Game Theoretic Approaches to Mitigate Cloud Security Risks: An Initial Insight

Abdelkarim Ait Temghart[1(✉)], M'hamed Outanoute[1], and Mbarek Marwan[2]

[1] TIAD Laboratory, FST, Sultan Moulay Slimane University, Beni Mellal, Morocco
[2] Smart Systems Laboratory, ENSIAS, Mohammed V, Rabat, Morocco

Abstract. Cloud computing is one of the most promising innovations impacting data storage and processing. And with it, clients rely on the IT solutions offered by an external provider instead of on-premise applications. Despite its enormous impacts, customers are still reluctant to outsource their business processes because of security concerns. As data is typically stored and governed by cloud vendors, users need to deal with security issues linked to the loss of control over their sensitive data. Cloud providers need to implement the appropriate security measures that might attract more clients while making the minimum investment. While used in various disciplines, game theory has recently expanded to investigate the effect of the defenders' and attackers' behaviors on strategic decision-making. This study aims to develop insights into how game theory can develop better security policies in cloud computing. First, we perform threat modeling to identify the potential threats facing cloud. Second, we identify the limitations of existing game based solutions and then suggest an improved model define an adequate strategy that would figure out the right balance between the required security level and the profit margins. Besides, we present future directions that can be explored to build highly reliable and optimal strategies for cloud services.

Keywords: Cloud computing · Security issues · Threats · Game theory

1 Introduction

It is commonly agreed that cloud computing has revolutionized the IT sector by pushing companies to opt a pay-per-use model for access on-demand services [1]. Concretely, a third-party vendor manages a huge range of functions from storage to processing. Despite its successes, cloud faces numerous obstacles that could affect its large-scale deployment and effective integration.

On the one hand, security concerns remain one of the most significant challenges facing public cloud [2, 3]. Note that traditional security measures focus considerably more on an access control and a secured communication channel between two sides (clients and cloud servers). Unfortunately, these encryption approaches are not suitable

The original version of this chapter was revised: The author Driss Ait Omar was included erroneously in the author list of the original publication and the name has now been removed. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-76508-8_33

M. Fakir et al. (Eds.): CBI 2021, LNBIP 416, pp. 335–347, 2021.
https://doi.org/10.1007/978-3-030-76508-8_24

for the cloud environment since the end-users may lose control over their outsourced data. Such situation would reduce the ability of cloud providers to run the arbitrary computations and execute queries over encrypted data as well [4]. Besides, cloud storage may confront all kinds of attacks, i.e. insiders and outsiders [5]. Hence, robust data security strategies are deployed before uploading data to the cloud computing [6]. Based upon this consideration, cloud providers should strive to protect their clients' privacy through standards that take into account the following factors: confidentiality assurance, integrity protection, availability, secure access, compliance with laws and regulation, service audition [7]. Obviously, the implementation of security measures is necessary to boost the large-scale adoption of this new technology. In fact, it is clearly evident that there is an economic gain for cloud providers when building customer trust and loyalty [8].

On the other hand, the required cybersecurity measures to tackle cloud threats are often considered a large investment with a low profit margin. In practice, developing efficient countermeasures that creates a win-win situation comes with new challenges linked to the exponential increase of cyber attacks. The adopted policy is usually updated by comparing the payoff with the cost of the chosen defense mechanisms. In this case, risk analysis and the decision-making process is applied in cloud environment to answer the question regarding how the cloud providers will react to the attacker actions and then select appropriate security policy.

Based on the circumstances described above, game theory models are used to address potentially conflictual issues between cloud providers and attackers by exploring and analyzing the interactions among [9–11]. Notably, these models can successfully overcome many limitations of traditional solutions as they are characterized by the following attributes: proven mathematics, reliable defense, timely action, distributed solutions [12]. Logically, threats modeling process is done at an early stage to determine the potential loss or damage when adversaries exploit cloud vulnerabilities to gain unauthorized access to an asset. In fact, the most difficult challenges influencing the adoption of the cloud multi-tenancy and distributed nature of this environment. In the next step, game-theory models are extensively applied in cloud computing to analyze the interactions between attackers and defenders [13]. This stage is very crucial in choosing the defense mechanisms that ensure the right balance between security and profit [14]. In this chapter, we concentrate on two major constraints during the problem formulation. First, robust security measures are required to attract more consumers and generate higher returns on investment. Second, this strategy may necessitate a heavy investment in terms of the operating costs of security countermeasures. In light of this fact, this study suggests a game theory model based on minimum expenses made on security measures, as well as high-profit margin services. Additionally, we show how existing models in each field are being adapted to deal with security and privacy concerns and their limitation as well. In this respect, we propose an improved attacker-defender game model to elaborate an optimal strategy that figures out the right balance between data security measures and the profitability. Unlike existing models, we suggest a hybrid approach based on threats modeling and zero-sum games for decision-making in cloud threats.

The rest of this paper is organized as follows. Section 2 examines and analyzes the related work in this field. Section 3 provides background information on cloud threats and

the principle of game theory, and we formulate and discuss the proposed game model. In Sect. 4, we highlight the major limitations of existing models as well as the fundamentals of the improved approach to tackle cybersecurity threats in cloud computing. Conclusion and perspectives are given in Sect. 5.

2 Related Work

This section briefly discusses the existing body of other researches related cyber-security game, and mentions how this method is used to analyze cloud market. In [12, 15], a comprehensive survey is provided especially the main difference between the existing game models applied to cyberspace security issues. To deal with complex systems, agent-based modeling and game theory are used to find the appropriate solution for attackers/defenders strategy [16]. In dynamic systems, stochastic game theoretic method and weighted directed graphs are used to detect intrusions in the case of computer networks [17]. Usually, game theory is used in risk analysis for strategic decision-making in the presence of adversarial attacks [18, 19]. In this respect, this technique is used for defending against a distributed denial of service attack in cloud computing [20]. In the same line, stackelberg games [21, 22] evolutionary game theory [23] are used to establish an optimal protection strategy by using game model of attack-defense scenarios. The authors in [24] rely on game theoretical analysis to determine the minimum verification requirement for cloud resources, and the optimal strategy of security policy. To this aim, they use Stackelberg game for deterministic verification model, and a probabilistic model as well. Alternatively, fuzzy inference method is used for selecting storage solutions in cloud [25]. In [26], the authors suggested a stackelberg game to find an optimal strategy that checks the outsourced data regarding its integrity and availability. In [27], game theory is used to define an optimal strategy for pricing scheme and resource allocation in cloud computing. They use mainly stackelberg equilibrium to obtain near optimal state for system's performance. Kamhoua in [28] use game theory to deal with cyber security interdependency in cloud computing. Basically, they analyze the impact of successful attacks on VM availability as well as the required expense associated with countermeasures. Besides, game theoretic model is used to ensure truth-telling ones among cloud providers. Tosh et al. use in [29] an evolutionary game theoretic model to share, among cloud providers, solutions that limit cyber attacks. More specifically, they use both dynamic cost scheme and distributed learning heuristic method to analyze how security investment affects the cybersecurity information sharing decisions.

As outlined above, significant progress has been realized in the analysis of cyber-security in cloud computing by using game theoretic models. However, the majority of existing approaches attempt to find the most generic solution that will work with all of the cloud threats. Besides, rigorous cloud threats evaluation methodology was not used. Unlike existing models, this study considers the importance of probabilistic risk models to analyze cloud threats. Additionally, we extend the traditional attacker-defender model by using a zero-sum game-theoretic to capture the dynamic nature of safety and security in cloud computing.

3 Background and Problem Statement

Overall, cyber-security is a critical process to successful identification of essential vulnerabilities and threats in cloud services so as to protect them. It is recognized that traditional methods usually involve a never-ending cycle of detection and response to new attacks taxonomy and countermeasures. Because of the cost involved in deploying security measures, we suggest game theory to make the analysis and then put forward suggestions for cloud providers to invest in optimal security strategies. In this section, we first introduce the case study that illustrates security risks in cloud computing. Afterwards, we discuss how to model these threats and potential countermeasures.

3.1 Scenario

As stated in the ISO/IEC 27005 guidelines [30], a formal risk management process is fundamental to identify, estimate and evaluate the potential attacks that affect data confidentiality, integrity, and availability. In general, one of the underlying principles of security is ensuring that all entities involved in data management should strongly consider compliance with regulations and privacy standards. Hence, data protection is crucial for a successful implementation and use of remote cloud applications.

Basically, the entire cloud ecosystem consists of four different entities [31]: (1) the data owner, who is also a cloud user and has large amount of data to be stored in the cloud computing. (2) The cloud consumer, who is authorized by the data owner to access his data. (3) The cloud server, which is managed by cloud providers to offer remote services like storage, data sharing and processing. (4) The third party auditor (TPA), which is the trusted entity that assesses the cloud storage security on behalf of the data owner upon request. The system architecture for cloud services can be depicted as in Fig. 1.

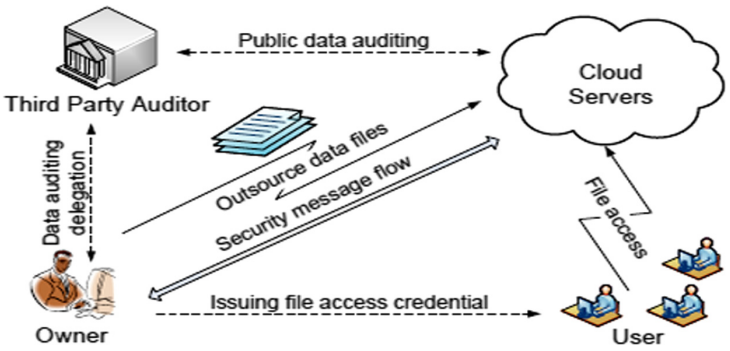

Fig. 1. The main parties involved in cloud ecosystem

In general, cloud service providers implement the necessary data protection mechanisms for online services to ensure compliance with cyber security regulations and the fulfilment of Service Level Agreement (SLA). Unfortunately, users and cloud providers may also cause vulnerabilities to distributed systems. In fact, user vigilance, information

leakage by social engineering, and unawareness of security threats can lead to damage [32]. Thus, users should be aware of risk factors that can lead to potential cloud vulnerabilities; among these are poor access management, data breach and data leak, data loss, insecure API, misconfigured cloud storage, DoS attacks, malicious insiders, account hijacking, hared dangers, etc. [33]. In this context, Table 1 provides the main threats and its impacts in cloud computing.

Table 1. The major cloud threats [34]

Threat	Property violated	Threat definition
Spoofing identity	Authentication	Pretending to be something (clients)
Tampering with data	Integrity	Change or modify the original data
Repudiation	Non- repudiation	Reject the responsibility of an action
Information disclosure	Confidentiality	Disclosure secret information
Denial of service	Availability	Prevent access online services
Elevation of privilege	Authorization	Execute or access cloud resources

Briefly, security risk can be formally defined as the possibility of a threat to exploit particular cloud vulnerability. Based on the nature of countermeasures, each risk correctly represents the relationship between the probability of security threat event and magnitude of its consequence, using their product [35].

$$\text{Risk} = \text{Threat probability} \times \text{Potential loss}$$

Let's consider two events X_1 and X_2 associated with two threats with different attack densities $\lambda 1$ and $\lambda 2$ respectively.

The probability of two attacks, which are observed in t time units, can be estimated as follows [36].

$$X(t) = X_1(t) + X_2(t) \text{ and for } t \geq 0$$

$$P\{X_1(t) = n_1\} = e^{-\lambda_1} \frac{(\lambda_1 t)^{n_1}}{n_1!}$$

$$P\{X_2(t) = n_2\} = e^{-\lambda_2} \frac{(\lambda_2 t)^{n_1}}{n_2!}$$

As the X (t) is a Poisson process, the probability of these attacks is.

$$\begin{aligned} P\{X(t) = n\} &= \sum_{n_2}^{n} P\{X_1(t) = n = n_2\} P\{X_2(t) = n_2\} \\ &= \sum_{n_2=0}^{n} e^{-\lambda_1 t} \frac{(\lambda_1 t)^{n-n_2}}{(n-n_2)!} e^{-\lambda_1 t} \frac{(\lambda_2 t)^{n_2}}{(n_2)!} \\ &= e^{(\lambda_1 t + \lambda_2) t} \frac{\{(\lambda_1 + \lambda_2) t\}^n}{(n)!} \end{aligned} \tag{1}$$

Hence, Hyper-Erlang distribution is used to model the effect of cloud attacks [36]:

$$G(x) = \sum_{i=0}^{n} P_i E_i^r(x) \; 0 < P_i \leq 1 \tag{2}$$

Where E_i^r is the r-stage Erlang distribution with the probability P_i.

We suppose that security attacks on cloud computing assumed to be a Poisson distribution with the effect parameters λ. Hence, the effect of security attacks in cloud computing can be expressed as [36]:

$$P\left\{G_t = \frac{r}{t}\right\} = \frac{e^{-\lambda t}\lambda t^r}{r!} \text{ where } \lambda, \; r \geq 0 \tag{3}$$

3.2 Game Theory for Modeling Cloud Attacks

Basically, we can perform risk analysis more accurately if we place the situation in the form of a 'game' with two players, i.e. attackers and defenders. The central idea behind using game analysis is to find out how the players choose their strategies in different situations that maximize their own utility. At its simplest level, game theory would help cloud providers define their security policy and understand the return of an investment compared to its risk.

Formally, there is two players P1 and P2 (attacker and defender) in the cloud security game. In this case, the player i selects a security strategy from S_j that generates the payoff/utility u_j. In this context, the combination of the selected strategies of the attacker or defender is considered as a strategy profile. Cyber-security game in cloud can therefore be formulated as follows:

$$Game = (P, (S_j)_{i \in P}, (u_j)_{i \in P}). \tag{4}$$

Obviously it is impossible for cloud providers to act against all the defensive attacks at all times. Moreover, each player's payoff is affected by both the actions taken by him and the other player. In fact, the attacker is trying to maximize the amount of damage and effect of security attacks in cloud computing, which are expressed in Eq. 3. In the same line, cloud providers need to invest in securing their data by implementing robust measures to reduce the risk of cyber attacks.

As a consequence, a good investment decision rule has to maintain a fair balance between the cost of each security policy and its generated revenue. The maximum utility is achieved if all players are expected to converge to the state represented by the Nash equilibrium. At this steady state of cloud market, there is no player who can improve its profit by unilaterally modifying its strategies if the actions of the other are fixed. Mathematically, the Nash equilibrium strategy is a best reaction for both services provider and attacker. A strategic form of a state is formalized as follows:

$$U_j\left(\gamma_j^*, \gamma_{-i}^*\right) \geq U_j\left(s_j, \gamma_{-i}^*\right) \;\; \forall s_j \in S_j, \forall j \tag{5}$$

Where the strategy γ^* is the Nash equilibrium.

For the sake of simplification, the used security game models in this study share the following key assumptions: (1) protection costs are identical for all cloud entities, (2) attackers launch only one kind of attack at a time, (3) all players' decision are made simultaneously.

It may be the case when a cloud provider wants to generate the expected profit B by choosing the appropriate measures that maintains trust level φ, where $0 \leq \varphi \leq 1$. In this case, a successful cyber-attack can cause major damage to cloud, which is denoted L. Additionally, the most common cybersecurity attacks carried out against cloud have the probability distribution p, where $0 \leq \rho \leq 1$.

Based on the circumstances of this case, the generic utility function [37] has the following structure:

$$\mathrm{U} = B - pL(1 - \varphi) \tag{6}$$

Note that the defender and the attacker strategy is limited by cost. Hence, we use a cost function f (x) [16] to define the relationship between security expenses and trust level φ.

$$\begin{array}{ccc} [0\ 1] & \longrightarrow & \mathbb{R} \\ \varphi & \longrightarrow & \mathrm{f}(\mathrm{x}) = \frac{ax^2}{bx-1} \end{array}$$

Where a and b are the scaling and asymptote parameters, respectively.

The attacker aims to maximize the amount of damage he causes, while the defender is trying to protect the targets and minimize the loss as well. Besides, this occurs because the attacker and the defender play simultaneously. An attacker-defender game represents the situation of a perfectly competitive in which one player can win something only by causing another player to lose it. The interactions of the attacker and the defender are typically modelled with a two-player zero-sum game aimed at more accurately predicting appropriate countermeasures against threats.

4 Improved Attacker-Defender Game Model

On the whole, attacker-defender game is a fairly new methodology for modeling security in highly complex distributed systems. The main feature of this modeling approach is the presence of a set of entities with different attributes and behaviors, and also the relationships between attackers and defenders.

In this case study, we will use a set of simple strategies for a non-cooperative game between a cloud provider and attacker. Logically, cloud providers can choose investing in protecting their data from cyber-attacks, recognizing that their choices will affect the expected profit. That is, each defender has two strategies: Invest in security (IS) or Not to Invest (NIS). In the same vein, the attacker has two strategies: launch an attack (A) on the cloud provider or Not launch an attack (NA). As security is the most principal factor in influencing the take-up of cloud services, end-users have two variants: trust (T) or (2) distrust (D) the cloud provider. After analyzing the interactions among players involved in cloud security, we use game theory models to produce an optimal decision-making for the adopted security policy.

Based on the circumstances described above, considering the case of a three-player game with a 3-tuple (T, IS, A) that represent a strategy profile, the utility function can be described as follows [38]:

The cloud payoff:

$$U(T, IS, A) = G - \lambda + a\lambda \tag{7}$$

Where

G: refers to the total costs of the delivered services
λ represents the total loss after attacks, which is calculated using Eq. 3
α is the probability of these attacks, which is calculated using Eq. 1

Naturally, each cloud provider would expect to get an outcome R obtained after investing in security measures and also incurs a cost e for the security expenses. Here the attacker can cause damage λ with a probability α by launching attacks against a particular cloud resource.

For Nash equilibria, it can help predict the behavior of the cloud provider wanting to maximize their payoff in the game [38].

$$R - e - \lambda(1 - \alpha) > R - \lambda, \text{ where } e < \lambda\alpha \tag{8}$$

It means that investing in security measures is the best option for the cloud provider in order to reduce risk of users' data leakage and improve the profit margin.

A survey of current game models applied in cloud demonstrates the importance of understanding the relation between the two parties involved in data security, i.e. providers and attackers. In general, the attacker's objective is in conflict with that of the cloud provider that aims at minimizing the damage of cyberspace. Thus, the issue between the provider and the attacker is commonly formulated as a non-cooperative model so as to capture the dynamic nature of the two parties' behavior. However, despite the importance of the existing models, most of them did not take into account other requirements linked to security's assumptions and constraints.

Based on this consideration, we are interested in dynamic non-cooperative model [39] because it is very useful in modelling and evaluating multiple actions taken by individual players. More precisely, we suggest zero-sum games for decision-making problems involving competition between cloud providers and attackers; where there is one winner and one lose. In fact, cloud providers have a strong interest in defending their facilities against intentional attacks, assuming the attacker will adopt a best response to defender's strategy. In other words, each cloud provider's gain or loss of utility is exactly balanced by the loss or gain of the attackers. Consequently, there is a single optimal strategy that is preferable to cloud provider to prevent data disclosure, while maintaining a reasonably high security level at low cost. This work introduced the idea that this conflict of interests could be formally expressed and analyzed by zero-sum games [40, 41]. For cloud threats, we rely on the study carried on the Sect. 3.1. For simplicity reasons, we only consider three elements to model the relation or competition in cloud market game: players, actions for implementing security strategy, and payoff matrix. Before giving the formal description of the game model, we first define the role of each player:

- **Players.** We consider two players: (1) attackers which benefit from harming cloud services (2) cloud provider utilize countermeasures to reduce the impact of attacks so as to protect clients' data.
- **Action sets.** It represents the sets of actions for each player. For cloud provider, we consider $D = \{d_1, d_2, \ldots, d_m\}$ as m refers to the number of the implemented security mechanism to protect outsourced data. Meanwhile, the attacker can conduct malicious actions that exploit n vulnerabilities in cloud computing; these actions are represented as $A = \{a_1, a_2, \ldots, a_n\}$.
- **Payoff matrix.** We use a reward function to essentially model the attacker's motivation and provider's payoff for an action Υ_{ij} (the action i for attacker and reaction j of cloud provider). This function is n × m matrix; each row represents the attacker action while each column is the possible cloud provider's reaction corresponding to this action. The payoff matrix can be expressed in the following way in mathematical terms:

$$\Upsilon = \begin{bmatrix} \Upsilon_{11} & \ldots & \Upsilon_{1m} \\ \vdots & & \vdots \\ \Upsilon_{n1} & \ldots & \Upsilon_{nm} \end{bmatrix} \tag{9}$$

The payoff function regarding cybersecurity in cloud computing can be expressed as follows [39]:

$$\Upsilon_{ij} = s_j - \left(s_i \times e_{ij}\right) + U \times p_i \times \left(1 - e_{ij}\right) + r_i \times \left(1 - e_{ij}\right), \forall i, j \tag{10}$$

Where

– s_i is the cost of implementing a defense strategy
– e_{ij} is the metric to measure efficacy of a defense mechanism
– U is the total production (the availability) of cloud services
– p_i is the rate of the loss in the cloud services caused by attack type i
– r_i is the recovery cost associated with action i due to a specific attack

To efficiently predict the behavior of attacker and defender, threat detection has evolved from static to dynamic behavioral analysis. Accordingly, the proposed approach to secure cloud computing is essentially composed of two stages: (1) threats modeling and (2) game theory optimization, as illustrated in Fig. 2.

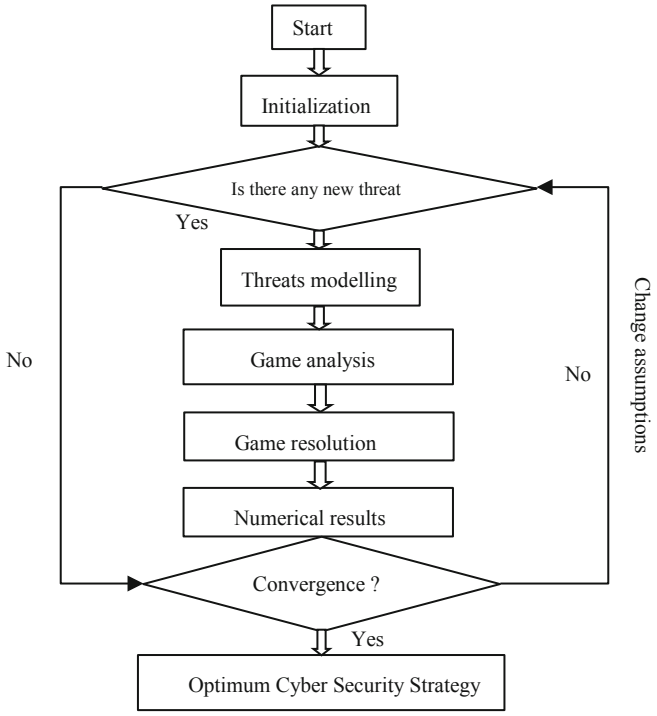

Fig. 2. The flowchart of the proposed approach

5 Conclusion

Despite still being in its infancy, the usage of game theory in cloud computing is a promising approach to promote this new paradigm. There have been several attempts to adopt game theory to ensure a healthy balance between productivity and security. Originally, game theory can successfully model the interaction between attackers and services providers. This work summarizes the advantages and limitations of existing game models to address cyber security risks in the cloud environment. Even though these models are extremely useful to find the most optimal solution, there are still improvements that need to be made to meet the expectations of both the providers and the end-users. In this respect, threats modeling methodology is an initial stage towards improving the elaboration of any security policy. Besides, it is important to select the most appropriate game theory model that well capture the essential characteristics of cloud computing and cyber security features. To this aim, we suggest zero-sum game model for selecting the most appropriate countermeasure options to a given threat in argue-scale cloud data centers. More precisely, the proposed strategy would undoubtedly help cloud providers take decisive and appropriate actions against adversary attacks. In the future work, we plan to analyze cybersecurity issues in cloud computing using zero-sum game with rational players and the proposed threats model [42]. Besides, we intend to study the influence of the suggested countermeasures on each player's payoff through numerical simulation and experimental validation. Another interesting and promising approach is the utilization

of evolutionary games [43, 44] to analyze the dynamic relationship between attacker and defender, a process which clearly follows the evolutionary models more closely. Besides, stackelberg game is also a promising technique to simulate attacker/defender behavior for situation where the defender only knows the prior probabilities of different types of attackers.

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing. Technical report, National Institute of Standards and Technology, vol. 15, pp. 1–3 (2009)
2. Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing V4.0, Cloud Security Alliance, Seattle, WA, USA (2017)
3. Mazhar, A., Samee, U.K., Athanasios, V.: Security in cloud computing: opportunities and challenges. Inf. Sci. **305**, 357–383 (2015)
4. Fernandes, D., Soares, L., Gomes, J., Freire, M.M., Inácio, P.: Security issues in cloud environments: a survey. Int. J. Inf. Secur. **13**(2), 113–170 (2013). https://doi.org/10.1007/s10207-013-0208-7
5. Pearson, S., Benameur, A.: Privacy, security and trust issues arising from cloud computing. In: Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science (CLOUDCOM), Washington, DC, pp. 693–702. IEEE Computer Society (2010)
6. Xiao, L., Xu, D., Mandayam, N.B., Poor, H.V.: Cloud storage defense against advanced persistent threats: a prospect theoretic study. IEEE J. Sel. Areas Commun. **35**(3), 534–544 (2017)
7. Singh, A., Chatterjee, K.: Cloud security issues and challenges: a survey. J. Netw. Comput. Appl. **79**, 88–115 (2017)
8. Radwan, T., Azer, M.A., Abdelbaki, N.: Cloud computing security: challenges and future trends. Int. J. Comput. Appl. Technol. **55**(2), 158–172 (2017)
9. Kwiat, L., Kamhoua, C.A., Kwiat, K.A., Tang, J., Martin, A.P.: Security-aware virtual machine allocation in the cloud: a game theoretic approach. In: Proceedings of the 8th IEEE International conference on Cloud Computing, CLOUD 2015, New York City, NY, USA, pp. 556–563 (2015)
10. Pillai, P.S., Rao, S.: Resource allocation in cloud computing using the uncertainty principle of game theory. IEEE Syst. J. **10**(2), 637–648 (2016)
11. Li, Y.P., Tan, S.Y., Deng, Y., Wu, J.: Attacker-defender game from a network science perspective. Chaos: Interdisc. J. Nonlinear Sci. **28**(5), Article ID 051102 (2018)
12. Do, C.T., et al.: Game theory for cyber security and privacy. ACM Comput. Surv. **50**(2), Article 30 (2017)
13. Wu, H., Wang, W., Wen, C., Li, Z.: Game theoretical security detection strategy for networked systems. Inf. Sci. **453**, 346–363 (2018)
14. Cheng, L., Ma, D.H., Zhang, H.Q.: Optimal strategy selection for moving target defense based on markov game. IEEE Access **5**, 156–169 (2017)
15. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A survey of game theory as applied to network security. In: Proceedings of the International Conference on 43rd Hawaii International Conference, pp. 1–10 (2010)
16. Alan Nochenson, C.F., Heimann, L.: Simulation and game-theoretic analysis of an attacker-defender game. In: Grossklags, J., Walrand, J. (eds.) GameSec 2012. LNCS, vol. 7638, pp. 138–151. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34266-0_8
17. Nguyen, K.C., Alpcan, T., Basar, T.: Stochastic games for security in networks with interdependent nodes. In: Proceedings of the International Conference on Game Theory for Networks, GameNets 2009, pp. 697–703. IEEE (2009)

18. Meng, S., Wiens, M., Schultmann, F.: A Game-theoretic approach to assess adversarial Risks. WIT Trans. Inf. Commun. Technol. **47**, 141–152 (2014)
19. Musman, S., Turner, A.: A game theoretic approach to cyber security risk management. J. Defense Model. Simul. Appl. Methodol. Technol. **15**(2), 127–146 (2018)
20. Wang, B., Zheng, Y., Lou, W., Hou, Y.T.: DDoS attack protection in the era of cloud computing and software defined networking. Comput. Netw. **81**, 308–319 (2015)
21. Jakóbik, A., Palmieri, F., Kołodziej, J.: Stackelberg games for modeling defense scenarios against cloud security threats. J. Netw. Comput. Appl. **110**, 99–107 (2018)
22. Jakobiki, A.: Stackelberg game modeling of cloud security defending strategy in the case of information leaks and corruption. Simul. Model. Pract. Theory **103**, Artile ID 102071 (2020)
23. Sun, P.J.: Research on the optimization management of cloud privacy strategy based on evolution game. Secur. Commun. Netw. **2020**, 18, Article ID 6515328 (2020)
24. Djebaili, B., Kiennert, C., Leneutre, J., Chen, L.: Data integrity and availability verification game in untrusted cloud storage. In: Poovendran, R., Saad, W. (eds.) GameSec 2014. LNCS, vol. 8840, pp. 287–306. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12601-2_16
25. Esposito, C., Ficco, M., Palmieri, F., Castiglione, A.: Smart cloud storage service selection based on fuzzy logic, theory of evidence and game theory. IEEE Trans. Comput. **65**(8), 2348–2362 (2016)
26. Ismail, Z., Kiennert, C., Leneutre, J., Chen, L.: Auditing a cloud providers compliance with data backup requirements: a game theoretical analysis. IEEE Trans. Inf. Forensics Secur. **11**(8), 1685–1699 (2016)
27. Jalaparti, V., Nguyen, G.D.: Cloud resource allocation games (2019)
28. Kamhoua, C.A., Kwiat, L., Kwiat, K.A., Park, J., Zhao, S.M., Rodriguez, M.: Game theoretic modeling of security and interdependency in a public cloud. In: Proceedings of IEEE 7th International Conference on Cloud Computing, pp. 514–521 (2014)
29. Tosh, D.K., Sengupta, S., Kamhoua, C.A., Kwiat, K.A.: Establishing evolutionary game models for cyber security information exchange (CYBEX). J. Comput. Syst. Sci. **98**, 27–52 (2018)
30. ISO/IEC 27005: Information technology security techniques information security risk management (2008)
31. Chang, V., Kuo, Y., Ramachandran, M.: Cloud computing adoption framework: a security framework for business clouds. Future Gener. Comput. Syst. **57**, 24–41 (2016)
32. Ravi Kumar, P., Herbert Raj, P., Jelciana, P.: Exploring security issues and solutions in cloud computing services: a survey. Cybern. Inf. Technol. **17**(4), 3–31 (2016)
33. Birje, M.N., Challagidad, P.S., Goudar, R.H., Tapale, M.T.: Cloud computing review: concepts, technology, challenges and security. Int. J. Cloud Comput. **6**(1), 32–57 (2017)
34. Julian, J.J., Surya, N.: A survey of emerging threats in cybersecuirty. J. Comput. Syst. Sci. **80**(5), 973–993 (2014)
35. Saripalli, P., Walters, B.: QUIRC: a quantitative impact and risk assessment framework for cloud security. In: Proceedings of International Conference on Cloud Computing, Miami, FL (2010)
36. Meetei, M.Z.: Mathematical model of security approaches on cloud computing. Int. J. Cloud Comput. **6**(3), 187–210 (2017)
37. Grossklags, J., Christin, N., Chuang, J.: Secure or insure? A game-theoretic analysis of information security games. In: Proceedings of International Conference World Wide Web Conference (WWW 2008), Beijing, China, pp. 209–218, April 2008
38. Njilla, L.Y., Pissinou, N., Makki, K.: Game theoretic modeling of security and trust relationship in cyberspace. Int. J. Commun. Syst. **29**, 1500–1512 (2016)
39. Lv, K., Chen, Y., Hu, C.: Dynamic defense strategy against advanced persistent threat under heterogeneous networks. Inf. Fusion **49**, 216–226 (2019)

40. Al Mannai, W.I., Lewis, T.G.: A general defender-attacker risk model for networks. J. Risk Finan. **9**(3), 244–261 (2008)
41. Halevy, N.: Resolving attacker-defender conflicts through intergroup negotiation. Behav. Brain Sci. **42**, E124 (2019)
42. Zarreha, A., Saygina, C., Wana, H., Leea, Y., Brachoa, A.: A game theory based cybersecurity assessment model for advanced manufacturing systems. Procedia Manuf. **26**, 1255–1264 (2018)
43. Cressman, R., Apaloo, J.: Evolutionary game theory. In: Başar, T., Zaccour, G. (eds.) Handbook of Dynamic Game Theory, pp. 461–510. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-44374-4_6
44. Khalifa, N.B., El-Azouzi, R., Hayel, Y., Mabrouki, I.: Evolutionary games in interacting communities. Dyn. Games Appl. **7**(2), 131–156 (2017)