A Survey of Game Theoretic Solutions for Cloud Computing Security Issues

Bernard Ousmane Sane[1](✉), Cheikh Saliou Mbacke Babou[1], Doudou Fall[2], and Ibrahima Niang[1]

[1] University Cheikh Anta Diop of Dakar, Fann Bp 5005, Dakar, Senegal
{bernardousmane.sane,cheikhsalioumbacke.babou, ibrahima1.niang}@ucad.edu.sn

[2] Nara Institute of Science and Technology, Ikoma, Nara 630-0192, Japan
doudou-f@is.naist.jp

Abstract. Cloud computing has become quintessential to information technology as it represents the foundation of all the emerging paradigms. Cloud computing uses virtualization to maximize resources utilization. Despite its benefits, organizations are still reluctant to adopt cloud computing due to its numerous security issues. Among the solutions that have been provided to solve cloud security issues, game theoretic proposals showed great potentials. In this paper, we survey the most representative game theoretic approaches to solve cloud computing security issues. We classify these approaches or methods based on their security scenarios and their respective solutions. We overview different solutions to control cloud vulnerabilities and threats using game theory. We also investigate and identify the limitations of these solutions and provide insights of the future of cloud security particularly on virtual machines, hypervisors and data security.

Keywords: Cloud computing · Game theory · Security · Countermeasures · Virtualization

1 Introduction

Cloud computing has become quintessential to information technology (IT) as it represents the foundation of all the emerging technologies: big data, Internet of Things (IoT), artificial intelligence (AI), etc. The security issues of cloud computing are numerous and complex, and greatly participate on preventing its widespread adoption [13,23]. The existing security solutions are not suitable for the dynamic aspect of cloud computing because they depend on traditional security models (BellLaPadula (BLP) model, Biba model, etc.), that are more adequate for static attack scenarios [33]. Additionally, the traditional cybersecurity solutions are lagging behind in terms of quantitative analysis and decision-making frameworks. Several solutions have been proposed to tackle the security

G. Bassioni et al. (Eds.): InterSol 2019, LNICST 296, pp. 1–12, 2019.
https://doi.org/10.1007/978-3-030-34863-2_1

Table 1. A summary of useful survey papers in cloud computing and (or) the domain of game theory.

Cloud computing						
Reference	Year	Data	VMs	Hypervisor	Method countermeasure using game theory	Mathematical perspective on game theory
[33]	2016	No	No	No	Yes	Yes
[23]	2016	No	Yes	Yes	Yes	No
[13]	2014	Yes	Yes	Yes	No	No
[14]	2019	Yes	Yes	No	Yes	No
This paper	2019	Yes	Yes	Yes	Yes	Yes

issues of cloud computing. Among them, game theory methods have particularly been effective [21,28]. As mentioned in paper [33], game theory and cybersecurity have similar features. Indeed, in game theory, a player's payoff depends on his strategy and the strategies of the other players. In cybersecurity, the security of an information system depends both on the administrator's security policy and on the attacker's strategies. This commonality makes game theory an essential mathematical tool for cloud computing security.

This manuscript is a survey of game theoretic methods for cloud computing security issues. We first classify game theoretic methods based on their security scenarios and respective solutions. Furthermore, from the threats and vulnerabilities on cloud computing, we study related security solutions that are based on game theory. We also provide research perspectives on cloud security, particularly on virtual machine, hypervisor and data security. In Table 1, we show how our paper differs from the existing survey papers – [13,14,23,33] – in this field.

This paper is organised as follows: in Sect. 2, we present cloud computing. In Sect. 3, we give some background and the application of game theoretical concepts to cybersecurity. In Sect. 4, we present a variety of threats associated with cloud computing systems and also their countermeasures by using game theory approaches. This paper ends with the main conclusions and discussion for future research in Sect. 5.

2 Cloud Computing Security

2.1 Cloud Computing:

IT resources have become easy to access with cloud computing where almost everything related to IT can be serviced through the Internet [22]. The major characteristics of cloud computing, such as elasticity (the ability to dynamically adapt to the users resource needs), pay-per-use (which means, you just pay the time services that you use), transfer of risk (a specific risk is passed from the developers to the providers), etc., have revolutionized the way that we make use of computing [29].

We acknowledge that there are many definitions of cloud computing [13,29,31]. However, the National Institute of Standards and Technology (NIST) definition seems to cover all essential aspects [30]: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". In summary, there are five essential characteristics: *on-demand self service*, *broad network access*, *resource pooling*, *rapid elasticity*, and *measured service*. Cloud computing has three service models:

- *Software as a Service (SaaS)*, in which ready-to-use applications are serviced to the customers,
- *Platform as a Service (PaaS)*, in which the cloud service providers (CSPs) provide design and development environments to the users
- *Infrastructure as a Service (IaaS)*, in which the CSPs provision manageable virtual machines to the users.

The NIST definition contends that there are four main deployment models in cloud computing:

- *Public clouds*, which are open to anyone,
- *Community clouds*, restricted to groups with similar goals,
- *Private clouds*, restricted to a single organization and,
- *Hybrid clouds*, a combination of the aforementioned.

Despite all its benefits, security is the most important factor that is hindering the wide use of cloud computing. In Subsect. 2.2, we present the classification of cloud vulnerabilities.

2.2 Cloud Computing Security Issues

We present a variety of threats associated with cloud computing systems and classify them into four categories according the services:

Infrastructure as a Service (IaaS)

- **Network threats:** in cloud computing, the virtual machines (VMs) are connected through a network. Adversaries can launch various kinds of attacks (XML Signature Wrapping Attack, Flooding Attack (DDoS), Metadata Spoofing Attack, etc.) in a cloud system through its network which may deteriorate the quality of cloud services.
- **Host threats:** are related to virtual machines, hypervisors and data. In fact, on an existing cloud system, the support for security isolation is limited. Since different VMs are sharing the same resources, the VM-based attacks exploit vulnerabilities in the virtual machines or the underlying hypervisor in the LAN (Local Area Network) to violate data protection and affect the cloud services. Host attacks can be split into subcategories:

- VM to VM attacks: in which we have cross-VM side-channel attacks, scheduler-based attacks, VM migration and rollback attacks, etc.
- VM to Hypervisor attacks: in which we have VM Hopping and VM Escape attacks, etc.
- Data attacks: in which we have Data Confidentiality, Data Integrity, Data Availability, Data Isolation, etc.

Platform as a Service (SaaS)

- **Application threats:** Risks associated with the Applications-based attacks include: Malware injection, steganography attacks, Web services- & protocol-based attacks, Security Misconfiguration, SQL Injection Attack.

Software as a Service (PaaS)

- **Information security policy issues:** the provider is the manager and he defines the security policy and the security mechanisms of the deployed services. Improper Data Sensitization, Information leakage, Vendor Lock-in are the problems that can arise from poor management.

3 Overview of Game Theory

In this section, we elaborate fundamental notions of game theory.

Definition 1. Game [28].
A description of the strategic interaction between cooperative and non-cooperative players where the payoff of a player's choice of action depends on the action of other players.
In game theory, we use the following terms to describe a game:

- **Player:** a participant of the game who is called to make a decision for actions.
- **Action:** an action by a player refers a move in the given game.
- **Payoff:** the recompense or penalty inflicted to a player as a result of his action in the game.
- **Strategy:** the Oxford Dictionary defines strategy as "*a plan of action or policy designed to achieve a major or overall aim*" in a game.

Definition 2. Game theory is a branch of mathematics used to model all situations where we need to make decisions.

Definition 3. Nash equilibrium: or strategic equilibrium, is a stable state of the game in which no player can unilaterally change his strategy and get a better payoff. It is represented by a list of strategies, one for each player.

Definition 4. Non-cooperative game [33]*:* is a game in which each player is interested by his own gain. The players are said to be selfish.

Table 2. Game models and security issues

Game model			Suitable scenario	Solution	Reference
Non-cooperative games	Static games	Incomplete imperfect	DDoS attacks vs admin network	Bayesian nash equilibrium	*Liu et al.* [18]
			Intrusion detection	Bayesian nash equilibrium	*Liu et al.* [19]
		Complete imperfect	Information warfare	Bayesian Nash equilibrium	*Carin et al.* [6], *Jormakka et al.* [11]
	Dynamic games	Complete imperfect	Intrusion detection	Optimal solution	*Alpcan et al.* [2]
			Network security	Nash equilibrium	*Nguyen et al.* [24]
		Incomplete imperfect	Network security	Nash equilibrium	*Alpcan et al.* [1]
			Network security	Nash and Bayesian	*You et al.* [4]
		Complete perfect	Computer network	Nash equilibrium	*Lye et al.* [20]
			Risk assessment	optimal solution	*Xiaolin et al.* [34]
			Security and intrusion detection	Nash equilibrium	*Nguyen et al.* [25]
		Incomplete perfect	Intrusion detection in mobile ad-hoc network	Nash and Bayesian	*Patcha et al.* [26]
			Information network	Nash equilibrium	*Alpcan et al.* [3]
			Intrusion response	Optimal solution	*Bloem et al.* [5]

Definition 5. Cooperative game [33]*:* is a competition between groups of players, rather than between individual players. Players who are in the same group cooperate.

Remark 1. In reality, many cybersecurity issues are non-cooperative games [33]. Hence, in the remaining of the paper, we will focus on Non-cooperative games.

3.1 Classification

Based on a number of stages (one or multiple), we have *Static* and *Dynamic games* [33].

- In a *static game* (or strategic game), each player makes a single decision at the beginning of the game at the same time and each of them has no information about the actions of the other players before making their own action.
- *A dynamic game* (or extensive game) is a game that is comprised of multiples steps, and players may have some information about the outcomes of the previous games.

We have the following sub-classes in Static and Dynamic Games:

- perfect information or not;
- complete information or not.

Table 3. Analysis of game theoretic methods for VM to VM attacks and VM to hypervisor attacks in cloud environments.

Cloud Resource Allocation Games, (*Jalaparti et al.* [10], 2010)

Characteristics	Parameters and assumptions	
a. Define a CRAG (cloud resource allocation game)	Game	CRAG: Static SCRAG: Dynamic
b. Prove that with a function named linear cost functions, the cost to the system at Nash equilibrium is at most a constant factor over the optimal	Game players	Cloud users Provider
c. Define an SCRAG (Stackelberg CRAG) and two types of strategies: Aloof Strategy [10] and Least cost first strategy [10]	Assumptions	- As resource, only CPU is considered for all clients - Selfish clients - The provider's goal is to optimize the total utility of the clients - The cloud has sufficient amount of resources
d. Using strategy named Least cost first at the SCRAG, they show the cost to the system at Nash equilibrium is at most $1/\alpha$ times worse compared to the optimal assignment for the CRAG where α is the fraction of jobs to the optimal assignment for the CRAG		

Game Theoretic Modeling Of Security And Interdependency In A Public Cloud, (*Kamhoua et al.* [12], 2014)

Characteristics	Parameters and assumptions	
a. Study the interdependence problem in a public cloud	Game	Static
b. Game theory is used to model the scenario in which an indirect attack is considered for independent users	Game players	Cloud users
c. The model is defined so that the hypervisor is not directly compromised	Assumptions	- Players are rational - Each player has two strategies: Invest in security or not

Security Aware Virtual Machine Allocation In Cloud: A Game Theoretic Approach, (*Kwiat et al.* [17], 2015)

Characteristics	Parameters and assumptions	
	Game	Static
a. Propose a solution that minimize interdependence in [12]	Game players	Cloud users
b. Nash Equilibrium doesn't dependent of the hypervisor's behavior with independent users (malicious or not)	Assumptions	- Players are rational - Each user runs only one virtual machine
c. Resolve issues of Interdependency among several users		

Establishing evolutionary game models for CYBer security information EXchange (Cybex), (*Deepak et al.* [32], 2016)

Characteristics	Parameters and Assumptions	
	Game	Non-cooperative dynamic game
a. Cybex (CYBer security information EXchange) game formulation and analysis	Game players	Firm
b. To find the optimal Equilibrium solution for the stability of a chosen strategy	Assumptions	- The players are rational - Firms are dynamically evolving and interacting in a non-cooperative manner

Remark 2. All static games are of the sub-class imperfect information because they only have one stage.

Table 2 shows the connection between cybersecurity and game theory. Flagship papers contributed to this relationship [15,16].

4 Discussions on Different Game Theory Methods Applied to Host Threats

We present the state-of-the-art practices to control virtual machines, hypervisors and data vulnerabilities using game theory.

4.1 Game Theoretic Methods Against VM to VM Attacks and VM to Hypervisor Attacks

Based on the independent nature of cloud users, the literature review suggests that using game theory can help solve many issues such as virtual machine allocation [27,35]. Hence, some papers like [10,12,17] focus on game theoretic approaches and their applications to efficient and secure virtual machine resource allocations.

In Table 3, we compare different papers that use game theoretic methods for virtual machine and hypervisor security on cloud computing system [10,12,17, 32].

4.2 Game Theoretic Methods Against Data Attacks

On cloud computing, many users share the same storage platform. This allows malicious (but legitimate) cloud users to get access and alter other users' data. In table 4, we analyse papers [7–9] that talk about data security on cloud computing.

4.3 Discussions and Challenges

In cloud computing, multiple clients share the same resources like CPU that could cause interference between users' tasks. For instance, if we consider the rates per CPU/hours, a client will be paid more when the server is loaded than when it is not. This means that the interaction between customer tasks has an impact on prices. However existing pricing and scheduling schemes do not focus on these interconnectedness between the clients who are hosted in the cloud. As solution, in 2010 *Jalaparti et al.* proposed a game theory method for modeling the complex client-client (CRAG) and client-provider (SCRAG) interactions in a cloud [10]. Unlike traditional solutions, they ensured that the pricing will be optimal and proportional to the resources used by the clients. On the provider side the resources will be used optimally.

On the other hand, a the major factor that makes difficult the adoption of the cloud comes from the danger of sharing the hypervisor. In fact, an attacker can launch an indirect attack on user x by first compromising the VM of user y and then passes on the hypervisor. If the latter is compromised, all the machines which are connected to it will be compromised including that of user x. This is an interdependency problem, where the security of one user may impact the security of another user. It is another interaction between cloud users that

Table 4. Analysis of game theoretic methods for data security in the cloud.

Smart Cloud Storage Service Selection Based on Fuzzy Logic, Theory of Evidence and Game Theory, (*Esposito et al.* [8], 2015)		
Characteristics	Parameters and Assumptions	
a. They used fuzzy inference for choosing the best service against the problem of storage service selection	Game	Non-cooperative game with complete information
b. Diverse formulations of the strategies to efficiently find the best solution	Game players	Customers
	Assumptions	-Egoistical players -Each player is interested by how to optimise its own cost without any consideration of the situation of the other players
Data Integrity and Availability Verification Game in Untrusted Cloud Storage, *(Djebaili et al.* [7], 2014)		
Characteristics	Parameters and Assumptions	
a. Resolve the cloud data check for that they define cloud storage verification game and find the Nash equilibrium for solving the game	Game	Non-cooperative game
	Game players	Third party auditor Cloud provider
b. Consider more realistic assumptions in their model	Assumptions	- The provider stores the clients data - The third party auditor checks data by using a deterministic schema - Strategy type: Mixed strategy - Third party auditor actions are ‘check’ or ‘not check’ - Cloud provider actions are ‘delete’ or ‘modify’
Auditing a Cloud Providers Compliance with Data Backup Requirements: A Game Theoretical Analysis, (*Ziad Ismail et al.* [9], 2016)		
Characteristics	Parameters and Assumptions	
a. Focus on verifying data availability when data is outsourced to the cloud provider	Game	Non-cooperative static game
b. Third party auditor’s optimal verification	Game players	The provider and the Third party auditor(TPA)
c. With a case study, they experiment the analytical results	Assumptions	- Players are rational - Auditor has as strategy to ‘check’ or ‘not check’ and the provider, ‘replicate’ or ‘not’

traditional security methods cannot resolve. We contend that game theory is exactly right for this situation. This is because it is described as a mathematical model between opposing, or cooperating decision-makers. Hence, *Kamhoua et al.* viewed attacks on the hypervisor and how to mitigate them from a game theoretical perspective [12]. *Kwiat et al.* [17] proposed a solution against the negative externality issue that was elicited in [12]. However, in [12] and [17] a game player knows other players estimated loss.

A collaboration of security agencies is necessary to cope with future cyber crimes. However, a framework is needed to facilitate the exchanges between the agencies or firms: Cybex (Cybersecurity Information Exchange). The authors in paper [32] studied Cybex using game theory, because Cybex involves firms, i.e., decision-makers. In addition, the connection between game theory and cybersecurty is already established [12,33]. However, the authors considered just two crucial problems related to cybersecurity.

Integrity and availability are the main issues we encounter while storing data in cloud computing systems. Despite the proposal of several verification schemes in the literature, questions are still asked about the frequency of verification schemes and their optimal/efficient usage. The best approach will be to use game theory to achieve the minimum cost, maintain accuracy and consistency. That is why in [7], the authors tried to find the best approach by treating the data integrity check issue as a non-cooperative game, and by deriving the minimum verification resource requirements and the optimal strategy of the verification. Similarly, *Ismail et al.* analyzed the issue of checking availability of the data when it is outsourced to a cloud service provider [9]. They formulated the issue between the cloud provider and the third party auditor as a non-cooperative game for finding an optimal data verification strategy.

As future works, [10] opens exciting challenges such as: the proposition of other game models that take into account different types of resources, including many cloud service providers, and various privacy and security constraints that a user might require, e.g., Client X may not want to be collocated with Client Y. It will be also interesting to redesign the proposal of *Kwiat et al.* [17] as a game with incomplete information and to extend the proposal of *Tosh et al.* [32] with different investment scenarios. The authors of [7] focus on data verification and integrity in cloud computing systems where the provider is dishonest. However, their work requires improvements by considering other assumptions such as the externalization of several types of a data to a provider, replication of data, etc. In [9], the authors experimented with the aforementioned situation by replicating each type of the same data numerous times in the cloud. They featured in limited parameters: size and sensitivity.

5 Conclusion

This survey summarizes the advantages and limitations of several cloud proposals on virtual machine security, hypervisor security and data security, that use game theory. In each category of the proposals, we reviewed the parameters, assumptions and characteristics of the proposed solutions. We notice that game theory solves many security issues that traditional methods cannot solve. Among these problems, we have: interactions between users tasks, interdependency problem between users on the same hypervisor, data verification for achieving minimum cost, maintaining accuracy and consistency data, etc. We observed fundamental limitations in some proposed game model solutions that should be taken into account in future research.

References

1. Alpcan, T., Basar, T.: A game theoretic analysis of intrusion detection in access control systems. In: 2004 43rd IEEE Conference on Decision and Control (CDC) (IEEECat. No.04CH37601), vol. 2, pp. 1568–1573 December 2004
2. Alpcan, T., Basar, T.: An intrusion detection game with limited observations (2005)
3. Alpcan, T., Pavel, L.: Nash equilibrium design and optimization. In: 1st International Conference on Game Theory for Networks, GAMENETS 2009, Istanbul, Turkey, 13-15 May 2009, pp. 164–170 (2009)
4. You, X.Z., Shiyong, Z.: A kind of network security behavior model based on game theory. In: Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 950–954, August 2003
5. Bloem, M., Alpcan, T., Basar, T.: Intrusion response as a resource allocation problem. In: Proceedings of the 45th IEEE Conference on Decision and Control, pp. 6283–6288, December 2006
6. Carin, L., Cybenko, G., Hughes, J.: Cybersecurity strategies: the queries methodology. Computer **41**(8), 20–26 (2008)
7. Djebaili, B., Kiennert, C., Leneutre, J., Chen, L.: Data integrity and availability verification game in untrusted cloud storage. In: Proceedings of 5th International Conference on Decision and Game Theory for Security, GameSec 2014, Los Angeles, CA, USA, 6-7 November 2014, pp. 287–306 (2014)
8. Esposito, C., Ficco, M., Palmieri, F., Castiglione, A.: Smart cloud storage service selection based on fuzzy logic, theory ofevidence and game theory. IEEE Trans. Comput. **65**(8), 2348–2362 (2016)
9. Ismail, Z., Kiennert, C., Leneutre, J., Chen, L.: Auditing a cloud providers compliance with data backup requirements: a game theoretical analysis. IEEE Trans. Inform. Forensics Secur. **11**(8), 1685–1699 (2016)
10. Jalaparti, V., Nguyen, G.D.: Cloud resource allocation games, March 2019
11. Jormakka, J., Mols, J.V.E.: Modelling information warfare as a game. J. Inform. Warfare **4**, 12–25 (2005)
12. Kamhoua, C.A., Kwiat, L., Kwiat, K.A., Park, J.S., Zhao, M., Rodriguez, M.: Game theoretic modeling of security and interdependency in a public cloud. In: 2014 IEEE 7th International Conference on Cloud Computing, pp. 514–521, June 2014
13. Khalil, I., Khreishah, A., Azeem, M.: Cloud computing security: a survey. Computers **3**, 1–35 (2014)
14. Koloniari, G., Sifaleras, A.: Game-theoretic approaches in cloud and P2P networks: issues and challenges. In: Sifaleras, A., Petridis, K. (eds.) Operational Research in the Digital Era – ICT Challenges. SPBE, pp. 11–22. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-95666-4_2
15. Kunreuther, H., Heal, G.: Interdependent security: the case of identical agents. Working Paper 8871, National Bureau of Economic Research, April 2002
16. Kunreuther, H., Kunreuther, H.: Interdependent security: the case of identical agents. J. Risk Uncertain. **26**, 2003 (2002)

17. Kwiat, L., Kamhoua, C.A., Kwiat, K.A., Tang, J., Martin, A.P.: Security-aware virtual machine allocation in the cloud: a gametheoretic approach. In: 8th IEEE International Conference on Cloud Computing, CLOUD 2015, New York City, NY, USA, 27 June - 2 July 2015, pp. 556–563 (2015)
18. Liu, P., Zang, W., Yu, M.: Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Trans. Inf. Syst. Secur. **8**(1), 78–118 (2005)
19. Liu, Y., Comaniciu, C., Man, H.: A Bayesian game approach for intrusion detection in wireless ad hoc networks. In: Proceeding from the 2006 Workshop on Game Theory for Communications and Networks, GameNets 2006. ACM, New York(2006)
20. Lye, K.-W., Wing, J.M.: Game strategies in network security. Int. J. Inf. Secur. **4**(1–2), 71–86 (2005)
21. Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.-P.: Game theory meets network security and privacy. ACM Comput. Surv. **45**(3), 25:1–25:39 (2013)
22. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A.: Cloud computing - the business perspective. Decis. Support Syst. **51**(1), 176–189 (2011)
23. Narwal, P., Kumar, D., Sharma, M.: A review of game-theoretic approaches for secure virtual machine resource allocation in cloud. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (2016)
24. Nguyen, K.C., Alpcan, T., Basar, T.: Security games with incomplete information. In: 2009 IEEE International Conference on Communications, pp. 1–6, June 2009
25. Nguyen, K.C., Alpcan, T., Basar, T.: Stochastic games for security in networks with interdependent nodes. In: 1st International Conference on Game Theory for Networks, GAMENETS 2009, Istanbul, Turkey, May 13-15, 2009, pp. 697–703 (2009)
26. Patcha, A. Park, J.: A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. In: Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, pp. 280–284, June 2004
27. Pillai, P.S., Rao, S.: Resource allocation in cloud computing using the uncertaintyprinciple of game theory. IEEE Syst. J. **10**(2), 637–648 (2016)
28. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A survey of game theory as applied to network security. In: 2010 43rd Hawaii International Conference on System Sciences, pp. 1–10, January 2010
29. Shahzad, F.: State-of-the-art survey on cloud computing security challenges, approaches and solutions. Proc. Comput. Sci. **37**, 357–362 (2014). The 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2014)/The 4th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2014)/Affiliated Workshops
30. Simmon, E., Bohn, R.B.: An overview of the NIST cloud computing program and reference architecture. In: Concurrent Engineering Approaches for Sustainable Product Development in a Multi-Disciplinary Environment - Proceedings of the 19th ISPE International Conference on Concurrent Engineering (ISPE CE 2012), Trier, Germany, 3–7 September 2012, pp. 1119–1129 (2012)
31. Takabi, H., Joshi, J., Ahn, G.-J.: Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. **8**, 24–31 (2011)
32. 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)

33. Wang, Y., Wang, Y., Liu, J., Huang, Z., Xie, P.: A survey of game theoretic methods for cyber security. In: 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), pp 631–636, June 2016
34. Xiaolin, C., Xiaobin, T., Yong, Z., Hongsheng, X.: A Markov game theory-based risk assessment model for network information system. In: 2008 International Conference on Computer Science and Software Engineering, vol. 3, pp. 1057–1061, December 2008
35. Xu, X., Yu, H.: A game theory approach to fair and efficient resource allocation incloud computing. Math. Probl. Eng. **1–14**(04), 2014 (2014)