ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1130-1134), Month: April - June 2015, Available at: www.researchpublish.com

Data Security and Privacy Protection Issues in Cloud Computing

[1]Ms. Rupali R. Kanthe, [2]Ms. Rinkle C. Patel

[1, 2] Department of MCA, IMCOST College, Thane (w), University of Mumbai, India

Abstract: **It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud. The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.**

Keywords: **access control; cloud computing; cloud computing security; data segregation; data security; privacy protection.**

I. INTRODUCTION

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. The emerging paradigm of cloud computing provides a new way to address the constraints of limited energy, capabilities and resources. However, security and privacy protection is a critical concern in the development and adoption of cloud computing. To avoid system fragility and defend against vulnerabilities from cyber attacker, various cyber security tools and techniques were developed. Compared with the traditional IT model, the cloud computing has many potential advantages. But from the consumers' perspective, cloud computing security concerns remain a major barrier for the adoption of cloud computing. According to a survey from IDCI in 2009, 74% IT managers and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues. Another survey carried out by Garter in 2009, more than 70% CTOs believed that the primary reason not to use cloud computing services is that there are data security and privacy concerns. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Serious security incidents even lead to collapse of cloud computing vendors. As administrators' misuse leading to loss of 45% user data, cloud storage vendor LinkUp had been forced to close.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1130-1134), Month: April - June 2015, Available at: www.researchpublish.com

II. DATA SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

1. Data Breaches:

When user uses services of cloud computing ,they may require some confidential information like credit card information. when normal processing is happens at that point of time it may possible that some unauthorized user may theft the confidential information and they can misuse the information. Therefore, there is risk of data breach in cloud computing.

2. Data Loss:

A data breach is the result of a malicious and probably intrusive action. Data loss may arise when disk drive dies without owner of data had not created backup.

And sometimes it also may happen that, there were encrypted data which is locked and some key are necessary to unlock the data and at that time data get loss when the key get loss. Data loss also done by the human and they may done this kind of thing for intensionally.

3. Account or Service Traffic Hijacking:

There are many services on internet but for using they user need to create their account and then they can start using the services. Account hijacking is common factor in cloud. Sometimes due to software vulnerabilities, trafficking and buffer overflow it may take place. This all risk may lead to loss of control over their account. An hijacker get control over user account can eavesdrop on transaction, manipulate data, give false responses to customers. This risk compromising with confidentiality.

4. Insecure APIs:

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these largely anonymous users might do to the service. The answer has been a public facing application programming interface, or API, that defines how a third party connects an application to the service and providing verification that the third party producing the application is who he says he is Leading web developers, including ones from Twitter and Google, collaborated on specifying OAuth, an open authorization service for web services that controls third party access.

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data.

It is necessary to overcome this all kinds of risk. It is require to use the security controls that protect sensitive and helps to overcome data loss, data breach and account trafficking.

There are some effective cloud security solution should incorporate three key capabilities:

- Data lockdown
- Access policies
- Security intelligence

First, make sure that data is not readable and that the solution offers strong key management. Second, implement access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root user cannot view sensitive information. Third, incorporate security intelligence that generates log information, which can be used for behavioral analysis to provide alerts that trigger when users are performing actions outside of the norm.

5. Data Ownership:

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved (e.g., [Goo10, Rap09]). Ideally, the contract should state clearly that the organization retains ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement to use the data for its own purposes, including intellectual property rights or licenses; and that the cloud provider does not acquire and may not claim any security interest in the data [Mcd10]. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

6. Data Location:

One of the most common compliance issues facing an organization is data location [Bin09, Kan09, Ove10]. Use of an in-house computing center allows an organization to structure its computing environment and to know in detail where data is stored and what safeguards are used to protect the data. In contrast, a characteristic of many cloud computing services is that detailed information about the location of an organization's data is unavailable or not disclosed to the service subscriber. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can to some extent alleviate this issue, but they are not a panacea. When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns (e.g., [CBC04]). Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations [Eis05]. Among the concerns to be addressed are whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post transfer, and whether the laws at the destination present additional risks or benefits [Eis05]. Technical, physical and administrative safeguards, such as access controls, often apply.

III. IDENTITY AND ACCESS MANAGEMENT

In today's cloud computing world it becomes very complicate to protect data from unauthorized.Identity management focus on who is owner of data which provides that particular information are of this particular owner.Identity mainly focus on privacy of user information.Whereas access management mainly focus on aacessibility of information.Access Management concern about who have the permission to access data.

Data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern. One recurring issue is that the organizational identification and authentication framework may not naturally extend into the cloud and extending or changing the existing framework to support cloud services may be difficult [Cho09]. The alternative of employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, is a complication that can become unworkable over time. Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard or the OpenID standard.

- **Authentication:**

A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information, such as assertions related to a subject or authentication information, between cooperating domains. SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the eXtensible Markup Language (XML) for its format. SOAP messages are digitally signed. For example, once a user has established a public key certificate for a public cloud, the private key can be used to sign SOAP requests. SOAP message security validation is complicated and must be carried out carefully to prevent attacks. For example, XML wrapping attacks have been

successfully demonstrated against a public IaaS cloud [Gaj09, Gru09]. XML wrapping involves manipulation of SOAP messages. A new element (i.e., the wrapper) is introduced into the SOAP Security header; the original message body is then moved under the wrapper and replaced by a bogus body containing an operation defined by the attacker. The original body can still be referenced and its signature verified, but the operation in the replacement body is executed instead.

- **Access Control:**

SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud subscriber privileges and maintain control over access to resources is also needed. As part of identity management, standards like the eXtensible Access Control Markup Language (XACML) can be used by a cloud provider to control access to cloud resources, instead of using a proprietary interface. XACML focuses on the mechanism for arriving at authorization decisions,

which complements SAML's focus on the means for transferring authentication and authorization decisions between cooperating entities. XACML is capable of controlling the proprietary service interfaces of most providers, and some cloud providers already have it in place. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, making it important to have safeguards in place to protect decision requests and authorization decisions from possible attacks, including unauthorized disclosure, replay, deletion and modification.

IV. CURRENT SECURITY SOLUTIONS FOR DATA SECURITY AND PRIVACY PROTECTION

There aredecentralized information flow control (DIFC) and differential privacy protection technology into data generation and calculation stages in cloud and put forth a privacy protection system called airavat. This system can prevent privacy leakage without authorization in Map-Reduce computing process. A key problem for data encryption solutions is key management. On the one hand, the users have not enough expertise to manage their keys. On the other hand, the cloud service providers need to maintain a large number of user keys. The Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) is trying to solve such issues. About data integrity verification, because of data communication, transfer fees and time cost, the users can not first download data to verify its correctness and then upload the data. And as the data is dynamic in cloud storage, traditional data integrity solutions are no longer suitable. NEC Labs's provable data integrity (PDI) solution can support public data integrity verification. Cong Wang proposed a mathematical way to verify the integrity of the data dynamically stored in the cloud. In the data storage and use stages, Mowbray proposed aclient-based privacy management tool. It provides a usercentric trust model to help users to control the storage and use of their sensitive information in the cloud. Munts-Mulero discussed the problems that existing privacy protection technologies (such as K anonymous, Graph Anonymization, and data pre-processing methods) faced when applied to large data and analyzed current solutions. The challenge of data privacy is sharing data while protecting personal privacy information. There are some proposed a privacy protection framework based on information accountability (IA) components. The IA agent can identify the users who are accessing information and the types of information they use. When inappropriate misuse is detected, the agent defines a set of methods to hold the users accountable for misuse. To protect the data from from unauthorized person we can protect the data by making simulator which ask the sender for password when sender saves the information and when it received by receiver and when receiver opens the file at that time simulator ask receiver for password which is created by sender. This password is personal between both parties that is sender and receiver.

V. CONCLUSION

Although cloud computing has many advantages, there are still many actual problems that need to be solved. The revenue estimation implies that cloud computing is a promising industry. But from another perspective, existing vulnerabilities in the cloud model will increase the threats from hackers. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues exist in all levels in SPI service delivery models and in all stages of data life cycle. The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. These concerns include whether personal information can be stored or read by third

parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements. According to the analysis for data security and privacy protection issues above, it is expected to have an integrated and comprehensive security solution to meet the needs of defense in depth. Regarding privacy protection, privacy data identification and isolation are the primary tasks. They should be considered during the design of cloud-based applications.

ACKNOWLEDGEMENT

The satisfaction that accompany the successful completion of any task would be incomplete without mentioning the names of people who made it possible, whose constant guidance and encouragement crowns all efforts with our success. At the very outset, I express my sincere gratitude to our Internal Guide Prof Sonia Dubey and Prof Mohan Chedes for all types of help and guidance provided to us.

REFERENCES

[1] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_ computing_security.

[2] Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02.http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing- security-risks-853

[3] Cloud Security Front and Center. Forrester Research. 2009-11-18.http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html

[4] Cloud Security Alliance. http://www.cloudsecurityalliance.org.

[5] Cloud Security Alliance, Security Guidance for Critical Areas of Focusin Cloud Computing, V2.1, http://www.cloud securityalliance.org/guidance/csaguide.v2.1.pdf.