10.1109/STAST.2011.6059252
[21] Zhang, Hengwei, Jinglei Tan, Xiaohu Liu, Shirui Huang, Hao Hu, and Yuchen Zhang. "Cybersecurity threat assessment integrating qualitative differential and evolutionary games." *IEEE Transactions on Network and Service Management* 19, no. 3 (2022): 3425-3437. https://doi.org/10.1109/TNSM.2022.3166348
[22] Gu, Ziqing, Yunlong An, Fangyuan Tan, Yang Li, and Sifa Zheng. "A game theory approach to attack-defense strategy for perception of connected vehicles." In *2019 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 2587-2594. IEEE, 2019. https://doi.org/10.1109/SSCI44817.2019.9002791
[23] Jin, Hui, Senlei Zhang, Bin Zhang, Shuqin Dong, Xiaohu Liu, Hengwei Zhang, and Jinglei Tan. "Evolutionary game decision-making method for network attack and defense based on regret minimization algorithm." *Journal of King Saud University-Computer and Information Sciences* 35, no. 3 (2023): 292-302. https://doi.org/10.1016/j.jksuci.2023.01.018
[24] Li, Shuai, Ting Wang, Ji Ma, and Weibo Zhao. "A three-party attack-defense deception game model based on evolutionary." In *2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, pp. 51-56. IEEE, 2023. https://doi.org/10.1109/ICCECE58074.2023.10135374
[25] Sui, Nannan, Dongmei Zhang, Wei Zhong, and Cong Wang. "Network selection for heterogeneous wireless networks based on multiple attribute decision making and Evolutionary Game Theory." In *2016 25th Wireless and Optical Communication Conference (WOCC)*, pp. 1-5. IEEE, 2016.
[26] Saaty, Thomas L. "Decision making with the analytic hierarchy process." *International journal of services sciences* 1, no. 1 (2008): 83-98. https://doi.org/10.1504/IJSSCI.2008.017590
[27] Saaty, Thomas L. "The analytical hierarchy process, planning, priority." *Resource allocation. RWS publications, USA* (1980).
[28] Saaty, Thomas L. "How to make a decision: the analytic hierarchy process." *European journal of operational research* 48, no. 1 (1990): 9-26. https://doi.org/10.1016/0377-2217(90)90057-I
[29] Rabia, Mohamed Amine Ben, and Adil Bellabdaoui. "Collaborative intuitionistic fuzzy-AHP to evaluate simulation-based analytics for freight transport." *Expert Systems with Applications* 225 (2023): 120116. https://doi.org/10.1016/j.eswa.2023.120116
[30] Hengwei, Zhang, Wang Jindong, Yu Dingkun, Han Jihong, and Wang Na. "Defense strategy selection based on signaling game." In *Third International Conference on Cyberspace Technology (CCT 2015)*, pp. 1-7. IET, 2015. https://doi.org/10.1049/cp.2015.0806
[31] Yang, Yu, Bichen Che, Yang Zeng, Yang Cheng, and Chenyang Li. "MAIAD: a multistage asymmetric information attack and defense model based on evolutionary game theory." *Symmetry* 11, no. 2 (2019): 215. https://doi.org/10.3390/sym11020215
[32] Aliahmadi, Alireza, Seyed Jafar Sadjadi, and Meisam Jafari-Eskandari. "Design a new intelligence expert decision making using game theory and fuzzy AHP to risk management in design, construction, and operation of tunnel projects (case studies: Resalat tunnel)." *The International Journal of Advanced Manufacturing Technology* 53 (2011): 789-798. https://doi.org/10.1007/s00170-010-2852-7