

Cloud Service Trust Model and Its Application Research Based on the Third Party Certification

Haiyong Xu¹, Junhai Ma¹ and Lei Li, Xueli Zhan^{1,2}

¹College of Management Economic, Tianjin University, Tianjin 300072, China

²School of Economics, Beijing Wuzi University, Beijing 101149, China

Email: lzqsly@126.com, mjhtju@aliyun.com, cghnju@aliyun.com

Abstract

With the development of computer and Internet technology, the concept of cloud computing has been accepted by related industries worldwide, especially on the development in the field of telecommunications and electronic commerce field rapidly. This paper introduces the meaning, characteristics of cloud computing, advantages and service pattern, and with the introduction of technology development present situation and the crisis of confidence by the cloud computing, describes the safety bottleneck problems faced in the promotion process of the cloud calculation. This paper presents cloud service trust model based on third party certification, and then through the analysis and study of the model, describes the security situation in the presence of third party certification body under the condition of cloud services, the Nash equilibrium solution; and the general cloud computing and e-commerce trust system were compared, the third party authentication mechanism can effectively play its advantages in supervision, has the huge influence of credit risk rating on its own transactions and future credit decision.

Keywords: Cloud Computing, The Third Party Certification, Game Theory, Nash Equilibrium

1. Introduction

Late 90's of the 20th century the rapid development of Internet, enterprises and individuals for data processing and storage, online transaction services business has put forward higher requirements, in order to meet the needs of people's needs and development, Internet Co invented the cloud computing technology, based on the large-scale computing problems also reduces the cost of computing become, Yu Shiyun another innovation of the information industry in 2003.

After years of development, the United States National Institute of standards and Technology (NIST) in 2011, gives the definition of cloud computing is the authority of the official, cloud computing is a pay per use pattern, this pattern available, convenient, on-demand network access to computing resources, configurable shared pool (resources including network, servers, storage, applications, services), these resources can be provided, only small investment management, or very little interaction with the service provider. And, NIST, cloud computing is divided into the following three levels of service mode, namely SaaS (Software as a Service, software as a service), PaaS (Platform as a Service, platform as a service) and IaaS (Infrastructure as a Service, infrastructure as a service).

As can be seen, cloud mainly involves two aspects, one is the infrastructure of cloud computing, which provides users with a more perfect system platform; the two is the application of cloud computing, which maximize the use of existing resources and cost savings.

The cloud infrastructure can be built on top of a large number of cheap server cluster, the redundancy among numerous servers, software can achieve high availability, so

compared with the traditional mainframes, the cloud to save the high cost, has an obvious advantage. And cloud computing using the underlying structure and application form of cooperation, to maximize the use of existing resources. Overall, cloud computing has the following three main features.

Cloud computing technology can according to the actual needs of users will be dynamic planning of physical and virtual resources.

Cloud computing has virtualization technology, can be used to compute resources in different regions of the summary, the effective realization of sharing all kinds of resources based on the platform.

Cloud computing is different with previous computing is that the user in the use of more convenient, fast and low cost.

In conclusion, the cloud of comprehensive application of distributed computing, Internet and large-scale resource management and information technology (as shown in Figure 1), including data center management, resource virtualization, massive data processing, computer security related issues, which belongs to the comprehensive system engineering.

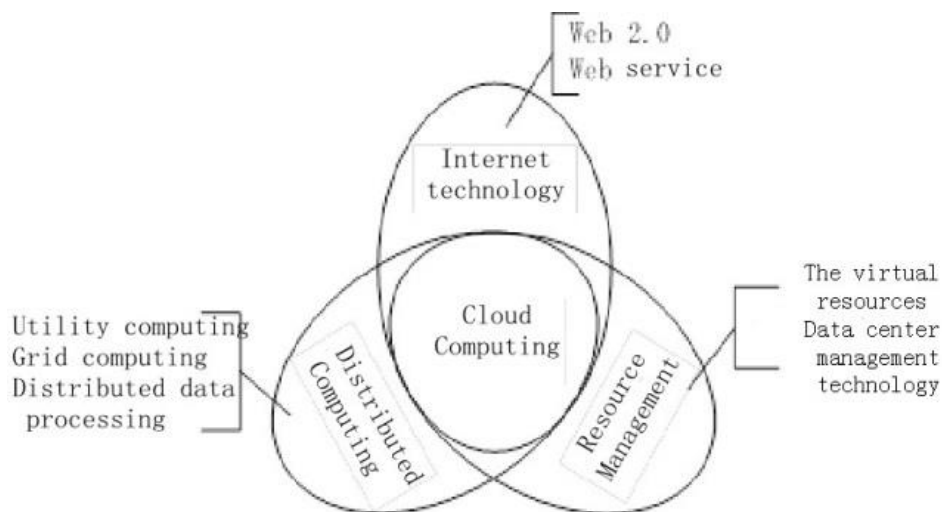


Figure 1. The Relationship Between Cloud Computing And Related Technology

2. Advantage of Cloud Computing

Compared with the traditional IT technology, cloud computing technology has the advantage.

2.1 Improve Resource Utilization

Cloud computing technology has virtualization technology is powerful, it can be a virtual server into multiple, can also be a number of physical IT resources are integrated into a virtual pool of resources, the effective realization of the flexible allocation of resources according to the user demand, improve the utilization efficiency of resources.

2.2 The Effective Realization of Automatic Operation

Cloud computing center is equipped with automatic scheduling of resources system, by monitoring the CPU, memory, I/O, storage and other functions, can realize the automatic deployment of resources to provide timely and perfect service for the user.

2.3 With Elastic Computing and Storage Capacity

Because the computing platform is used in the vertical expansion of the traditional way, so the computing and storage capacity is not flexible enough, cannot meet the demand of computing and storage of sudden. At the same time, the traditional computing platform can meet the demand is limited, the use of planning, construction, operation resources generally low rate. However, cloud computing is used in expanded mode transverse; greatly promote the flexibility of resource utilization.

2.4 Reduce the Terminal Request of User

An important feature of cloud computing services is, only need to pay a fee to acquire resources, computation required by network service. With internet access, cloud computing can set the complex computing tasks on the server, and simple interface can be standardized can enjoy cloud services.

3. Cloud Computing Development Present Situation and the Crisis of Confidence

3.1 The Development Status of Cloud Computing

Cloud computing is the foundation of related technology in cluster computing, utility computing, grid computing, service computing and so on, a new technology to produce the evolution, the. Cloud computing is a great innovation of information industry.

In 2007, Stanford University and many other famous American universities began to cooperate with Google, IBM, IT enterprise, joint research and development of cloud computing technology. With the deep research of scholars, academic circles in the cloud computing related to find more and more field, many research achievements have been published in academic journals and their International Conference on computing technology, gratifying achievements. And in the Eucalyptus and other open source cloud computing platform, cloud computing technology obtained the better popularization and application.

At the same time, research and development of each IT industry leading enterprises are also in the cloud computing technology has made the results attract people's attention. In addition, many countries in the world are the same in cloud computing research and application fields of invested a lot of manpower, material and financial resources, and the development of cloud computing as a strategic period of development in the future. For example, the United States government has established the application of cloud computing technology in the federal government's website. Save the money for the government; the British government has established a national platform for Cloud Computing (G-Cloud), and about 66.7% of British companies used a cloud computing service, which provides technical support for the development and innovation of each enterprise; China will cloud computing development included in the "Twelfth Five Year" plan, and start from the developed Shanghai, Beijing, Shenzhen City, in telecommunications, petroleum and petrochemical, transportation and other industries as a pilot, for the development of cloud computing service innovation demonstration work gradually, has greatly promoted the development of national information.

3.2 The Trust Crisis of Cloud Computing Faced

In the information age brings us convenient at the same time, also bring unpredictable challenges, information security is one of the biggest challenges.

Cloud computing brings hitherto unknown change to its unique advantages for the IT industry. Cloud computing applications rely on the powerful cloud platform to ensure that the service flexibility, but the infrastructure for each application is not fixed, which makes

the system difficult to maintain the user's data security and privacy. At the same time, the related resources provide cloud services unified storage in a pool of resources, by multiple managers to supervise, it is impossible to implement unified security management or establishment of safety protection measures and perfect. The cloud platform processing massive data computation and storage tasks all the time, the need for strong security measures to protect the massive information processing needs. Because of the lack of time for cloud computing research field of information security, has not formed the theoretical basis and establishing and maintaining the required information security and related technology products.

Cloud computing in the majority of people is the main form of the future to provide network services. However, the study on cloud computing is still facing many difficulties, the urgent key problems including cloud cloud security, standardization management, unified Cloud Architecture, parallel computing programmability, virtualization technology and service migration smoothly *etc.* With the popularization of applications on the cloud, cloud security issue has become the biggest bottleneck restricting current cloud computing promotion.

2009 survey: more than 70% of the surveyed enterprises despite the urgent demand of the cloud, but for the private data security and privacy concerns and delay acceptance of cloud computing schedule. In 2009 March, Google has leaked a large number of user file events. In 2009, February and July, Amazon because of "simple storage service" for the two time the disruption caused a cloud service website Yong paralysis. A series of cloud security accident outbreak exacerbated people concerned about the security of cloud. Therefore, carries on a thorough analysis of the cloud system, solve the cloud security problems is the first priority to promote the continuous development of cloud computing.

4. Analysis of Energy use Efficiency of Each City in Shandong Province

A large number of facts show that the trust relationship between different entities of in-depth study of the cloud environment, and security mechanism based on trust to ensure safety operation of the cloud system is very necessary. However, trust is a concept which is difficult to handle, it is difficult to find an appropriate method to accurately define and evaluate the trust relationship between entities. Therefore the design to adapt to the new trust cloud computing model and solve the trust based security scheme is a difficult and challenging work. Finish the job or be further will provide a useful reference for the solution of cloud security issues, so as to promote the further development of cloud computing research.

Based on the analysis of trust crisis which cloud computing faces, this paper established a trust cloud service model based on third party certification, to maximize the improvement of the existing cloud service security system, provides a scientific, comprehensive, system operation system for cloud users and cloud service providers.

4.1 Cloud Service Flow Figure based on Third Party Certification

As shown in Figure 2, the so-called third party certification refers to the certified for safety, find a neutral body can cloud services to parties, and constrain each other's behavior. By the method of standardization technical measures to supervise the cloud service, for security vulnerabilities exist to modify, and to evaluate the level of security system, is conducive to safeguarding the interests of both sides of cloud services, enhance the level of trust each other.

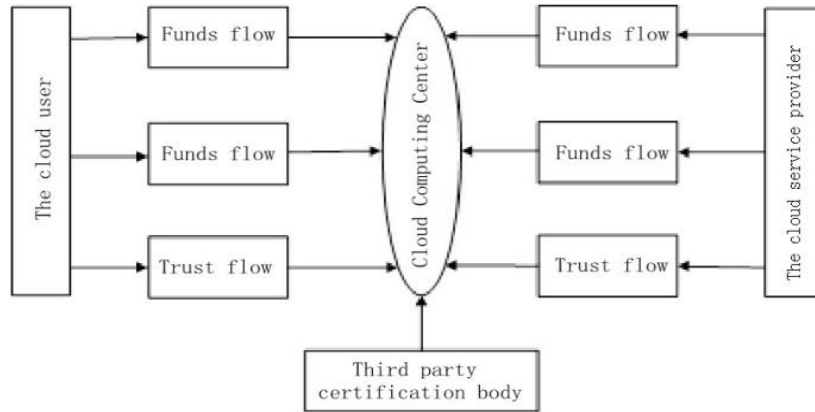


Figure 2. Cloud SERVICE FLOW FIGURE based on Third Party Certification

Hypothesis:

Based on the cloud service flow Figure, this paper put forward the following hypothesis.

First, the cloud service providers and recipients are perfectly rational economic man.

Second, both sides cloud service process can obtain all information through appropriate channels, and two mutually independent, and make a decision.

Third, the cloud service process will only exist in two states and trustworthy and fraud.

The Related Parameters

S_t Meanscredit coefficient of third party certification body in the t phase, this paper assumes that the initial credit coefficient S_0 zero.

s_t Means the credit value of third party certification body in one exchange made, credit coefficient by accumulation mode is simple to calculate the third party certification body, $S_{t+1} = S_t + s_t$.

$p(s_t)$ Means the cost when the cloud users enter into the cloud services platform in the t phase.

Π_t Meansthe return the cloud users got after the cloud services trade is end in t phase, only when $\Pi_t > 0$, the three party certification body can get commission.

ε Means the resulting percentage that third party certification body in a cloud service transactions and the cloud user gains is positive, $0 \leq \varepsilon < 1$.

M_t Means the price of service product in t phase.

N_t Means the gain of third party certification body, which mainly includes each transaction commission and dismiss fraud cloud users two parts. $N_t = p(S_t) + \varepsilon\Pi_t(M_t, S_t)$

The method can effectively ensure the cloud users and cloud service providers in the cloud products trading interests, cloud users will fully rely on credit evaluation of the suppliers to make the third party certification body level in the choice of the cloud service provider, so the third party certification body of the credit rating is very important. Positive feedback can increase revenue for the third party certification body, the cloud

service provider and cloud users, negative feedback can be made by credit coefficient to generate future income effect. $\frac{\partial p}{\partial S_t} > 0$ and $\frac{\partial \Pi_t}{\partial S_t} > 0$, then $\frac{\partial N_t}{\partial S_t} = \frac{\partial p}{\partial S_t} + \varepsilon \frac{\partial \Pi_t}{\partial S_t} > 0$.

Service Transaction Mechanism Process:

Cloud services trading mechanism of third party certification is a dynamic management process based, mainly divided into the security system to prevent, manage and post rewards and punishments and other major. Below is mainly about the services the major steps in the process are analyzed and introduced.

First, before the cloud service transactions, the cloud user needs first to pay a service fee to the third party certification body in the cloud computing platform $p(S_0)$, and then in every service after the success of the transaction is also required to pay royalties $\varepsilon \Pi_t$.

Second, in a cloud computing service transaction process, cloud users and cloud service providers formed a two person game state. If the cloud service provider to trade for integrity, then the credit coefficients are third party certification institutions increased s_t ; if the cloud service provider to trade for fraud, if the third party certification agencies to give be fraud compensation certain, then the credit line number increases s_t , if it fails to provide compensation, reduce credit coefficient s_t .

Third, at the end of a cloud service transaction, if the transaction is one of the two parties found the other party fraud, you can appeal to apply to the third party certification body, costs A. Through the investigation and analysis, if the existence of fraud, the third party certification body has the right to demand payment fraud is fraud compensation B, fraud is equally have the right to decide whether to accept the results of the survey. The method to ensure the integrity of the income is greater than 0, the amount of compensation B is larger than or equal to the square of fraud losses λu_t , and the cost of A, *i.e.*, $B \geq \lambda u_t + A$. If the cloud service trade both sides recognized the existence of fraud, all need to pay compensation to the third party certification body B.

Fourth, if according to the standard of fraud to pay compensation, then the cloud computing platform is still regarded as the integrity of the cloud user, will not have a negative impact on the future of cloud service transactions. However, if the fraudulent party refused to pay compensation, then the third party certification body will confiscate the initial payment of service charges, the dismissal of, and the information on the cloud computing platform.

Fifth, under normal circumstances, if the cloud users want to exit the third party certification body can be fully retrieve initial pay service fees. But, if it is fired, the service fee will be forfeited, not to return.

4.2 Cloud Services Trust Game Model

The existing cloud service trust game model

Assume that in the absence of third party certification institution, game situation between the cloud provider and cloud user transactions occur, as shown in Table 1.

Table 1. Game Situation between the Cloud Provider and Cloud User Transactions

The cloud service provider	The cloud user	
	Honest	Cheat
Honest	u_t, u_t	$-\lambda u_t, (1 + \alpha)u_t$
Cheat	$(1 + \alpha)u_t, -\lambda u_t$	$0, 0$

As shown in Table 1, if the cloud service provider and the cloud user both have an honest deal, they both earn u_t ; if one of them exist cheat action, then the cheater earns $(1 + \alpha)u_t$, the honest earns $-\lambda u_t$ ($\lambda > 0, \alpha > 0$). Because $(1 + \alpha)u_t > u_t$, when one side choose cheat, the optimal decision of the other side is cheat; and owing to $-\lambda u_t < 0$, so when one side choose cheat, the optimal decision of the other side is cheat. So the (cheat, cheat) is the Nash equilibrium.

The cloud service trust game model based on third party certification body

Suppose in the presence of the third party certification body condition, the game process of cloud users and cloud service providers in the transaction process as shown in Table 2.

Table 2. Game Situation In The Presence Of the Third Party Certification

The cloud service provider	The cloud user	
	Honest	Cheat
Honest	$(1 - \beta)u_t, (1 - \beta)u_t$	$B - \lambda u_t - A, (1 + \alpha)(1 - \beta)u_t - B$
Cheat	$(1 + \alpha)(1 - \beta)u_t - B, B - \lambda u_t - A$	$-B, -B$

In the process of cloud service transactions, owing to

$$(1 - \beta)u_t > (1 + \alpha)(1 - \beta)u_t - B$$

So when one side choose honest, the optimal decision of the other side is honest; and because $B - \lambda u_t - A > -B$, so when one side choose cheat, the optimal decision of the other side is honest either; so the (honest, honest) is the Nash equilibrium of the model, so we know that cloud service trading mechanism based on the third party certification mechanism for cloud users and cloud service providers bring security assurance.

Through the detailed analysis of the cloud service trust game model based on third party certification, we have drawn the following conclusions.

First, When $B \geq (1 - \beta)\alpha u_0$, The cloud service provider will choose honest fair in the third party certification body condition.

When there exist cloud trade between cloud users and cloud service providers, two cloud service provider strategy yields as shown in Table 3.

Table 3. The Income of Two Kinds of Cloud Service Provider Strategies

The cloud service provider	The cloud user	
	Honest	Cheat
Honest	$(1 - \beta)u_0 + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t$	$B - \lambda u_t - A + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t$
Cheat	$(1 + \alpha)(1 - \beta)u_0 - B + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t$	$-B + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t$

θ is discount factor, and meet $\theta = \frac{1}{1+i}$, $0 < \theta < 1$, i is the market interest.

When the cloud user choose honest, if

$$(1 + \alpha)(1 - \beta)u_0 - B + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t \leq (1 - \beta)u_0 + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t,$$

The optimal decision of cloud service provider is honest; when the cloud user choose cheat, if

$$B - \lambda u_t - A + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t \geq -B + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t$$

The optimal decision of cloud service provider is still honest. A comprehensive analysis of the above two inequalities, we can draw that when $B \geq (1 - \beta)\alpha u_0$, no matter the choice of the cloud user, the optimal decision of cloud service provider is honest.

Second, when the cloud users find itself is cheated, it will be to the third party certification body for compensation.

Cloud services trading mechanism in this paper can ensure the transaction integrity party gains constant greater than zero, $B - \lambda u_t - A > 0$, then we can get $B > A$. When the cloud users find itself is fraud, although the need to pay the fee of A, but the B can effectively make up for the cost, so the cloud user will compensate the appeal to the third party certification body.

Third, when

$$B < p(S_0) + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t - k \sum_{t=1}^{\infty} \theta^t (1 - \beta')u_t'$$

Cheater in the transaction will pay to be cheated party compensation B. (Among them, k is the third party certification, registered the probability of success in the other third party certification body; $\sum_{t=1}^{\infty} \theta^t (1 - \beta')u_t'$ is the profit that the cheater gained from $t = 1$)

This is because in the transaction, when one side choose cheat, and its total profit is:

$$\Pi_1 = (1 + \alpha)(1 - \beta)u_0 - B + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t$$

But after expelled by third party certification body, and enter into other third party certification body as the k probability, the total profit of the cheater is

$$\Pi_2 = (1 - \beta)(1 + \alpha)u_0 - p(S_0) + k \sum_{t=1}^{\infty} \theta^t (1 - \beta')u_t'$$

So, if and only if $\Pi_1 > \Pi_2$,

$$B < p(S_0) + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t - k \sum_{t=1}^{\infty} \theta^t (1 - \beta')u_t'$$

the cheater will choose to pay to be cheated party compensation B.

Forth, When $B < Q_0 - Q_{0(h)}$, If the cheater refuses to pay compensation to the cheated party, the third party certification body will pay compensation to the cheated. (Q_t for the third party certification body before the t phase has always been honest exchange can obtain the expected total discounted revenue; and $Q_{t(h)}$ said when a fraudulent transaction phase t, third party certification body to ensure the future of other members of the integrity of transactions of the total discounted revenue.)

$$\frac{\partial N_t}{\partial S_t} > 0, \text{ so } Q_t > Q_{t(h)}. \text{ When one side choose to cheat, Third party certification}$$

body to the cheated payment compensation, total income of third party certification date for: $E_1 = \beta(1 + \alpha)u_0 - B + Q_0$;

When the cheater and third party certification authority is not to pay compensation, the transaction is deemed fraudulent transactions, total income of third party certification date for: $E_2 = \beta(1 + \alpha)u_0 + Q_{0(h)}$. So, if and only if $E_1 > E_2$, $B < Q_0 - Q_{0(h)}$, Third party certification body will pay compensation to the cheated side.

Fifth, in the cloud service model based on trust third party certification body, when meet the following inequality conditions (honest, honest) strategy is the Nash equilibrium solution of the model of the game.

$$\max\{A, (1 - \beta)\alpha u_0\} \leq B < \max\{p(S_0) + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t - k \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t, Q_0 - Q_{0(h)}\}$$

According to the first and second conclusion above, we can easily get $B \geq \max\{A, (1 - \beta)\alpha u_0\}$. And from the third conclusion, In the event of cheat, cheater will pay compensation B, the forth conclusion guarantee after the cheat happen, If the cheater does not pay, it will be paid by third party certification body, thereby ensuring transaction integrity, so, we can get

$$B < \max\{p(S_0) + \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t - k \sum_{t=1}^{\infty} \theta^t (1 - \beta)u_t, Q_0 - Q_{0(h)}\}$$

The inequality of conditions, both parties to the transaction after repeated game, can reach (honest, honest) Nash equilibrium.

In this model, the trust in the interaction, were evaluated by the third party, reflects the interaction of fairness and justice, the cloud users and cloud service providers in equal status, is conducive to the development of cloud computing. After the interaction, the cloud provider of third party users trust value evaluation, reduced by third party and user collusion fraud may, also puts forward requirements for the quality assessment of the third party; cloud users submit evaluation of cloud service providers, but also prevent the third party and the cloud service provider collusion may, and the cloud service provider's service quality requirements are put forward. In this way, the three party to participate in the activities of the benign interaction to the interdependent and mutual constraints.

5. Conclusion

Firstly, based on the game theory and the cloud service transaction characteristics, respectively to establish the presence or trust the cloud service game model has no third party certification body, through the analysis of the game model, draw the conclusion: the introduction of third party certification is necessary to solve the problem of trust measures cloud. Through a series of propositions, build trust cloud service management mechanism based on trusted third party. Finally, comparative study. This paper establishes the trust management mechanism and model,

Model in many ways effectively constrain the parties to the transaction cloud services fraud, which play the role of supervision and restraint, trust cloud services have significant risk control.

References

- [1] Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", *Internet Services Appl.*, vol. 1, no. 1, (2010), pp. 7–18.
- [2] M. Randles, D. Lamb, E. Odat and A. Taleb-Bendiab, "Distributed redundancy and robustness in complex systems", *J. Comput. System Sci.*, vol. 77, no. 2, (2011), pp. 293–304.
- [3] D. Kusic, J. Kephart, J. Hanson, N. Kandasamy and G. Jiang, "Power and performance management of virtualized computing environments via lookahead control", *Cluster Computing*, vol. 12, no. 1, (2009), pp. 1–15.
- [4] M. Cardosa, M. Korupolu and A. Singh, "Shares and utilities based power consolidation in virtualized server environments", in: *Proceedings of IFIP/IEEE Integrated Network Management (IM'09)*, (2009), pp. 327–334.
- [5] L. Grit, D. Irwin, A. Yumerefendi and J. Chase, "Virtual machine hosting for networked clusters: Building the foundations for autonomic orchestration", in: *Proceedings of the 2nd International Workshop on Virtualization Technology in Distributed Computing*, (2006), p. 7.
- [6] A. Menezes and N. P. Smart, "Security of signature schemes in a multi-user setting", *Des. Codes Cryptogr.*, vol. 33, no. 3, (2004), pp. 261–274.
- [7] W. Ogata, K. Kurosawa and S.-H. Heng, "The security of the FDH variant of Chaum's undeniable signature scheme", in: S. Vaudenay (Ed.), *Public Key Cryptography*, in: *Lecture Notes in Comput. Sci.*, Springer, vol. 3386, (2005), pp. 328–345.
- [8] S. Saeednia, S. Kremer and O. Markowitch, "An efficient strong designated verifier signature scheme", in: J.I. Lim, D.H. Lee (Eds.), *ICISC*, in: *Lecture Notes in Comput. Sci.*, Springer, vol. 2971, (2003), pp. 40–54.
- [9] W. Susilo, F. Zhang and Y. Mu, "Identity-based strong designated verifier signature schemes", in: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), *ACISP*, in: *Lecture Notes in Comput. Sci.*, Springer, vol. 3108, (2004), pp. 313–324.
- [10] C. H. Tan, "Signcryption scheme in multi-user setting without random oracles", in: K. Matsuura, E. Fujisaki (Eds.), *IWSEC*, in: *Lecture Notes in Comput. Sci.*, Springer, vol. 5312, (2008), pp. 64–82.

Author



Haiyong Xu

1970.11 Shandong Wei Fang

Author's profile:

PhD student of Tianjin university collage of management and economic department