Game theory approach in decision-making to invest in modules

Amir-Hossein Yadollahi
Salman Goli Bidgoli
Department of Computer Engineering, Faculty of Electrical and Computer Engineering, Kashan University, Kashan, Iran.

Abstract

Cloud computing involves a variety of technologies, including networking and virtualization, to meet the new needs of users, but is vulnerable to many security threats. To provide the necessary level of security in cloud computing, decision-making on the type and number of security modules used by cloud service users and then paying the relevant fees is of particular importance. Game theory, with the ability to model the behaviour of users and attackers of a supervisor and analyze the possible strategy and profitability of each, can suggest a suitable strategy for investing in the security modules of a virtual machine. In our previous work, we used game theory to analyze the decision to invest in one of the security modules for each of the actors. The purpose of this article is to study the effect of the three parameters "different investment costs", "probability of success of the attack on the user" and "probability of success of the attack on the supervisor" and to make an appropriate decision in this situation. Based on the simulation results, it can be said that given the different values of the probability of a successful attack on a supervisor, a predetermined investment can lead to a proper Nash equilibrium. In general, at low costs or in the case of increasing the cost of investing in security, the user tends to constantly change his strategy and provide the desired security conditions. The results also show that as the probability of a successful attack on a user not investing in security increases, so does the security investment cost.

Keywords: *Cloud Computing, Investing in Security, Game Theory, Repeated Game.*

Introduction

Cloud computing has become an integral part of information technology[1]. This technology has been designed to provide services such as data storage, data analysis, and remote access[2]. Cloud computing services are provided by data centres located in different parts of the world [3]. Therefore, this issue is the main cause of new threats that are emerging day by day. Security is the most important aspect of cloud computing and data privacy. It can be related to both hardware and software [4]. Cloud computing has recently attracted a lot of attention due to its economics and quality of services. In the last decade, cloud services have inevitably become involved in daily life, businesses, and people through products and services [5]. Given such astonishing growth, considering security challenges is very important and costly, and requires decisions about the extent of implementation and investment. This is at a time when security considerations are often overlooked by customers due to the performance and relative reliability of cloud services [6]. Therefore, despite the numerous benefits of the cloud computing model for businesses or individuals, security problems are still declared the top cloud challenge in 2020 [5].

When a direct attack on a machine is carried out on a supervisor, it may indirectly spread to another user's virtual machine. This phenomenon does not exist in conventional traditional networks, but in which an attacker must use a multi-step method to indirectly attack multiple users. Thus, the interdependence of security between users of a supervisor has posed a serious challenge to cloud service providers [7]. An important issue in cloud computing is how to create and connect virtual machine instances with security modules. The way virtual machines are assigned to users by cloud service providers has a direct impact on the security of the user and other users. Our goal in this article is to use the knowledge gained from this modeling to help cloud computing providers make decisions about spending on virtual machine security modules. Most of the studies conducted in the field of securing cloud services rely on expensive hardware approaches. In some studies, in this field, the proposed models intelligently select the most suitable module among all possible modules for attack detection. Choosing a specific detection module instead of using all of them in parallel not only leads to lower energy consumption but also increases the overall efficiency of the defence system. In methods based on game theory, based on the obtained Nash equilibrium values, the attack is distinguished from normal requests, and the severity of the attack and its origin is determined. These results can help in choosing the right module to create security. In this study, assuming the existence of complete virtualization, using game theory, a suitable solution for making decisions about investing in security modules is presented.

The main purpose of this research is to help the appropriate decision of cloud computing providers on virtual machine security modules with optimal investment using game theory. Game theory is a mathematical model that deals with the interactions between different players by analyzing strategies and choices. Game theory has also been extended to computer science due to its high adaptability in various sciences [8]. In this article, assuming the existence of complete virtualization, the game theory has been used in the field of investment decisions in security modules. One of the most important differences between this study with other similar research [7]–[9] is the use of the repeated game to analyze and determine the appropriate Nash equilibrium under different scenarios. The difference between the present article and the previous study published by the authors [10], is the investigation of the effect of the probability of a successful attack on a supervisor, "different investment costs" and "probability of success of the attack on the user". Section 2 describes the system model and the basic model in cloud computing. Section 3 explains the details of the game architecture used as a repeated game model and section 4 describes the results of the model and its analysis. Finally, Section 5 concludes and examines the impact of repeated play on virtual machines.

Currently, cloud computing is very important due to its wide and comprehensive applications. The significant expansion and acceptability of cloud computing, along with other advantages, creates new challenges of virtual machine security [11]. Recent surveys show that security and efficiency are the two main priorities for using cloud services [12]. Security in virtualization acts as a barrier to network access .This technology provides dedicated security services in the cloud along with a firewall .Companies and service providers can invest in creating this security environment and provide dedicated resources in a cloud structure to service subscribers. As a real-world example to understand the proposed approach, if an attacker successfully gains access

to a virtual machine by exploiting a vulnerability in one of the applications running on that virtual machine, it can attack other applications that are placed on different virtual machines in the same network. If the virtual machines are running on the same physical host as the physical machine being attacked, it may be difficult to detect such a network attack. Therefore, each of the applications should invest in security to prevent the attacker's attack, and a lack of investment can increase the possibility of the attacker's attack. The conditions, time, and amount of investment in security according to the conditions of other applications are among the things that can be examined in the proposed approach to make the right decision. The results of the analysis and implementation help the cloud service user to adopt the most suitable strategy and achieve the best result in terms of cost and security by considering the cost of security services, the probability of attack, and the resulting cost.

In this article, the basics of the system and the basic model are discussed in section 2 and the repetitive game model is explained in section 3. The results of this research are analyzed in section 4 and finally, the conclusions of this research are presented in section 5.

2. Description of the system and basic model

For system modelling, it is assumed that in a public cloud computing infrastructure, a supervisor is running and there are n users, each of whom is running a virtual machine on that. In this system, the cloud user manages the virtual machines by their interface. It is also assumed that the cloud user will act in good faith. Therefore, in this article, only one target user is examined. In the game model presented in [9], there are four players, which include an attacker and three users. These four players are playing through two supervisors. The conditions of the game are such that each player can calculate his profit in each selection and choose the best decision for himself. During these successive selections, each player finally reaches the equilibrium in which he has earned the most profit. In this game, the attacker has three strategies to attack. The first strategy is to attack user 1 (A_1), the second strategy is to attack user 2 (A_2) and the third strategy is to attack user 3 (A_3). One of the rules of the game is that the attacker attacks only one user at a time. Possible choices for any user include investing or not investing (using one of the default security modules with paying its cost) in security. For ease of reviewing the relationships and results presented in this paper, the symbols and parameters used in Table 1 are presented.

Table 1: Introduction of the parameters used in this article

Description	Symbol	Description	Symbol
The probability of a successful attack on a supervisor	$\boldsymbol{\pi}$	security investment	$\boldsymbol{I(H_2)}$
The security investment cost in	$\boldsymbol{e}$	Lack of investment in security	$\boldsymbol{N(H_1)}$
The overall benefit of a cloud service	$\boldsymbol{R}$	i'th user's cost in decision making	$\boldsymbol{L_i}$
Attacking user i (strategyA_i) and not investing the desired user in the security	$\boldsymbol{(A_i, N)}$	The probability of success of an attack on a user who has invested in security	$\boldsymbol{q_I}$
Attacking user i (strategy A_i) and investing the user in the security	$\boldsymbol{(A_i, I)}$	The probability of success of an attack on a user who has not invested in security	$\boldsymbol{q_N}$

Suppose User 2 is looking to conclude whether to invest in a security module or not. This decision is made in situations where user 1 decides not to invest (not paying the cost and using security modules) and user 3 decides to invest in security. In this situation, the attacker has three strategies in front of A_1, A_2, and A_3. Table 2 shows the profits and losses of each player and attacker in different decisions. According to the results of the study [9], it has been determined that always (N, A_3) is a possible Nash equilibrium for this game.

Table 2: Game model in the base state [9]

		User 2	
		$N(H_1)$	$I(H_2)$
Attacker	A_1	$R - q_N \pi L_2$ & $q_N L_1 + q_N \pi L_2$	$R - e$ & $q_N L_1$
	A_2	$q_N L_2 + q_N \pi L_1$ & $R - q_N L_2$	$q_I L_2 + q_I \pi L_3$ & $R - e - q_I L_2$
	A_3	R & $q_I L_3$	$R - e - q_I \pi L_2$ & $q_I L_3 + q_I \pi L_2$

3. Repeated game model

A repeated game is an extensive form of the game that consists of many repetitions of some basic games. Repeated games bring to mind the idea that the player must consider his current impact on the performance of other players. The user may select and use a cloud service for a long time. Therefore, this service may be attacked many times and in different ways. This indicates that the user must constantly change their strategy to optimize the cost of security. This highlights the need to examine the repeated game in security investment. In the following, two different modes for game design are examined, during which each of the two desired strategies can be Nash equilibrium.

A: Suppose that (A_3, I) is a Nash equilibrium, the game designer has considered the following strategy for the repeated game:

In the first step, the attacker attacks user 3 and does not attack user 2 until he has used security mechanisms (Equation 1). But if user 2 violates and decides not to use one of the security mechanisms embedded in the current period, the attacker attacks him (user 2) (equation 2). As a result, the user decides to invest in security. In this case, the temptation of user 2 to violate the game from (A_3, I) to (A_3, N) will be equal to Equation 3.

$$(\mathrm{A_3}, \mathrm{I}) = (\mathrm{q_I L_3} + \mathrm{q_I}\pi\mathrm{L_2}\,, \mathrm{R\text{-}e\text{-}q_I}\pi\mathrm{L_2}) \text{ forever} \quad (1)$$

$$(A_2, I) = (q_I L_2 + q_I \pi L_3\,, R - e - q_I L_2)\ forever \quad (2)$$

$$R - (R - e - q_I \pi L_2) = e + q_I \pi L_2 \quad (3)$$

If δ shows the probability of repetition in the repeated game, to calculate the probability of repetition we can write:

$$e + q_I \pi L_2 < \delta(u(A_3, I) forever - u(A_2, I) forever) \quad (4)$$

Next, by inserting the values of u from Table 2 and then by simplifying it, Equation 5 is obtained.

$$\delta > \frac{e + q_I \pi L_2}{e + q_I L_2} \quad (5)$$

B: Suppose that (A_3, N) is a Nash equilibrium, the game designer has considered the following strategy for the repeated game:

In the first repetition, User 2 doesn't invest in security, and the attacker does not change his strategy until he attacks User 3 (Equation 6). But if the attacker violates, user 2 invests in security (Equation 7). In this case, the attacker's willingness to a violation in the game from (A_3, N) to (A_2, N) will be equal to Equation 8.

$$(A_3, N) = (q_I L_3\ , R)\ forever \quad (6)$$
$$(A_2, I) = (q_I L_2 + q_I \pi L_3\ , R - e - q_I L_2) forever \quad (7)$$
$$q_N L_2 + q_N \pi L_1 - q_I L_3 \quad (8)$$

Therefore, to calculate the probability of repetition, we have:

$$q_N L_2 + q_N \pi L_1 - q_I L_3 < \ \delta(u(A_3, N) forever - u(A_2, I) forever) \quad (9)$$

Following the same process performed for Equation 4, Equation 10 can be obtained by inserting the values u from Table 2 and simplifying it.

$$\delta > \frac{q_N L_2 + q_N \pi L_1 - q_I L_3}{q_N L_2 + q_N \pi L_1 - q_I \pi L_3 - q_I L_2} \quad (10)$$

4- Results and analysis

In Section 3, scenarios and penalties for violation of Nash equilibriums were studied. In case "A", where the objective is to (A_3, I) be Nash equilibrium. It can be said with the probability of $\alpha = \frac{e + q_I \pi L_2}{e + q_I L_2}$ the state (A_3, I) is Nash equilibrium. Figure 1 shows the probability of game repetition for different values of L_2 $(1 < L_2 < 100)$. As can be seen, given the varying amounts of probability of a successful attack on a supervisor (π), predetermined investment or non-investment strategies can lead to an appropriate Nash equilibrium. At small π values, which means the reduction of the probability of a successful attack on a supervisor, the higher the cost (L_2), the less likely the game will be repeated and the user will continue the game with the same policies. In general, at low costs, the probability of the game repetition increases, and the user tends to constantly change his strategy and provide the desired security conditions. On the other hand, as the percentage of the security investment cost increases, the probability of repeating the game also increases. Therefore, compared to the study [10], these cases show how many parameters can be effective in changing the strategy by the user and increase the desire to repeat the game to change the strategy by more than 90%. These parameters are "investment costs", "probability of success of the attack on the supervisor" and "probability of success of the attack on the user".

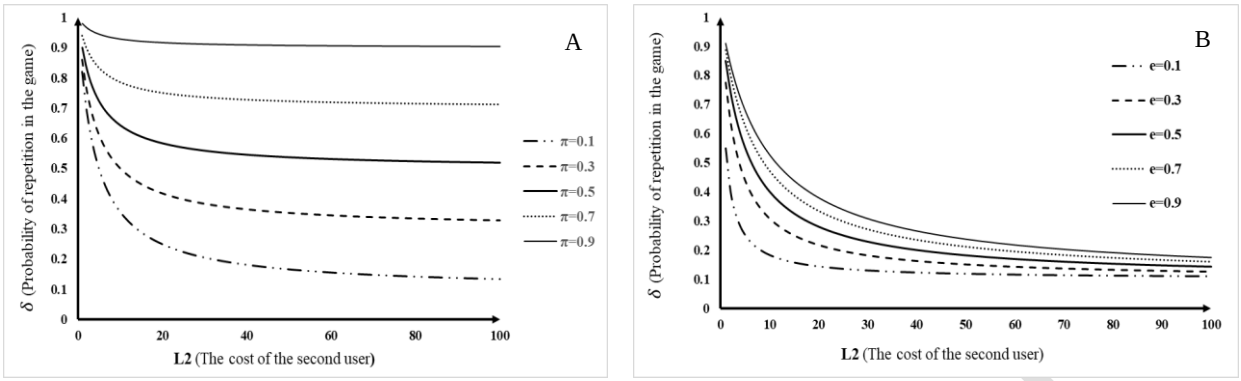

Figure 1: Probability changes of δ according to the potential penalty range of user 2 (A: The different probability of a successful attack on a supervisor and B: the percentage increase in security investment cost)

For example, for case A, to check the repeated game, we will consider the problem assuming L2=20. According to the parameters of this example, the profit and loss table related to the first stage of this game will be summarized in Table 3. As can be seen, in the first stage, the Nash equilibrium in this state is (A3, N).

Table 3: Game model and profit and loss table for L2=20

		User 2	
		$N(H_1)$	$I(H_2)$
Attacker	A_1	(1.2 , 0.7)	(0.4 , 1.1)
	A_2	(8.04 , -6.5)	(3 , -0.9)
	A_3	(10 , 1.5)	(10.2 , 0.9)

Suppose the desired scenario in this repeated game is the same Nash equilibrium (A3,N) for different values of L2. Therefore, the attacker attacks user 3 until user 2 invests in security, and the penalty for playing N by user 2 is that the attacker attacks user 2 himself until the end of the game. According to the table, in this case, the temptation of user 2 for a violation in the game is 1.5-0.9=0.6. Therefore, the probability of repeating the game to check this Nash equilibrium is calculated with the help of equation 5. Therefore, with the value of α=1/4, or in other words, with a probability of 25%, it can be said that the game (A3, I) is a Nash equilibrium with the assumption of L2=20.

In case "B", where the goal is to state (A_3, N) be a Nash equilibrium of, with the probability of $\alpha = \frac{q_N L_2 + q_N \pi L_1 - q_I L_3}{q_N L_2 + q_N \pi L_1 - q_I \pi L_3 - q_I L_2}$ percent it can be said that the game (A_3, N) is Nash equilibrium. Figure 2 shows the δ graph for different values of L_2 (given that $L_1 < L_2 < L_3$ hence $1 < L_2 < 100$) for the repeated game in this state. In the explanation of the presented diagram, it can be said that according to the relations presented in the mixed Nash equilibrium section and considering the different probability of a successful attack on a supervisor (π), the values of L_2 and π can be effective in the Nash equilibrium of (A_3, N) (Horizontal section of Figure A) or the mixed Nash equilibrium governing the game (curved section of Figure A). Figure B also shows the effect of δ on the different probability of success of an attack on a user who did not invest in

security (q_N). The results show that as the probability of success of an attack on a user who has not invested in security increases, the value of L2 investment cost to intend to repeat the game must increase so that the user tends to change his strategy and supply his suitable security conditions. Figure 2 (A) also shows that as the value of π increases, the probability of choosing a mixed strategy decreases and the curved part of the graph disappears. Therefore, the probability of repetition of the game in unit strategies increases. These changes could not be examined in the study [10] due to the lack of study of the effect of the parameter of "probability of a successful attack on the supervisor".

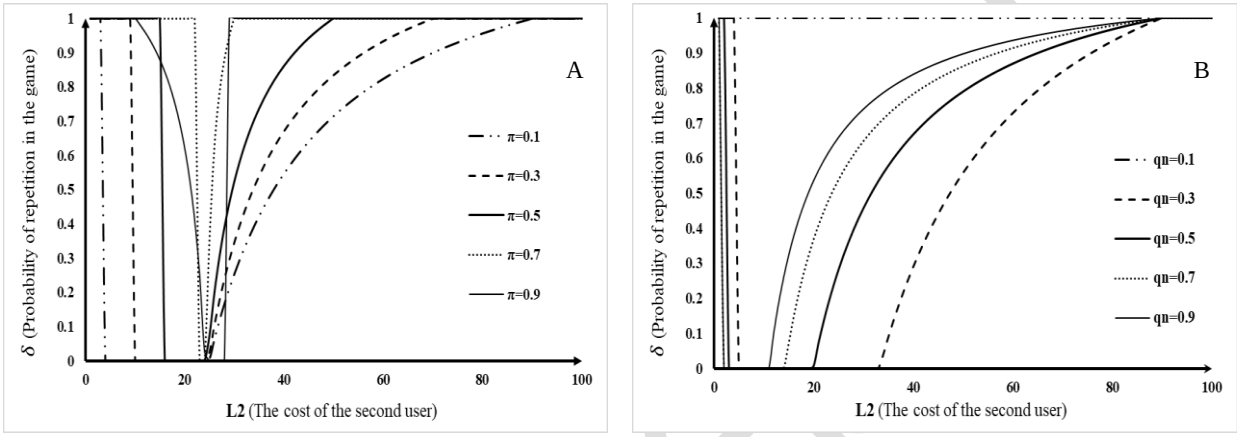

Figure 2: Probability changes δ according to the potential penalty range of user 2 (A: according to the different probability of a successful attack on a supervisor and B: according to the different probability of success of an attack on a user who did not invest in security)

The values of α and δ determine the difference in the cost of investing in security. This means that the difference in the investment cost is related to continuing the game with the desired Nash equilibrium or violating it and accepting the penalty cost (according to the percentage of α and δ or the tendency to repeat the game with the Nash equilibrium under consideration). This means that if the percentage of willingness to pay is high for the said player who did not invest in security, he no longer has the desire to invest in security. But if this percentage is low, it increases the risk of not investing in security. The player is forced to accept the penalty (paying the cost of investing in security) and prefers to invest in security.

In the continuation of the statistical tests of the hypothesis Cronbach's alpha coefficient was calculated to determine the significance of the obtained results, the results of which are shown in Table 4. In a hypothesis test, the probability value (p-value) is equal to the lowest value of the significance level or the probability of the first type of error, which causes the null hypothesis to be rejected. One of the methods of measuring the internal consistency of the results is to calculate Cronbach's alpha coefficient. Cronbach's alpha coefficient should be higher than 0.7. The results of the hypothesis test and Cronbach's alpha coefficient greater than 0.95 show that the difference in the values shown in Figures 1 and 2 is statistically significant.

Table 4: Results of calculations and statistical tests

statistical analysis	π values	e values

	0.1	0.5	0.9	Total	0.1	0.5	0.9	Total
Average	0.213	0.562	0.912	0.562	0.137	0.232	0.297	0.225
Minimum	0.134	0.519	0.903	0.134	0.108	0.142	0.174	0.108
Maximum	0.821	0.9	0.98	0.98	0.55	0.85	0.91	0.91
Variance	0.014	0.004	0.00018	0.067	0.0037	0.0051	0.0012	0.0316
Hypothesis test P_Value	1				1			
Cronbach's Alpha	0.957				0.968			

5. Conclusion

The unique features of a cloud computing structure and complete virtualization can provide new grounds for attack. One of the issues addressed in this article is the issue of new user login, which may pose security threats to other users if the decision of security non-investment is made (non-payment of cost and use of one of the security modules). The amount of "investment cost on security (e)" plays a key role in determining the Nash equilibrium, and as the percentage increase in security investment cost increases, the user tends to constantly change his strategy and provide the desired security conditions. On the other hand, according to the relationships presented in the mixed Nash equilibrium section and considering the different probabilities of a successful attack on a supervisor, the values of L_2 and π can be very effective in the Nash equilibrium of only one strategy or the mixed Nash equilibrium governing the game. Therefore, for users, knowing the values of e and π can be very important in decision-making on whether the proposed cloud computing security modules are a useful tool to provide adequate security at a low cost. As a future task, different costs of attacks and their effects can be considered differently, and user strategies for selecting one of the security modules can also be fuzzily modeled to provide more detailed results of the interaction between security policies and costs.

References

[1] T. P. Shabeera, S. D. M. Kumar, S. M. Salam, and K. M. Krishnan, "Engineering Science and Technology , an International Journal Optimizing VM allocation and data placement for data-intensive applications in cloud using ACO metaheuristic algorithm," *Eng. Sci. Technol. an Int. J.*, 2016, doi: 10.1016/j.jestch.2016.11.006.

[2] M. K. Sasubilli and V. R, "Cloud Computing Security Challenges , Threats and Vulnerabilities," Int. Conf. Inven. Comput. Technol., pp. 476–480, doi**:** 10.1109/ICICT50816.2021.9358709.2021.

[3] B. Alouffi, M. Hasnain, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security : Threats and Mitigation Strategies," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3073203.

[4] S. C. Satapathy and V. Bhateja, *Lecture Notes in Networks and Systems, Communication Software and Networks*, Janusz Kac. Proceedings of INDIA: Springer, doi: 10.1007/978-981-15-5397-4.2019.

[5] S. B. Ousmane, B. C. S. Mbacke, and N. Ibrahima, "A game theoretic approach for virtual machine allocation security in cloud computing," in *ACM International Conference Proceeding Series*, 2019, vol. Part F1481, doi: 10.1145/3320326.3320379.

[6] K. Prabhakar, K. Dutta, R. Jain, M. Sharma, and S. K. Khatri, "Securing Virtual Machines on Cloud through Game Theory Approach," *Proc. - 2019 Amity Int. Conf. Artif. Intell. AICAI 2019*, pp. 859–863, 2019, doi: 10.1109/AICAI.2019.8701229.

[7] C. S. Lee, "Multi-objective game-theory models for conflict analysis in reservoir watershed management," *Chemosphere*, vol. 87, no. 6, pp. 608–613, 2012, doi: 10.1016/j.chemosphere.2012.01.014.

[8] V. Kakkad, H. Shah, R. Patel, and N. Doshi, "ScienceDirect ScienceDirect A Comparative study of applications of Game Theory in Cyber A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing . Security and Cloud Computing .," *Procedia Comput. Sci.*, vol. 155, no. 2018, pp. 680–685, 2019, doi: 10.1016/j.procs.2019.08.097.

[9] L. Kwiat, C. A. Kamhoua, and K. A. Kwiat, "Risks and Bene fi ts : Game-Theoretical Analysis and Algorithm for Virtual Machine Security Management in the Cloud," *IEEE Comput. Soc.*, pp. 49–80, 2018.

[10] A. H. Yadollahi, J. Salimi Sartaghti, and S. Goli Bidgoli, "Modeling the Security of Virtual Machines in the Cloud using Repetitive Game Theory," *Soft Comput. J.*, 2021, doi: 10.22052/SCJ.2021.242842.0.

[11] S. Razzaghzadeh, P. Norouzi Kivi, and B. Panahi "A hybrid algorithm based on Gossip architecture using SVM for task scheduling in cloud computing," Soft Comput. J., 2021, *9*(2), 84-93. doi: 10.22052/scj.2021.242822.0.

[12] E. Asadollahi, S. A. Asghari, "Prediction of Appropriate Number of Virtual Machines based on Time Series and Artificial Methods via Virtual machines Clustering," Soft Comput. J., 2021, *6*(1), 66-77.