Job Security in the Cloud Computing

Tuo Yupeng, Xu Jie, Xu Zhikai, and Ye Jianwei

***Abstract*—Cloud computing is a burgeoning Internet computing paradigm. The convenient, cheap and elastic resources in the cloud are attracting the users to migrate their assets (data, computing and software, etc.) into it. However, cloud also caused the serious worry about the security of those assets, since the resources are not under the control of the users. Traditional security mechanisms are usually aimed at single autonomous domain and are not suitable for protection of those assets migrating between autonomous domains. This paper caters to the security of aforesaid migrated assets, defines them as job, studies their security demands, analyses the security threats to them, and proposes the essential protecting mechanisms for it. Our work is from the point of view of the users, and thus will be more suitable for solving the security problem of their assets.**

***Index Terms*—Cloud computing, security, job, asset, protection.**

I. Introduction

Cloud computing is becoming one of the most development direction of IT field. Its concept that "the network is the computer", is attracting the users to migrate their assets (data, computing, software, etc.) into the cloud, for reducing their hardware acquisition and maintenance cost. However, cloud also caused the serious worry about data security. According to the survey [1] of IDC, 74.6% of the users said that their most concern about the cloud computing is the security of their assets. Recently, the various Data leakage accidents of Amazon, Google and other cloud computing sponsors encourage their worry. Therefore, the assets security solution is the key of the popularization and development of cloud.

Traditional security mechanisms (such as risk evaluation, access control, etc.) are mainly aimed at single autonomous domain where a super security administrator exists, and so are not suitable for cloud which is composed of multiple autonomous domains, which have heterogeneous security states, security mechanisms and have no a centralized super administrator. When the users send their assets into a cloud, they lose the control to their assets, and don't know whether the cloud will give their assets enough protection, especially when the assets migrate between autonomous domains.

Traditional security mechanisms may secure the cloud infrastructures, but are not enough for protecting the migrating assets. Therefore, new security technology architecture must be studied.

Traditional security mechanisms may secure the cloud infrastructures, but are not enough for protecting the migrating assets. Therefore, new security technology architecture must be studied.

Manuscript received October 11, 2014; revised December 12, 2014. This work was supported by the National Natural Science Foundation of China under Grant 61100188.

Tuo Yupeng and Ye Jianwei are with Institute of Information Engineering, CAS, China (e-mail: {tuoyupeng, yejianwei}@iie.ac.cn).

Xu Jie is with National Computer Network Emergency Response Technical Team Coordination Center of China (e-mail: xujie@cert.org.cn).

Xu Zhikai is with Haerbin Institute of Technology, Heilongjiang, China (e-mail: zhikaixu@foxmail.com).

II. Related Works

In the researches on the security of the cloud computing and distributed computing, much security mechanisms is proposed. We summarize them as follow.

A. Security Models

For the cloud computing security, some security models have been studied, including mainly the layered static models and lifecycle dynamic models. Well-known static models include the 7-layer security model [2], SACS mode l [3], trust-based model [4], and so on. Dynamic models mainly include authentication-monitor model [5] and service composition model [6].

Those models aimed at not the security of users' assets but the security of cloud computing platform, so are unable to protect the assets roundly, especially to internal attacks.

B. Trusted Computing

Since the source of the users' security concern is the mistrust to the cloud platform, the most direct solution is to build trust. The existing solutions include TPM-based methods and reputation-based methods. TPM-based methods rely on TPM [7] hardware as trust root to sure the integrity of upper software, hence is expensive and limited. The reputation-based methods [8] rely on the action history of software and system.

The trusted computing methods can't solve all security problems, but are suitable as security basis.

C. Risk Evaluating

Risk evaluating is the most traditional security mechanism in information system. By now, the risk evaluating for the cloud is directly derived from the traditional one, such as [9], [10]. They all make the cloud platforms as the evaluating objects but the users' assets. So, they can't evaluate the risk to the assets roundly since the security cloud may attack the assets still.

D. Authenticating, Authorizing and Access Control

In general, the cloud is composed of heteroideous autonomic domains, so the inter-domains authentication is essential. Because the single authenticating center is unpractical for a huge cloud, the researchers study layered authentication, such as HIBC [11] and corresponding certificate management and authenticating process.

The other problems are inter-domain policy merging and fine-grain authorizing. The existing policy merging

mechanisms include those in [12], [13]. Current fine-grain authorizing mechanisms all based on DIFC [14].

E. Data Security

For the data confidentiality, traditional method is encryption. In order to keep the computability of data, researchers proposed the CED [15] and GC [16].

For the data authenticity, the main methods include POR[17], PDP [18], and so on.

F. Computation Security

The hardware-based methods are mainly those based on TPM.

Pure software methods for confidentiality have CEF[19], black box security [20], environment-key [21], etc.

Pure software methods for authenticity include mainly Protective assertion [22] and State evaluation function [23].

III. Job and Its Security Demands

A. Job Definition

Definition Job. A job is composed of program files, data and executing instruction. The computers control the program files and data of the job, and execute it by its executing instruction. A job has the following features:

- *I* it is used to do special function planed by its owner.
- *I* it is executed in the cloud and is the direct consumer of the cloud resources.
- It includes one or multiple program files, and may include multiple data or no data.

B. Job Security Demands

The jobs are the assets of the users, represent the users' fundamental interests, and hence need following security requirements:

- The data can be accessed normally by authorized objects.
- The programs can be executed normally by authorized objects.
- The private data, program codes and executing states can't be perceived or pilfered by unauthorized objects.
- The programs and data can't be forged or tampered, and executing states and functions can't be changed unauthoritatively.
- The jobs' owners can authorize the excitation of their programs and the access to their data.
- The jobs can be supervised by their owners to assure above requirements to be met in their whole lifecycle.

According to above requirements, the security demand of the job meets the CACA model, and thus includes four attributes:

- Confidentiality. It represents the demand that the job's computation and data should not be leaked or access unauthoritatively.
- Authenticity. It represents the demand that the job's computation and data should not be forged or tampered.
- Controllability. It represents the demand that the user can authorize the access to his job and can supervise the whole lifecycle of the job.
- Availability. It represents the demand that the job's data can be accessed and job's computation can be performed normally.

IV. Threats to Job Security

In the cloud, the surrounding of a job is composed of the cloud infrastructures and services. Once a job migrates from its owner host into the cloud, it will be wholly under the control of the cloud infrastructures and services. This is the source of most security concerns.

In general, the jobs may face three types of attackers – external attackers, infrastructures providers, service providers, shown in Fig. 1. The external attackers may be hackers making traditional network attacks, or malicious users attacking other jobs in the same cloud. The infrastructures providers and service providers may direct operate the jobs since they directly control them. Though above three type of attackers perform different attack methods, they have the same goal – pilfering private information, forging or tampering the jobs, or destroying the execution of the jobs.

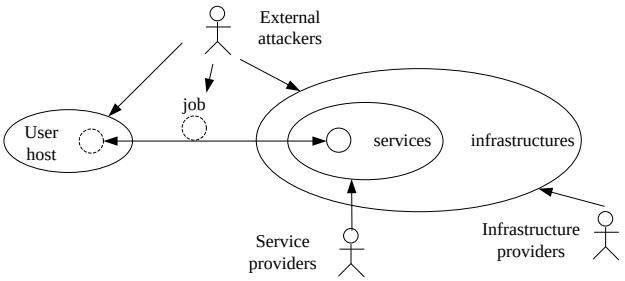


Fig. 1. Threats to the job in cloud.

We study the main 44 security risks in the cloud [24], group them to 7 categories, and show the relationship between them and the job's security demands in Table I.

A. Security Management Risks

T1. The security of the cloud providers can't be assessed in advance.

T2. Traditional risk assessments for information system don't suit the cloud.

T3. The cloud providers will not carry out the safety measures the users asked.

T4. The security policies in the cloud are not consistent to those uses want.

T5. The qualification and security certificates can't be audited comprehensively.

T6. The changes of the cloud security state are unable to be perceived in time.

B. Data Security Risks

T7. The cloud providers should not encrypt users' data as required.

T8. The cloud providers cannot completely isolate the data of multiple users.

T9. The cloud providers will probably pilfer the users' privacies.

T10. The data will probably be sniffed when being transferred.

T11. The loss of the keys causes the leakage of private data.

T12. The cloud providers don't clean the data as required.

T13. The cloud providers analyse the data unauthoritatively.

T14. The cloud providers can't check the integrity of the

data periodically.

T15. The cloud uses customized data formats that can't be used in other cloud.

T16. The faults of the cloud result in the loss of data.

T17. The loss of the keys causes the encrypted data useless.

C. Service Security Risks

T18. The services have no isolated surroundings, leading to be disturbed.

T19. The cloud providers steal the business secrets from the services.

T20. The cloud returns false computing results.

T21. The faults of the cloud lead the services to be breakdown.

T22. The cloud uses customized service interfaces not be used in other cloud.

T23. The cloud breakdown causes redevelopment and redeploy of the services.

T24. The cloud can't assure the QOS of the services.

D. Virtualization Security Risks

T25. The bugs in supervisors cause inter-access between the virtual machines.

T26. The vulnerabilities in v-machine images threat data and services in it.

T27. The faults of v-machine break the data and services in it.

T28. The migrations of v-machines invalid the trusted computing mechanisms.

T29. The complex lifecycle increases the control difficulty to data and services.

E. Authorization and Access Control Risks

T30. Traditional authorization and control don't fit inter-domain jobs.

T31. Heterogeneous authorization and control can't secure migrating jobs.

T32. The dynamic and expansibility make the protecting border indistinct.

T33. The cloud may subcontract the jobs to the uncontrolled third-parties.

T34. The losses of keys make the certificates invalid and misused.

T35. The uses of authorization add the password/certificates forging attacks.

F. Evidence Collection and Audit risks

T36. The cloud doesn't support the evidence collection for audit.

T37. The cloud may delete, destroy or forge evidence.

T38. The cloud may choose keeping silence when security incidents occur.

G. Laws Support Risks

T39. The actual location of the data may beyond the control of the origin laws.

T40. The actual location of the data may have no laws for the data protection.

T41. No enough information can be provided when the legal disputes occur.

T42. The cloud analyses the data illegally.

T43. The contracts may imply clauses that may harm the users.

T44. The subcontracts may break the protection of the contracts.

TABLE I: CORRESPONDING BETWEEN THREATS AND SECURITY DEMANDS

	Confidentiality	Authenticity	Controllability	Availability
T1-T6	●	●	●	●
T7	●			
T8	●	●	●	
T9-T13	●			
T14		●		
T15-T18			●	
T19	●			
T20		●		
T21-T24			●	
T25-T26	●	●	●	●
T27		●	●	
T28-T33				●
T34-T35	●	●	●	●
T36-T38				●
T39-T44	●	●	●	●

V. PROTECTING MECHANISMS FOR THE JOB

For the security of the job in its whole lifecycle, five essential protecting mechanisms must be applied, including trust mechanism, evaluating mechanism, scheduling mechanism, defending mechanism and auditing mechanism.

Trust mechanism is used to build trust relationship between the job owners and other four security mechanisms, hence makes the users believe that the other security *me*chanisms will work well.

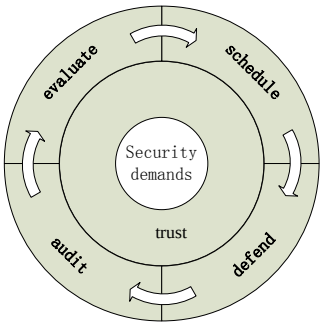


Fig. 2. security mechanism framework for the job in the cloud.

Evaluating mechanism is used to evaluate the security states of the cloud infrastructures and services. According to the evaluating results, the job owners can select more secure infrastructures and services to build surroundings for their jobs.

Scheduling mechanism selects proper infrastructures, services and defending mechanisms to make enough secure running surroundings for the jobs by the security states and jobs' security demands.

Defending mechanism enhances the jobs or prevents the attacks to the jobs.

Auditing mechanism is used to supervise the jobs' whole lifecycles and analyse the jobs' running processes.

Above five security mechanisms must work together to provide dynamic security for all jobs, they may include

some existing security technologies listed in part II. The trust mechanism is basis, and other four mechanisms perform protecting. They relationship is shown in Fig. 2.

VI. Conclusions

Aiming at core security problem in the cloud computing – job security, this paper studies the shortcut of the traditional security mechanisms, presents the security demands of the jobs, analyses the threat to the jobs, and proposes five essential security mechanism. Our work can effectively secure the jobs. Next step we will focus on proposed five security mechanisms.

Acknowledgment

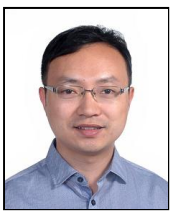
This work was supported by the National Natural Science Foundation of China (Grant No. 61100188).

References

[1] IDC. IT Cloud Services User Survey. pt.2: Top Benefits & Challenges. [Online]. Available: http://www. blogs.idc.com/ ie/? p=210.
[2] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v1.0. [Online]. Available: http://www. cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf.
[3] J. Xue and J. J. Zhang, "A brief survey on the security model of cloud computing," in *Proc. the 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, Hong Kong, 2010, pp. 475-478.
[4] W. Li, L. Ping, and X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in *Proc. the 2010 International Conference on Electronics and Information Engineering*, Japan, 2010, pp. 14-19.
[5] G. Peterson, "Don't trust and verify: A security architecture stack for the cloud," *IEEE Security and Privacy*, vol. 8, no. 5, pp. 83-86, 2010.
[6] H. Takabi, J. Joshi, and G. J. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environments," in *Proc. the 34th Annual IEEE International Computer Software and Applications Conference Workshops*, Seoul, Korea, 2010, pp. 393-398.
[7] Trusted Computing Group. Trusted Platform Modules Strengthen User and Platform Authenticity. [Online]. Available: https://www. trustedcomputinggroup.org/specs/TPM/Whitepaper_TPMs_Strengthe n_User_and_Platform_Authenticity _Final_1_0.pdf.
[8] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud security with virtualized defense and reputation-based trust mangement," in *Proc. the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, Chendu, China, 2009, pp. 717-722.
[9] X. Zhang, N. Wuwong, H. Li *et al.*, "Information security risk management framework for the cloud computing environments," in *Proc. the 10th IEEE International Conference on Computer and Information Technology, Bradford*, United kingdom, 2010, pp. 1328-1334.
[10] P. Saripalli and B. Walters, "QUIRC: A quantitative impact and risk assessment framework for cloud security," in *Proc. the 3rd International Conference on Cloud Computing*, Miami, FL, USA, 2010, pp. 280-288.
[11] L. Yan, C. Rong, and G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," in *Proc. the 1st International Conference on Cloud Computing*, Beijing China, 2009, pp. 166-177.
[12] L. Gong and X. Qian, "The complexity and composability of secure interoperation," in *Proc. the 1994 IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, CA, USA, 1994, pp. 190-200.
[13] L. Gong and X. Qian, "Computational Issues in Secure Interoperation," *IEEE Transactions on Software Engineering*, vol. 22, no. 1, pp. 43-52, 1996.
[14] A. C. Myers and B. Liskov, "Protecting privacy using the decentralized label model," *ACM Transactions on Computer Systems*, vol. 9, no. 4, pp. 410-442, 2000.
[15] M. Abadi and J. Feigenbaum, "Secure circuit evalution," *Journal of Cryptology*, vol. 2, no. 1, pp. 1-12, 1990.
[16] A. C. C. Yao, "How to generate and exchange secrets," in *Proc. the 27th IEEE Symposium on Foundations of computer Science*, Toronto, Ont, Can, 1986, pp. 162-167.
[17] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. the 14th International Conference on the Theory and Application of Cryptology and Information Security*, Melbourne, VIC, Australia, 2008, pp. 90–107.
[18] G. Ateniese, R. Pietro, L. Mancini *et al.*, "Scalable and efficient provable data possession," in *Proc. the 4th International Conference on Security and Privacy in Communication Networks*, Istanbul, Turkey, 2008, pp. 1-11.
[19] T. Sander and C. Tschudin, "Protecting mobile agents against malicious hosts," *Mobile Agents and Security*, 1998, pp. 44-60.
[20] F. Hohl, "Time limited blackbox security: Protecting mobile agents from malicious hosts," *Mobile Agents and Security*, 1998, pp. 92-113.
[21] J. Riordan and B. Schneier, "Environmental key generation towards clueless agents," *Mobile Agents and Security*, 1998, pp. 15-24.
[22] L. L. Kassab and J. Voas, "Agent trustworthiness," in *Proc. the ECOOP'98 Workshops*, Demos, and Posters Brussels, Belgium, 1998, pp. 121-133.
[23] W. Farmer, J. Guttman, and V. Swarup, "Security for mobile agents: authentication and atate appraisal," in *Proc. the 1996 4th European Symposium on Research in Computer Security*, Rome, Italy, 1996, pp. 118-130.
[24] R. Chow, P. Golle, M. Jakobsson, *et al.*, "Controlling data in the cloud: Outsourcing computation without outsourcing control," in *Proc. the 2009 ACM Workshop on Cloud Computing Security*, CCSW '09 Chicago, 2009, pp. 85-90.

Tuo Yupeng was born in Hebei China in 1984. He received his B.E. degree in software engineering from Haerbin institute of technology, Heilongjiang China in 2007 and He received his M.E. degree in software engineering from Haerbin Institute of Technology, China, in 2009. He main research interests include network security and information security.

He worked at Institute of Computing Technology in Beijing, China. He worked as an engineer from 2009 to 2012. Then, he worked at Institute of Information Engineering of Chinese Academy of Sciences in Beijing, China as an engineer since 2012.



Xu Jie was born in Shanxi China in 1982. He received his D.E. degree in signal process and multimedia from Institute of Computing Technology CAS, China in 2013. He main research interests include signal process, network security and information security.

He worked at National Computer Network Emergency Response Technical Team Coordination Center of China in Beijing, China as an Engineer since 2013.

Xu Zhikai was born in Shandong China in 1988. He received his B.E. degree in computer science from Haerbin Institute of Technology, Heilongjiang, China in 2010. He received his M.E. degree in computer system structure from Haerbin Institute of Technology, China in 2012. His main research interests include distributed computing, cloud computing.

He is working for his degree of D.E. since 2012 in Haerbin Institute of Technology, China.

Ye Jianwei was born in Zhejiang China in 1978. He received his B.E. degree in computer science from Haerbin Institute of Technology, Hei Longjiang, China in 2001 and He received his M.E. degree in computer system structure from Haerbin Institute of Technology, China in 2003. He received his D.E. degree in computer structure from Haerbin Institute of technology, China in 2011. His main research interests include distributed computing, network security and information security.

He worked at Haerbin institute of technology in Haerbin, China and he was working as a lecturer from 2003 to 2012. Then, he worked at Institute of Information Engineering of Chinese Academy of Sciences in Beijing, China as a senior engineer since 2013. He has published more than 20 papers. His research interests include distributed computing, cloud computing, grid, computer network security, information security, etc.