Cloud Computing Security Problem (Data Privacy) and Strategy

Piyush Singh Katiyar
Assistant System Engineer, Tata Consultancy Services Ltd., New Delhi

ABSTRACT: *Cloud computing is an increasingly popular technology that involves the use of networked servers to support centralized data storage, software as a service (SaaS), virtualization, and web-services, just to mention a few. The benefits of the cloud include economies of scale, overhead and cost savings, simplification of IT management, and more. Despite the capabilities and advantages of cloud computing, however, the technology has not lived up to its billing as "supposedly" offering superior and even infallible security. In fact, the cloud computing presents significant and diverse problems/challenges with fundamental security issues such as data privacy. A multi-layered security strategy can, however, help organizations address this security problem.*

Keywords - *Cloud Computing Security, Data protection strategy, CSA Data Protection Policy.*

I. INTRODUCTION

The first step in developing a strategy for a problem like data privacy is to fully define and understand the problem itself. In this respect, data privacy risks are higher in the cloud environment for the simple reason that the data owner does not physically protect and/or manage the system. In fact, the cloud subscriber does not typically know the location of the data center and storage hardware, and/or "what networks are transmitting the data." Perhaps most critically, cloud subscribers must recognize that moving into the cloud extends a great deal of trust and responsibility to the cloud provider.

As Dr. Giles Hogben of ENISA explains, most risks in the cloud are not new, but they are amplified by the following factors: "resource concentration, trustworthiness of insiders, hypervisors - hypervisor layer attacks on virtual machines are very attractive, more data in transit (without encryption), management interfaces – big juicy targets." Fig. 1 clearly shows the security as foremost threat in cloud computing.

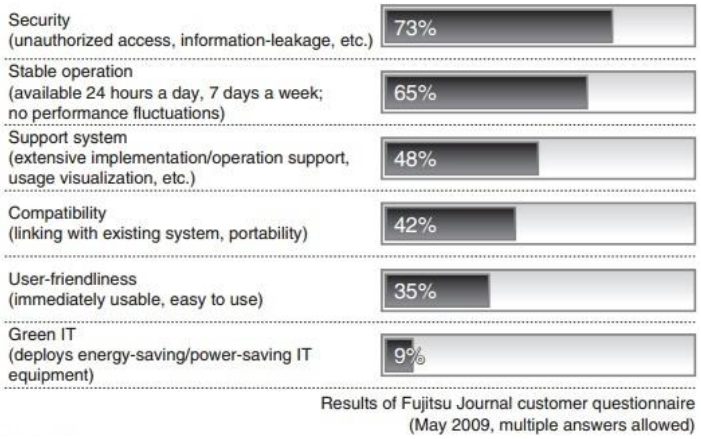


Fig. 1: Concerns in using cloud computing

In sum, data privacy can pose a huge security challenge/problem if the cloud provider and subscriber do not take the necessary steps to manage and secure the system services.

II. ADOPT A GOVERNANCE STRATEGY

Some companies make the mistake of assuming that the cloud does not require management on the subscriber's end. To ensure data privacy cloud subscribers must, first and foremost, be proactive in managing the cloud service. Along these lines, a number of components are essential for an effective governance strategy/policy. Foremost, the cloud subscriber should require a vendor agreement that includes a "contract or service level agreement." The contract/agreement should specifically address data privacy issues with assurances of proper security policies and implementations. Secondly, the subscriber must perform a risk assessment. The risk assessment should identify the potential threats to data privacy - outside intruders, hackers, cloud provider employees, and so forth. Based on the findings of Bisong and Rahman, the cloud computing governance function should also require the following: "risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements and transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the IT organization." Summarily, a well-designed governance strategy is an essential step in helping

the cloud subscriber be proactive in reducing and controlling the vast majority of data privacy risks.

III. Require User Permission for Data Access

In cases of intrusion by means of user id fraud, a simple solution can be offered - namely, requiring actual user permission for data access. As a security measure, the cloud must always detect when a user is attempting to access data. In every instance, the valid user should be notified of the access request. A notification message can be sent to the data owner (i.e., valid user) via email, cell phone, or any other medium. The valid user can then either grant or deny data access permission to the requesting party. Without such permission, however, nobody can ever access the private/confidential data. Most importantly, researcher Sonam Singh points out that this simple data security strategy is both cost effective and assures the data owner/valid user that his/her data is always secure.

IV. Comply with CSA Data Protection Policy Recommendations

In addressing the problem/challenge of data privacy, the "Cloud Security Alliance" encourages organizations to view the issue in the larger context of data loss/leakage. Data in the cloud is always at risk of being damaged, lost, or stolen.

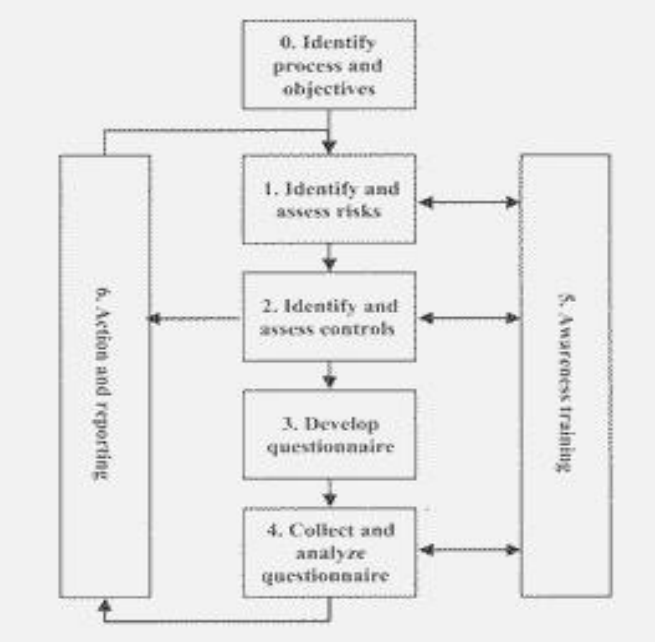
Therefore, a strategy must be aimed at reducing the risk/threat. With this goal in mind, CSA recommends six steps or measures that cloud subscribers should include in their data security policy and strategy. The measures include the following:

1) Implement strong API access control
2) Encrypt and protect integrity of data in transit
3) Analyze data protection at both design and run time
4) Implement strong key generation, storage/management, and destruction practices
5) Contractually demand providers to wipe persistent media before it is released into the pool
6) Contractually specify provider backup and retention strategies

Fig. 2: CSA Life Cycle Stages

In the order of presentation, the CSA approach addresses data security at the presentation layer, business layer, and data layer. On the front-end, for instance, simply addresses two key goals:

i) Making sure that users are who they say they are, and



ii) Ensuring that users are allowed to do only what they are authorized to do.

By encrypting and protecting data in transit, the cloud subscriber can, at least in some cases, make interception of private data an unprofitable undertaking for the hacker. As for the third element, data protection must be viewed as a part of the systems life cycle. Therefore, CSA recognizes that data privacy issues and security should be never be an afterthought. Risk assessments and solutions must be built into the system at design time and then tested and improved during implementation and deployment (i.e., run time). CSA recommendations further reinforce the need to contractually specify data privacy expectations with the cloud vendor. Thus, overall, the CSA framework approaches data privacy as a matter of proactive policy for prevention of security breaches before they ever happen.

V. Fortify Traditional Authentication with Identifier/Password Format

A complementary strategy element for protecting the cloud against intrusions by invalid users involves one-time password authentication using device authentication. With one-time password authentication, the user "enters a temporary password displayed on a dedicated card or on a mobile phone into a field on a Web screen as authentication information." In brief, this approach eliminates the possibility of a password being reused after being intercepted or stolen. Like all security strategies, device authentication

has its shortcomings. It does not, for example, preclude the possibility that a hacker/thief could come into possession of the authenticated cell phone or other digital device. But, device authentication does provide a layer of fortification of one of the biggest risks to data privacy on the cloud environment – namely, user identification and password theft.

Finally, many data privacy breaches occur as result of ghost IDs. Ghost IDs are "leftover IDs of users who have lost their usage rights [and/or] users who have been given inappropriate rights." In most cases, these types of problems are a result of failed control mechanisms and poor management. The solution, therefore, is proactive governance of systems on the subscriber's end. In other words, IT managers and security practitioners must make sure that changes to user roles and privileges are always reflected immediately in the cloud authentication system.

VI. CONCLUSION

Despite its many benefits, cloud computing presents significant problems with fundamental security issues like data privacy. A multi-layered security strategy can, however, help organizations address this security problem. Data privacy is a composite problem in the cloud computing environment that requires the cloud provider and subscriber to take the necessary steps to manage and secure system services. Some companies make the mistake of assuming that the cloud does not require management on the subscriber's end. However, a well-designed governance strategy is an essential step in helping the cloud subscriber be proactive in reducing and controlling the vast majority of data privacy risks. In cases of intrusion by means of user id fraud, a simple solution can be offered - namely, requiring actual user permission for data access. The CSA framework approaches data privacy as a matter of proactive policy for prevention of security breaches before they ever happen. A complementary strategy element for protecting the cloud against intrusions by invalid users involves one-time password authentication using device authentication. Finally, IT managers and security practitioners must make sure that changes to user roles and privileges are always reflected immediately in the cloud authentication system.

VII. Acknowledgement

I would like to thank Mr. Virendra Kumar, Assistant Professor, School of Computing Science & Engineering, Galgotias University, for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper.

REFERENCES

[1] Singh, S. *Data Security Issues and Strategy on Cloud Computing. International Journal of Science, Engineering and Technology Research, August 2013; 2(8).*

[2] Bisong, A, Rahman SM. *An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 2011 January; 3(1).*

[3] Hogben G. *ENISA-Cloud Computing Security Strategy. European Network and Information Security Agency 2010.* Available from *http://www.terena.org/activities/tf-csirt/meeting30/hogben-cloudcomputing.pdf*

[4] Bisong, A, Rahman SM. *An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 2011 January; 3(1).*

[5] Srinivasamurthy, S, Liu DQ. *Survey on Cloud Computing Security.* Department of Computer Science, Indiana University Purdue University Fort Wayne July 2010.

[6] Okuhara M, Shiozaki T, Suzuki T. *Security Architectures for Cloud Computing. Fujitsu Sci. Tech. J. 46(4) 2010 October: 400.*

[7] Brukbacher, S. Practical *Strategies for Managing Risk in Cloud Computing. Boulder, CO: Educause Center for Applied Research Bulletin 3, 2011.*

[8] Figliola, PM, Fischer EA. *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management. Congressional Research Service 2014 February 3; R42887.*

Author's Profile

Mr. Piyush Singh Katiyar (Assistant Syetem Engineer), His Educational Qualification is :B.Tech(Computer science and Engg.) from Integral University, Lucknow, India. Current Employer is Tata Consultancy Services Ltd., Gurgaon, India. His working area: Software Engineering and Cloud computing.