Dynamic Scenarios of Trust Establishment in the Public Cloud Service Market

Soyoung Kim
Technology Opportunity Research Team
Korea Institute of Science and Technology Information
Seoul, Korea
e-mail: sykim8171@kisti.re.kr

Junseok Hwang, Jörn Altmann
Technology Management, Economics and Policy Program
Seoul National University
Seoul, Korea
e-mail: Junhwang@snu.ac.kr, jorn.altmann@acm.org

***Abstract*—The adoption of the public cloud by firms and individuals has been slowed because of the lack of trust. This research seeks the rules of trust establishment between the public cloud providers and users through signaling game theory, analyses dynamic scenarios in which the pervasive distrust arises, and suggests policy guidelines. The theoretical analysis results suggest that the most critical task is to make a pool of trustworthy public cloud service providers to establish an efficient market. The results also show that prudent policy design is desirable. Specific case studies and simulations will be conducted as further studies.**

Keywords-public cloud computing; trust; signaling; equilibrium; dynamic.

I. INTRODUCTION

The public cloud has been a valuable tool for firms and individual users to reduce their Information Technology costs. A number of public cloud services such as Amazon's AWS or HP's cloud service have been launched. Even telecom vendors, contents providers, web portals and small Information Technology solution vendors are participating in the race between public cloud services. A few companies have been started to compete on price as competition has intensified [1].

However, the users may not select a cloud service only by its price and performance. The criteria for selecting a cloud service are not only these two factors. Trustworthiness and reliability are also important criteria for selecting a cloud service. Therefore, the establishment of trust is one of the major challenges for the growth of the public cloud market [2]. The users' concerns about security and privacy threats hinder the diffusion of the public cloud [3]. The public cloud market now needs policy solutions to address the users' concerns rather than technological solutions [4].

This study analyses, with game theoretical insights, the process of trust establishment and distrust pervasiveness when users select a public cloud service. In particular, the signaling game is adopted to find several types of the equilibrium and to analyze several dynamic paths from equilibrium. Policy guidelines are also discussed with the dynamic scenarios.

The remainder of the paper is organized as follows. The next section reviews the related literature. Section III proposes the trust signaling game in the public cloud market. Section IV investigates the dynamic scenario of trust establishment. Section V suggests preliminary results and discussion. Finally, Section VI provides a conclusion and a future work.

II. LITERATURE REVIEW

Research on trust establishment and management related to cloud services has increased as more kinds of cloud computing have been provided to personal users and private companies. Researchers have focused on the issues of possible risks and threats, such as data loss and personal information disclosure [3]. Some researchers have pointed out that these risks and threats to security and privacy had slowed down the adoption of cloud computing services [5]. Some researchers have proposed identity management and authentication systems [6] for mitigating those risks and threats or have suggested a reputation mechanism based on a trust management framework [7].

Research on trust management related to network based transactions between unknown users has a history of decades [8, 9]. These trust management frameworks mostly have their theoretical background in game theory, particularly 'the prisoners' dilemma' [10].

Another type of game, 'the signaling game [11]' would be useful to analyze the process that could help a user select the most trustworthy (or productive) provider among several of them, especially when information asymmetry exists between a user and a provider so that a user cannot know the exact type of a provider. Several studies adopted the signaling game to develop the autonomous agents' strategies for selecting their partners on a network [12, 13]. Most of these studies focused on finding the best strategy of an individual agent rather than finding policies that make a socially efficient equilibrium.

A particular piece of research in the political science field adopted the signaling game to analyze the dynamics of general trust in society [14]. It showed how society's trust tends to oscillate between high and low levels in the long run. However, the study more focused on scrutinizing in the cycles of the general trust levels in a society rather than finding a solution to address problems of pervasive distrust.

Based upon previous research, this paper focuses more on finding policies and solutions to make a socially efficient equilibrium and to address an emergence of generalized distrust.

 ISBN: 978-1-61208-216-5

III. TRUST SIGNALING GAME IN THE PUBLIC CLOUD MARKET

Recently, the public cloud service market has had a number of providers, so it is almost a competitive market. Vendors try to increase the probability of being selected by users through advertising their performance, service prices, or trustworthiness. Users make their decisions based on these signals from vendors. This section firstly investigates the criteria for the existence of a stable equilibrium when a number of providers and users send and receive signals and make partnerships.

A. Process of Trust Establishment

The criteria for selecting partners for users are price, performance, trustworthiness, and so on. This theoretical analysis focuses on trustworthiness.

The process of trust establishment has roughly three steps [15]. The first step is when the market initiates before the trust develops concretely. A user faces the signaling game situation in which a user meets an unknown cloud service provider. The provider sends a characteristic signal to the user and the user makes a decision of selecting a partner by investigating the provider's signals with proper price. Then the connected partners transact or communicate.

The second step is the process of trust formation. As the first step is repeated, the transaction history and a trust relationship are accumulated. The total trust level of the market can increase or decrease with specific paths of trust formation.

The third step is the steady-state. Once the trust establishment reaches a stable equilibrium, a small loss or disturbance of trust cannot affect the equilibrium. This study focuses on what factors make a successful path from the second step to the third step and what factors make the transition a failure.

B. Fundamental Rules of Trust Establishment

In the first step, a service provider intends to increase the probability of being selected by users by signaling his/her trustworthiness in various ways. Simultaneously, a user observes those signals and decides whether or not to trust the provider. Our previous work briefly analyzed this signaling game model and suggested three propositions about signaling cost structures and market environment conditions in network based transactions [16].

Service providers, or cloud providers in this case, are divided into two types. One type is the good provider who observes the promised rules and the other type is the bad provider who violates the rules or does damage to the partner. The proportion of bad type providers in the total provider population is denoted by π_B ($0 \le \pi_B \le 1$). A provider sends signal e ($0 \le e \le 1$) to users, and a single signal costs c(e).

Users are all the same type. A user receives a signal from a provider, examines the signal, estimates the type of the provider, and suggests a charge for the trustworthy transaction, w(e).

Once the partner and the charge are determined and the transaction conducted, the payoff for the user is subsequently fixed. The payoff for a user varies with the type of partner. If a user meets a good type provider, the user receives the proper value of cloud service, v ($v \ge 0$) and the provider also receives the proper payoff, v. However, a bad type partner does not deliver the proper value of cloud service and does damage to the user with an amount of 'L' ($L \ge 0$). Therefore, the bad type provider extort the payoff v and the additional value L from the user. What is important here is that the user cannot be aware of the type of his/her partner.

The total expected utility for the bad type provider is determined by the following equation: $u_B(e)=v+L+w(e)-c_B(e)$ and the for good type provider is determined by the following equation: $u_G(e)=v+w(e)-c_G(e)$.

Without a signal, the user suggests the fee to the unknown provider for the cloud computing service as the following equation: $\bar{w} = -\pi_B(v+L)+(1-\pi_B)v = v-\pi_B(2v+L)$. This means the expected payoff for a single transaction.

In this model, the following three propositions are concluded.

- Proposition 1. (The separating equilibrium) When the level of trustworthiness of a participant is used as the signal, the signal can be effective in distinguishing one provider from another, assuming the cost of the trust level signaling is sufficiently distinct from each other.
- Proposition 2. (The pooling equilibrium) The equilibrium in which the two types of providers select the same trustworthiness level as a signal is not stable if the signaling cost structure is distinct.
- Proposition 3. The effectiveness of the trustworthiness level signaling depends on the proportion of bad type participants in the market.

For example, if the trust signaling cost of the bad type provider is $c_B(e)=e$ and the cost of good type provider is $c_G(e)=\gamma e$ ($0<\gamma<1$), the user distinguishes the good type provider from the bad type provider with only their signals, as long as the equilibrium signal e* falls into the following range in Equation (1). In this equilibrium the good type provider selects e=e* and the bad type provider selects e=0.

$$v \le e^* \le \frac{v}{\gamma} \tag{1}$$

If two types of provider select their signals in the range of Equation (2), they can select the same level of signal as equilibrium. However, it is an unstable state.

$$e^* \le v - \pi_B(2v+L) \tag{2}$$

Proposition 3 means that the costly signaling regime is useful only if the proportion of bad type providers falls into the range of Equation (3).

$$\gamma\frac{v}{2v+L} < \pi_B < \frac{v}{2v+L} \tag{3}$$

 ISBN: 978-1-61208-216-5

IV. DYNAMIC SCENARIO OF TRUST ESTABLISHMENT

The trust signaling game described in Section III is a static and single round situation. The second process of trust establishment is a dynamic process in which the trust relationships stay in equilibrium or leave it.

A. Potential for a Pareto Improvement in the Equilibrium

When the separating equilibrium has been reached, the equilibrium signal of a good type provider is e* and the signaling cost is γe. A bad type provider does not send a signal and pay any cost. In a dynamic situation, bad type providers gradually leave the market and the ratio of bad type providers, π_B, decreases.

If π_B decreases down to this level, good type providers have incentives to lower their signaling costs so that increases the total payoff. In terms of individual rationality, the expected payoff of a good type provider if he/she decides not to send a signal in this situation is shown in the following Equation (4).

$$u_G(e)|_{e=0} = 2v - \pi_B(2v+L) \quad (4)$$

The expected payoff of Equation (4) is more than 2v-γe*. There is potential for a Pareto improvement when π_B decreases gradually. It means that the expected payoff of one player can increase without decrease of the other's expected payoff. It reaches the Pareto efficient state when π_B finally falls to zero. However, users stay with the same payoffs because of the assumption of the zero profit condition.

The situations where providers and users believe each other to conduct themselves properly and choose each other as partners make the transactions and communications more efficient. This is the benefit of an economy of trust.

B. The Countinuous Needs of Costly Signals

The Pareto optimum described in the previous subsection is not stable, because a good type provider can become a traitor or change his/her type in the real world market. Or, a newcomer provider of bad type can enter the market.

When a single bad type provider appears in the market with no signaling, π_B turns into a higher value than zero. This traitor or newcomer can gain a higher payoff than any other good type providers with an amount of 'L'. The users lose their payoff by the same amount. The sum of payoffs of all market participants does not change; however the share of users transfers to the share of traitors or newcomers.

Once this transformation happens, users calculate the proportion of bad type providers again, and introduce the price related to the proportion, and finally the market adopts the costly signaling regime.

C. The Dynamics of the Trust Equilibrium Shift

The last situation of dynamic trust transition is when the proportion of bad type providers exceeds the range defined by the third proposition of Section III. The separating equilibrium with costly signaling is in stable equilibrium; therefore users can still distinguish a good type provider from a signal only if the value of πB is in the range defined by Equation (3). When the damage from a bad type provider's behavior increases exceptionally, the separating equilibrium in which the two types of providers select the different trustworthiness level as a signal fails to stay stable. Figure 1 illustrates the relationship between the dynamic states of trust establishment and the proportion of bad type providers. Part (a) indicates the possible region of separating equilibrium, part (b) is the transition region of separating equilibrium and non-signaling pervasive trust and (c) is the market reduction region.

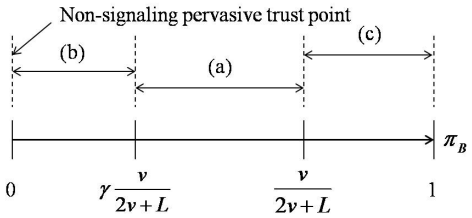

Figure 1. Dynamic states of trust establishment

V. SIMULATION DESIGN AND DISCUSSION

The dynamics of trust can be more clearly understood with a simulation based on parameters which reflect the market conditions in the real world. Figure 2 shows the causal loop diagram of a dynamic model of trust establishment in the public cloud service market. The proportion of bad type providers, π_B, is the most central variable which affects many other variables and receives feedback. This variable can be controlled by these exogenous variables which are denoted by 'E' with policy decisions.

The ratio of a good type provider's signaling cost to a bad type provider's cost, γ, affects the signaling costs of two type providers and the levels of signals are affected by these costs. The probability of being selected by a user and the signaling cost affect the utility of a provider as well as the non-signaling price, $\bar{w}$. The utility of a provider affects the entrance and leaving rate of a provider. The amount of damage from misbehavior by a bad type provider, L affects the utility of a bad type provider

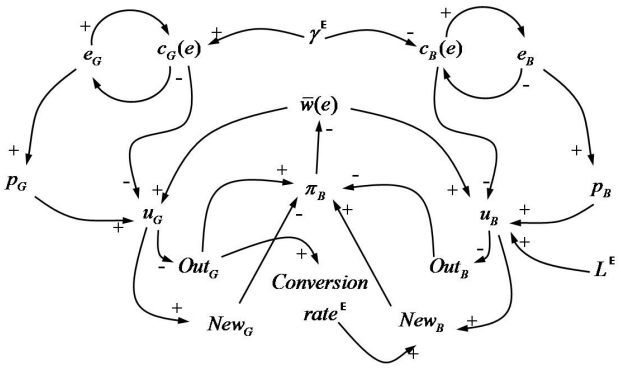

Figure 2. The causal loop diagram of a dynamic model of trust establishment in the public cloud service market

The results of designed simulation is expected to show the quantitative relationship between the variables which are illustrated in the Figure 2.

It is obvious that non-signaling pervasive trust is the optimal state of the market. The second best state is when users can easily distinguish the good type providers with signaling in the separating equilibrium. The best or second best states can be realized by prudent policy design which can control several related variables in the causal loop diagram.

The basic condition is to increase the signaling cost for bad type providers more than for good type providers. Reputation based mechanisms or third party authorization mechanisms can be possible methods to increase the signaling cost of a bad type provider.

If the costly signaling is maintained after most of the bad type providers have retired, the conversion of good type providers into bad ones or the entrance of new bad type providers can be blocked. However, costly signaling is inefficient when the proportion of bad type providers is substantially low. Then, it is worth considering the community of good type providers or their agreement for an efficient market. Either monitoring and penalty contracts or agreements have to exist in such communities [17].

VI. CONCLUSION AND FUTURE WORK

The fundamental rules and dynamic scenario of trust establishment are important factors that should influence the decision makers in the industry sector or a government which intends to promote the public cloud service market.

The theoretical analysis results of this research suggest that the most critical task is to make a pool of trustworthy public cloud service providers to establish an efficient market. The results also show that prudent policy design, which makes signaling costs different for different types of providers is desirable. It also shows that even in a trustworthy market, minimum monitoring and penalty contracts are needed and individual users have to invest in security at an optimal level.

Future work will verify the theoretical model of this paper with simulations and specify the dynamic scenarios of trust establishment and transition with several case investigations into various types of cloud computing services. In particular, the presented causal loop diagram will be validated and its parameters will be examined.

ACKNOWLEDGMENT

This research was supported by the KCC (Korea Communications Commission), Korea, under the CPRC (Communications Policy Research Center) support program supervised by the KCA (Korea Communications Agency). (KCA-2012-(11-941-1-005))

REFERENCES

[1] Larry Dignan, Cloud's price race to zero: Microsoft cuts Azure pricing, eyes Amazon, article of www.zdnet.com, March 9, 2012. http://www.zdnet.com/blog/btl/clouds-price-race-to-zero-microsoft-cuts-azure-pricing-eyes-amazon/71246

[2] S. M. Habib, S. Ries, and M. Mühlhäuser, "Cloud Computing Landscape and ResearchChallenges regarding Trust and Reputation," in Symposia and Workshops on Ubiquitous, Autonomic andTrusted Computing, Xi'an, China, 2010, pp. 410–415.

[3] S. Pearson, "Taking account of privacy when designing cloud computing services." In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, May 2009, pp. 44-52.

[4] M. Nelson,"The Cloud, the Crowd, and Public Policy," Issues In Science And Technology, vol. 25, no. 4, 2009.

[5] H. Takabi, J.B.D. Joshi and G.J. Ahn. "Security and Privacy Challenges in Cloud Computing Environments." IEEE Security & Privacy, vol. 8, no. 6, 2010, pp. 24-31.

[6] L. Yan, C. Rong, and G. Zhao. "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography,". In The First International Conference on Cloud Computing, pp. 167–177, 2009.

[7] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," IEEE Int'l Conf. Dependable, Autonomic, and Secure Computing (DASC 09), IEEE CS Press, 2009.

[8] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," working Paper for the NBERWorkshop on Empirical Studies of Electronic Commerce, 2000.

[9] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis. Support Syst. Vol. 43, 2007, pp. 618–644.

[10] R. Axelrod, The Evolution of Cooperation, Basic Books: New York, 1984.

[11] A. M. Spence, (1973). "Job market signaling," Quarterly Journal of Economics, vol. 87, no. 3, pp. 355–374.

[12] A. Lopez-Paredes, M. Posada, C. Hernandez, and J. Pajares, "Agent based experimental economics in signaling games in Complexity and artificial markets," Lecture Notes in Economics and Mathematical Systems, vol. 614, 2008, pp.121–129.

[13] A. Patcha and J. Park, "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks, " International Journal of Network Security, vol.2, no2, 2006, pp.131–137.

[14] T. Ahn, and J. Esarey "A Dynamic Model of Generalized Social Trust," Journal of Theoretical Politics, vol. 20, no. 2, 2008, pp. 151–180.

[15] M. Head, and K. Hassanein, "Trust in e-Commerce: Evaluating the Impact of Third-Party Seals", Quarterly Journal of Electronic Commerce, vol. 3, no. 3, 2002, pp. 307-325.

[16] S. Kim, and J. Hwang, "Theoretical Analysis and Simulation to Investigate the Fundamental Rules of Trust Signaling Games in Network-based Transactions", The Third International Conference on Future Computational Technologies and Applications, 2011.

[17] J. Hwang, S. Kim, H. Kim and J. Park, "An optimal trust management method to protect privacy and strengthen objectivity in utility computing services," International Journal of Information Technology & Decision Making, vol. 10, issue 02, 2011, pp. 287-308.

 ISBN: 978-1-61208-216-5