A Game Theoretic Framework for Cloud Security Transparency

Abdulaziz Aldribi, Issa Traore

The Department of Electrical and Computer Engineering,
University of Victoria, Victoria, Canada
aaldribi@uvic.ca
itraore@ece.uvic.ca
www.isot.ece.uvic.ca

Abstract. Over the past few years cloud computing has skyrocketed in popularity with the IT industry. Connected to this growing popularity is an increasing level of concern over the security of the cloud computing infrastructure. Despite this concern, cloud providers do not disclose any information about their security precautions. With no information on the security precautions, a provider's clients cannot be certain that their applications are safe from attack. Furthermore, clients are not granted access to the network level of the system to implement any of their own security features.
In this paper we approach cloud security transparency constraints from a game theoretic perspective. Specifically, we model the security transparency problem as a dynamic non-cooperative game theoretic problem, whereby the provider and client are modelled as the players in the game. A theoretical analysis through which the provider or client can compute his/her best strategy to reach the Nash equilibrium is presented.

Keywords: Cloud Computing; Cloud Security; Transparency; Game Theory.

1 Introduction

Cloud computing solutions are rapidly increasing in popularity within the IT industry. However, security still remains a major concern for cloud adopters and potential clients [1]. Despite the great level of concern for security, most cloud providers offer little to no assurance of precautionary measures to their clients. The reason may be the opposing interests of the provider and the client with respect to security transparency. For the provider, increasing security transparency essentially means making their security implementations more visible to the client [2]. Transparency poses problems for the provider. For instance, if a client has malicious intent, they would have detailed knowledge of the system. Providers often service multiple clients on a single server; providers will not disclose any information to one client that could compromise the others. This poses the question of how clients can trust their provider's security setup with such

little information on it. If a client has customers, and is responsible for their sensitive information, the client cannot reassure their customers of the security precautions taken by the provider without any information.

In this paper, we employ game theory to investigate analytically and help formulate and analyse approaches to security transparency in cloud computing. In particular, we present a theoretical model through which the client and provider can compute their best strategy to reach the Nash equilibrium to enter into a contract. To our knowledge this is the first work in the literature that applies game theory to decision making to solve the security transparency issue of contracts.

The rest of the paper is sectioned as follows. A coverage of related work is given in Section 2. Section 3 reflects on the motivation behind this paper based on a theoretical gaming approach to security transparency in cloud computing, and it presents the analytical results. Finally, the paper's conclusion is provided in Section 4.

2 State of the Art

Despite no directly related work to security transparency in cloud computing, there have been multiple attempts to improve it. We list two examples of these attempts. The first allows the clients to conduct limited cloud monitoring and penetration testing on the VM they are deployed on. The second example takes the approach of suggesting security disclosure principles for the initial contract between a provider and a potential client. By disclosing limited security information, hopefully a potential client would be satisfied with the precautions a provider has taken.

2.1 Amazon Web Services

Amazon Web Services (AWS) has recognized the problem in security transparency between client and provider and have made strides towards limited network monitoring for their clients. If a client submits a formal request, AWS will allow limited penetration testing. To do this AWS requires the client submit a start and end date of their testing, only use approved testing tools,and not impede the performance of the resources, since they are sharing them with other clients [3]. Another option that AWS offers for monitoring is called "Cloud Watch". Cloud Watch is an Amazon developed tool that allows clients to monitor their VMs' resource usage and other customizable metrics. Cloud Watch is a subscription based tool which charges by the hour or per metric [4].

2.2 Sun Microsystems

In 2009, Sun Microsystems published a paper on "Cloud Computing with Transparent Security" [5]. In the paper, Sun proposes implementing a certain set of

transparency standards that a provider must meet in their initial sign up contract. Sun recommends that the provider disclose common security policies and practices but withhold details of their architecture. In the paper, they also recognize some key benefits of increasing security transparency:

- improved trust from the client, potentially resulting in faster adaptation
- helps provider to better understand and manage customer expectations related to security
- educe the amount of time and resources spent, by the provider, reassuring clients of potential risks (eg: AWS frequently needs to respond to client requests for penetration testing)

Although this idea gives a good basis for the initial contract, we believe that it would not increase transparency enough to give client's peace of mind. The only way for a client to fully trust a provider's security setup is to allow them to implement or control a portion of it.

3 Analyzing Transparency Constraints Using Game Theory

Game theory as a mathematical notion provides a set of tools to analyse and model interactive decision making situations between agents with conflicting interests. It is also defined as the study of how the ultimate result of a competitive circumstance is decided on by the action of the players involved in the game, based on the purposes and preferences of these players, and on the strategy that is used by each player [6]. In this section we take advantage of Game Theory to obtain the best security transparency decision in Cloud Computing.

In subsection 3.1, the importance of security in cloud computing for both provider and client is discussed using game theory. The interaction between the provider and the client regarding transparency in cloud security is presented in subsection 3.2. The concept of Nash equilibrium is presented in subsection 3.3 for transparency in cloud security and we address how game theory can help decision makers with that. This section closes with subsection 3.4 by studying the effect of mixing a game strategy if it is used to sign the contract between provider and client if the provider is willing to ensure transparency to the client.

3.1 Dominance "from Prisoner's Dilemma Game [7]"

In game theory, a game (G) contains three components (P,S,U), where P is the set of players, S is the set of strategies, and U is the set of payoff functions. In the game in this section all players are assumed to be rational, which means their choice will be according to the outcome they prefer most since they know their opponent's choice. There are two strategies for every player, X and Y; strategy X is said to dominate strategy Y if the outcome resulting from X is better than the outcome resulting from Y. Therefore, since all players are rational they will never choose to play a dominated strategy. Discovering which strategies dominate will

lead the rational player to choose only one of their strategies.
This example illustrates the dominant strategy, and it has been presented here to show how security is very important for both the cloud provider and client to enter into a contract:
Player 1 (P_1) : is a cloud provider
Player 2 (P_2) : is a client
Provider offer $\rightarrow (High, Low)$ Security
Client will $\rightarrow (Buy, Don't\ buy)$
They are considering entering into a contract from a cloud service for a period of time. The cloud service provider has two security level options to provide to the client: High or Low. A low security option is not a viable option for the provider since the chance of breaching security is high and that will cost too much if it happens. High security is the only desirable option for the client, thus the contract will not be signed if the provider chooses to provide a cloud service with low security. The client has to choose 'Buy or Don't buy' according to the level of security that is provided by the cloud service provider. However, the level of security put into the contract cannot be verified by the client.

Table 1. Dominance strategy: High - Low security game between a cloud provider P1 and a client P2

P_1 \ P_2	Buy	Don't Buy
High	A,a	A,b
Low	B,c	C,a

The payoff matrix of the game's dominance strategy is shown in Table 1 for two different types of strategies, where the following variables are defined:

- A and a represent the most preferred outcome for P_1 and P_2, respectively;
- B and b represent the second most preferred outcome for P_1 and P_2, respectively;
- C and c represent the least preferred outcome for P_1 and P_2, respectively.

In the matrix, the possible payoffs for P_1 and P_2 are presented as variables to show it in a general form. Player 1 chooses a row, either High or Low, and Player 2 chooses one of the columns Buy, Don't buy.
In this example "High" is a strategy that dominates the "Low" strategy for the cloud provider. Regardless of whether the client chooses to buy or not, the provider always prefers to provide high security protection. Therefore, since the client believes that the cloud provider is rational and always prefers a High security level, they will choose buy and enter into a contract with the cloud provider. Therefore, "Buy" is a strategy that dominates the "Don't buy" strategy for the client.
In the remainder of this section we will formulate the game and present the

expected utility for both the cloud provider and client if they would like to sign a contract. If (P_1) chooses "High" the payoff will be (A) and if the client chooses "Buy" which dominates "Don't buy", then the payoff for both provider and client is (A,a), resulted from playing (High,Buy) strategies , which always dominates "Low, Don't buy" strategies.
In this example "High" strictly dominates "Low" for (P_1) and "Buy" strictly dominates "Don't buy" for (P_2). Here we can see what the expected utility is for both the cloud provider and client if they would like to sign a contract, and what is best for them.The first two equations are the expected utilities for client if buys the service or not:

$$EU_{buy} = 0.5 \times a + 0.5 \times c \tag{1}$$

$$EU_{Don't\ buy} = 0.5 \times b + 0.5 \times a \tag{2}$$

The folowing equations are the expected utilities for provider if provides High or Low security

$$\begin{aligned} EU_{high} &= 0.5 \times A + 0.5 \times A \\ EU_{high} &= A \end{aligned} \tag{3}$$

$$EU_{low} = 0.5 \times B + 0.5 \times C \tag{4}$$

Let σ donate the probability that a player plays a particular pure strategy, then we finds the expected utility if it provides High or Low security to the provider, and Buy or Don't buy for the client . The client's expected utility of playing "Buy" can be written as pure strategy as a function of the provider's mixed strategy:

$$EU_{buy} = \sigma_{high} \times a + \sigma_{low} \times c \tag{5}$$

The client's expected utility of playing "Don't buy" as a pure strategy is :

$$EU_{Don't\ buy} = \sigma_{high} \times b + \sigma_{low} \times a \tag{6}$$

Now we are looking for a mixed strategy from the provider that leaves the client indifferent situation between his/her pure strategies. In other words, we want to find σ_{high} and σ_{low} such that:

$$EU_{buy} = EU_{Don't\ buy} \tag{7}$$

This implies the following:

$$\sigma_{high} \times a + \sigma_{low} \times c = \sigma_{high} \times b + \sigma_{low} \times a \tag{8}$$

And since

$$\sigma_{high} + \sigma_{low} = 1 \tag{9}$$

then

$$\sigma_{low} = 1 - \sigma_{high} \tag{10}$$

We get

$$\begin{aligned} \sigma_{high} \times a + (1 - \sigma_{high}) \times c &= \sigma_{high} \times b + (1 - \sigma_{high}) \times a \\ \sigma_{high} \times a + (c - c \times \sigma_{high}) &= \sigma_{high} \times b + (a - a \times \sigma_{high}) \\ 2 \times a \times \sigma_{high} - c \times \sigma_{high} - b \times \sigma_{high} &= a - c \end{aligned} \tag{11}$$

$$\sigma_{high} = \frac{a - c}{(2a - c - b)} \tag{12}$$

By substituting σ_{high} into $\sigma_{high} + \sigma_{low} = 1$ we get

$$\sigma_{low} = 1 - \left(\frac{a - c}{(2a - c - b)} \right) \tag{13}$$

So if the provider chooses high security with probability $\frac{a-c}{(2a-c-b)}$ and low with probability $1 - \left(\frac{a-c}{(2a-c-b)}\right)$then the client will earn the same payoff for selecting either to buy or not as a pure strategy.

Now it is possible to calculate a mixed strategy for the client that leaves the provider indifferent between his two pure strategies:

$$EU_{high} = \sigma_{buy} \times A + (1 - \sigma_{buy}) \times A \tag{14}$$

$$EU_{low} = \sigma_{buy} \times B + (1 - \sigma_{buy}) \times C \tag{15}$$

$$EU_{high} = EU_{low} \tag{16}$$

This implies

$$\sigma_{buy} \times A + (1 - \sigma_{buy}) \times A = \sigma_{buy} \times B + (1 - \sigma_{buy}) \times C \tag{17}$$

Which gives:

$$\sigma_{buy} = \frac{A - C}{B - C} \tag{18}$$

$$\sigma_{Don't\ buy} = 1 - \left(\frac{A - C}{B - C} \right) \tag{19}$$

So if the client chooses to buy with probability $\frac{A-C}{B-C}$ and not to buy with probability $1 - \left(\frac{A-C}{B-C}\right)$ then the provider is in-between providing high security and low security as a pure strategy.

3.2 Transparency in Cloud Security

In this example we apply the same previous game strategy to find out if the contract will be signed or not and whether the client requests security transparency from the provider. All players are assumed to be rational, which means their choice will be according to the outcome they prefer most since they know their opponent's choice.
The cloud service provider has two security transparency level options to provide to the client More or Less. The Less security transparency option is the preferable option for the provider since the main concern of the provider is to protect the cloud from any chance of breaching security. More security transparency is the only desirable option for the client who would like to protect his data from any security issues, thus the contract will not be signed if the provider chooses to provide cloud services with less security transparency. The client has to choose Buy or Don't buy according to the level of security transparency that is provided by the cloud service provider.

Table 2. Utility matrix of P_1 and P_2 dependent on the transparency level

P_1 \ P_2	Buy	Don't Buy
More	C,c	C,b
Less	B,c	A,a

Table 2 illustrats the outcome of the provider and client, if they sign or not the contract, depends on the transparency level. In this example "Less" is a strategy that dominates the "More" strategy for the cloud provider. Regardless of whether the client chooses to buy or not, the cloud provider always prefers to provide less transparency in the security for the client for protection reasons. And since the client believes that the cloud provider is rational and will always prefer less security transparency, then the client will prefer not to sign a contract with that provider. Therefore, the rationality of both players leads to the conclusion that the provider will provide less security transparency and as a result the contract will not be signed.

In this section we will formulate the game and present the expected utility for both the cloud provider and client if they would like to sign a contract.
The expected utility for the cloud provider is expressed as:

$$\begin{aligned} EU_{More} &= 0.5 \times C + 0.5 \times C \\ EU_{More} &= C \end{aligned} \tag{20}$$

$$EU_{Less} = 0.5 \times B + 0.5 \times A \tag{21}$$

And the expected utility for the client is given by :

$$\begin{aligned} EU_Buy &= 0.5 \times c + 0.5 \times c \\ EU_Buy &= c \end{aligned} \tag{22}$$

$$EU_{Don't\ buy} = 0.5 \times b + 0.5 \times a \tag{23}$$

By solving these equations, it is possible to figure out what the best for provider is to ensure high or low security transparency, and whether the best option for the client is to sign the contract(i.e. buy) or not.
Now let us use sigma (σ) to represent the probability that a player plays a particularly pure strategy.
Let us find the expected utility of providing more or less security transparency for the provider, and whether to sign the contract or not for the client.

$$EU_{Buy} = \sigma_{More} \times c + \sigma_{Less} \times c \tag{24}$$

$$EU_{Don't\ buy} = \sigma_{More} \times b + \sigma_{Less} \times a \tag{25}$$

We want to find σ_{More} and σ_{Less} such that:

$$EU_{Buy} = EU_{Don't\ buy} \tag{26}$$

This corresponds to:

$$\sigma_{More} \times c + \sigma_{Less} \times c = \sigma_{More} \times b + \sigma_{Less} \times a \tag{27}$$

And since

$$\sigma_{More} + \sigma_{Less} = 1 \tag{28}$$

Then

$$\sigma_{More} = 1 - \sigma_{Less} \tag{29}$$

Which implies:

$$(1 - \sigma_{Less}) \times c + \sigma_{Less} \times c = (1 - \sigma_{Less}) \times b + \sigma_{Less} \times a \tag{30}$$

This gives:

$$\sigma_{Less} = \frac{b - c}{a - b} \tag{31}$$

So if the provider chooses less transparency with probability $\frac{b-c}{a-b}$ and more transparency with probability $1 - \left(\frac{b-c}{a-b}\right)$, then the client will earn the same payoff for selecting either to sign or not to sign the contract.

3.3 Transparency in Cloud Security using Nash Equilibrium

From the previous examples, knowledge of the dominating strategies by players will give them advice on how the game could be played. However, this is not always the case with all games that they have dominating strategies, thus it will be difficult for players to play the game if there is not enough advice on all outcomes. Therefore, the players need a more general strategy, which is the main concept of Nash equilibrium. Nash equilibrium recommends an action profile for each player so that no single player has an incentive to deviate from its current optimal strategy and cannot obtain a higher payoff, assuming that each player follows the recommendation since both of them are rational [8]. From the previous example, we will examine the utility outcome for both provider and client if the provider is willing to provide more security transparency to the customer. Also, the client can change the game by giving him the right to cancel the cloud service contract if the security transparency is less than expected.

Table 3. Utility matrix of provider and client which leads to Nash equilibrium

P_1 \ P_2	Buy	Don't Buy
More	A,a	C,b
Less	B,c	B,b

Table 3 is the utility matrix of provider and client that shows the resulting game; it is clear that the most preferred outcome for both provider and client is for more security transparency to be provided and the contract to be signed by the client. Also, since the client has the opt out option in the contract, his or her second preferred outcome will be not to sign or even cancel the contract if the provider changes the transparency level.
In this game there is no dominating strategy for either the provider or client. Instead, there are two Nash equilibria: one of them is the strategy combination (less, don't buy). The second one is the strategy combination (more, buy); this strategy is in equilibrium since the player P_2 prefers to sign the contract when the transparency is more and player P_1 prefers to provide more transparency if the client will sign the contract. Both Nash equilibria are logical options for the provider and client on how to play the game. Since Nash equilibrium strategies are chosen by the players, they will rationally stay with their strategies and will not change.
Now, this game can be formulated and the expected utility presented for both the cloud provider and client if they would like to sign a contract. The expected utility for the cloud provider can be expressed as:

$$EU_{More} = 0.5 \times A + 0.5 \times C \tag{32}$$

$$EU_{Less} = 0.5 \times B + 0.5 \times B = B \tag{33}$$

And the expected utility for the client is given by:

$$EU_{Buy} = 0.5 \times a + 0.5 \times c \tag{34}$$

$$EU_{Don't\ buy} = 0.5 \times b + 0.5 \times b = b \tag{35}$$

By solving these equations, it is possible to figure out which options are the best for the provider and the client. For the provider, the choice will be between high or low security transparency,while for the client it will be about whether to Buy or Do not buy. Let us find the expected utility of providing more or less security transparency by the provider, and signing the contract or not by the client.

$$EU_{Buy} = \sigma_{More} \times a + \sigma_{Less} \times c \tag{36}$$

$$EU_{Don't\ buy} = \sigma_{More} \times b + \sigma_{Less} \times b \tag{37}$$

We want to find σ_{More} and σ_{Less} such that:

$$EU_{Buy} = EU_{Don't\ buy} \tag{38}$$

This corresponds to

$$\sigma_{More} \times a + \sigma_{Less} \times c = \sigma_{More} \times b + \sigma_{Less} \times b \tag{39}$$

And since

$$\sigma_{More} + \sigma_{Less} = 1 \tag{40}$$

We have

$$\sigma_{More} = 1 - \sigma_{Less} \tag{41}$$

Which gives:

$$(1 - \sigma_{Less}) \times a + \sigma_{Less} \times c = (1 - \sigma_{Less}) \times b + \sigma_{Less} \times b \tag{42}$$

By solving this equation we get

$$\sigma_{Less} = \frac{a - b}{a - c} \tag{43}$$

So if the provider chooses less transparency with probability $\frac{a-b}{a-c}$ and more transparency with probability $1 - \left(\frac{a-b}{a-c}\right)$,then the client earns the same payoff for selecting either to sign or not to sign the contract.

3.4 Transparency in Cloud Security using a Mixed Strategy

Not every game in strategic form always has a Nash equilibrium that makes each player definitely choose it. Therefore, the player may decide to choose one of these pure strategies randomly with certain probability. A mixed strategy is the idea that when the player randomizes his strategy selection, any finite strategic form of the game has equilibrium if a mixed strategy is allowed.
In this example, a mixed strategy is applied to transparency in cloud security, assuming that the cloud provider is willing to provide transparency in security to the client and the client will sign the contract. The main concern for the provider is that if the client performs malicious activities, they may attack the provider cloud or other client's services. Therefore, the provider would like to be sure that the client follows the regulations and does not intend to violate them. In this scenario the provider has two strategies, either to monitor (Moni) the client activities which will cost the provider, or to rely on the contract regulations (don't Moni) and assume that the client will not violate them. For client strategies, if he or she intends to carry out malicious activity (Malic) and gets caught by the provider, which will cost him or her too much by either paying money and/or being put in jail. The alternative for the client is to perform normal activities (denoted Nor).

Table 4. Utility Matrix for Mixed strategy

P_1 \ P_2	Nor	Mal
don't Mo	A,b	C,a
Mo	C,b	B,c

Table 4 shows the resulting game. The main difference in this game compared to the previous games is that this game does not have equilibrium in pure strategies. Since the most preferred outcome for provider comes from choice that is different from client choice (similarly for the client). Therefore they will not remain on one choice.
For example, if the provider chooses not to monitor the activities of the client, assuming that the client will be using the transparency features normally, now if the client chooses to behave normally the outcome will be in the provider's favour which is (A,b). However, if the client turns out to be an attacker and his or her activities become malicious, the provider will lose too much and the outcome will be on the side of the client (C,a). If the provider chooses to monitor and the client performs malicious activities, that will result in them getting caught by the provider and the outcome will be worse for the client (B,c).

By visiting all cases, the provider would strongly prefer for the client to behave normally and not perform or intend any malicious activities, but this is not always the case. Therefore, the provider will monitor the client's activities

if it is felt that the types of activities are risky. If the provider always chooses not to monitor the client's activities, then this will turn out to be a dominating strategy and the client will perform malicious activities which results in a unique equilibrium. From Table 4, this game has no equilibrium in pure strategies, since if the provider is not willing to change their choice and if it is not monitoring, the most preferred outcome for the client without doubt would be to perform malicious activities.

Since this game is a kind of a mixed strategy, the players should maximize their worst outcome against all possible choices of the other players. For example, a mixed strategy for the provider in this game is to monitor the client activities with a certain probability. This monitoring probability could be used to find out what will lead to equilibrium. If the probability of monitoring the client activities is very low, then the client will get outcome (b) for behaving normally, while a better outcome (a) will be gained if he or she changes their behaviour to be malicious. On the other hand, if the probability of inspection is much higher, then the expected outcome for the client if he or she behaves in a malicious way is the worst outcome (c), thus the client will behave normally to improve his or her outcome and become (b). If the provider knows when the client will be indifferent, this means they know when the client will possibly randomize between his or her strategies for behaving normally or maliciously, since both of these strategies give the same outcome.
In this last part, we will find the probability that makes the client indifferent.

$$EU_{Nor} = \sigma_{don't\ Mo} \times b + \sigma_{Mo} \times b \tag{44}$$

$$EU_{Mal} = \sigma_{don't\ Mo} \times a + \sigma_{Mo} \times c \tag{45}$$

We want to find $\sigma_{don't\ Mo}$ and σ_{Mo} such that:

$$EU_{Nor} = EU_{Mal} \tag{46}$$

This corresponds to:

$$\sigma_{don't\ Mo} \times b + \sigma_{Mo} \times b = \sigma_{don't\ Mo} \times a + \sigma_{Mo} \times c \tag{47}$$

And since

$$\sigma_{don't\ Mo} + \sigma_{Mo} = 1 \tag{48}$$

Then

$$\sigma_{don't\ Mo} = 1 - \sigma_{Mo} \tag{49}$$

Which implies:

$$(1 - \sigma_{Mo}) \times b + \sigma_{Mo} \times b = (1 - \sigma_{Mo}) \times a + \sigma_{Mo} \times c \tag{50}$$

This gives:

$$\sigma_{Mo} = \frac{b - c}{c - a} \tag{51}$$

So if the provider chooses to monitor the client activities with probability $\frac{b-c}{c-a}$ and does not monitor with probability $1-\left(\frac{b-c}{c-a}\right)$, then the client earns the same payoff for selecting either to behave normally or to perform malicious activities in the cloud or for other clients.

From all the previous case studies, techniques from game theory have been applied to help formulate and analyse the conflict between the cloud provider and client to reach an agreement, and for more transparency in security to be obtained by the client.

4 Conclusion

Security is one of the primary concerns with cloud computing. The provider that successfully assures clients that their applications are safe will be the provider that gains more clients. in this paper, techniques from game theory have been applied to help formulate and analyse solutions to security transparency that the provider could offer to the client, who would require more transparency in security to sign the contract. Moreover, through equilibrium analysis of the transparency security game, the provider can gain a deeper understanding of client strategies. As has been discussed in this article, the application of game theory with incomplete and imperfect information is an emerging field in security transparency in cloud computing, with no papers published so far.

From our research, it is clear that providers want to gain clients' trust. If clients trust their provider, they will recommend their provider. Building strong relationships between the clients and the provider is vital to cloud computing, and we believe this relationship can be achieved by giving clients a bigger sandbox to play in.

5 Acknowledgment

This research is supported by the Qassim University and the Ministry of Education of the Kingdom of Saudi Arabia.

References

1. Gens,F.:IT cloud services user survey.pt.2: Top benefits and challenges,IDC eXchange,(2008) http://blogs.idc.com/ie/?p=210
2. Pauley,W.A.:Cloud Provider Transparency: An Empirical Evaluation.In: Security and Privacy,vol.8, pp.32-39.IEEE Press(2010)
3. Penetration Testing, http://aws.amazon.com/security/penetration-testing/
4. AWS CloudWatch Cloud-based Server Monitoring,http://aws.amazon.com/cloudwatch/
5. Micro, S.: Building Customer Trust in Cloud Computing with Transparent Security. Sun Micro White Paper(2009)

6. Midha, S., Sharma, A. K.,sSikka, G.: A survey on wireless sensor network clustering protocols optimized via game theory,vol.11,pp.8-18. ACM SIGBED Review (2014)
7. Kreps, D. M., Milgrom, P., Roberts, J., Wilson, R.:Rational cooperation in the finitely repeated prisoners' dilemma.In: Journal of Economic theory,vol.27,pp.245-252.(1982)
8. Nash, J.: Equilibrium points in N-person games. In: Proceedings of the National Academy of Sciences,vol.36,pp.48-49 (1950)