Privacy And Data Security Issues in Cloud Computing

Rasika S. Badre, Nilesh M. Tarbani

Abstract—Cloud computing has powerful advantages and many enterprise applications and data are migrating to public or hybrid cloud. Currently, we have given rise to the success of cloud computing. By applying cloud computing in business application to the third party it causes some issues related to security and privacy it will become a critical. After complete study of cloud computing they get a new common goal to review of existing security and privacy problems. We have identified five most representative security and privacy attributes in cloud computing i.e., confidentiality, integrity, availability, accountability and privacy-preservability.By using these attributes, we get the relationships among them, the weakness that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud environment.

Index Terms— Minimum 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

1 Introduction

NOWADAYS in cloud computing many organizations, by putting their applications we get increase benefits in Small and Medium Business (SMB) enterprises. It may lead to gain in efficiency and effectiveness in developing and deployment because of adoption of cloud computing as well as save the cost in purchasing and maintaining the infrastructure.

It enables on demand provisioning of computational and storage resources which is represented by a new business model and paradigm. Because of cloud computing fact it gives economic benefits which consist of the main drive. As well as cloud computing offers an effective way to reduce capital expenditure and operational expenditure.The definition of cloud computing is given in many literatures but it has not recognize widely.

2 Literature Review

The cloud computing has many potential advantages as compared to the traditional IT model. But from the customers perspective, cloud computing security concerns remain a major problem for the adoption of cloud computing. As per to a survey from IDCI in 2009, 74% IT managers and CIOs believed that the primary challenge that obstruct 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.

If cloud computing service providers touted the reliability and security of their services then the actual deployment of cloud computing services is not as safe as reliable they claim. In 2009, the major cloud computing vendors successively appeared in several accidents. In March 2009, security vulnerabilities in Google. We see, a global failure up to 4 hours in Google Gmail. It was exposed that there was serious security vulnerability in VM war virtualization software for Mac version in May 2009. People with beyond what is seen 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.delivery models and deploy models of cloud computing, compared with the traditional IT environment, however, cloud computing may face different risks and challenges. In cloud computing environments there is also present traditional security issues. Traditional security mechanisms are no longer suitable for applications and data in cloud. Due to the openness and multi-characteristic of the cloud, cloud computing is bringing excellent impact on information security field:

(1) There are features of cloud computing models i.e., dynamic scalability, service abstraction, and location transparency that all kinds of applications and data on the cloud platform have no fixed infrastructure and security boundaries.

(2) As per to the service delivery models of cloud computing, resources cloud services based on may be by multiple providers. As there is a disagreement of interest, it is difficult to deploy a unique security measures.

(3) Because of the openness of cloud and sharing virtualized resources can also used by other unauthorized users.

(4) As the cloud platform has to deal with massive information storage and to acess a fast delivery, cloud security measures have to meet the need of massive information processing.

V. Kavitha and S. Subashini made an investigation on cloud computing security issues from the cloud computing service delivery models (SPI model) and give a detailed information and assessment method description for every security issue. Mohamed Al Morsy, John Grundy and Ingo Müller explored the cloud computing security issues from different perspectives and also including security issues associated with cloud computing architecture, service delivery models, cloud characteristics. Yanpei Chen, Vern Paxson and Rand H. Katz believed that two aspects are to some degree new and essential to cloud: first, the complexities of multi-party trust considerations, and second the ensuing need for mutual auditability. They also point out some new opportunities in cloud compu-

ting security.

3 About Cloud Computing And Security Issues

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

2.2 Cloud Architecture

Fig. 1 shows the general architecture of a cloud platform also called as cloud stack. Building upon hardware facilities are mostly supported by modern data centers. Cloud services may be offered is in various forms i.e., from the bottom layer to top layer. In a cloud stack, each particular layer represents one service model. There are three services.

1.Infrastructure-as-a-Service (IaaS).

2 Platform-asa-Service (PaaS).

3.Software as a Service (SaaS)

Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, where resources are aggregated and it managed physically , and the services are delivered in forms of storage, network or computational capability. The middle layer delivers Platform-asa-Service (PaaS), in which services are provided for programming or software execution . Software as a Service (SaaS) is in top layer, in which a cloud provider further confines client flexibility by merely offering software applications as a service. Apart from the service, the cloud provider maintains a suite of management tools and facilities are available to manage a large cloud system.

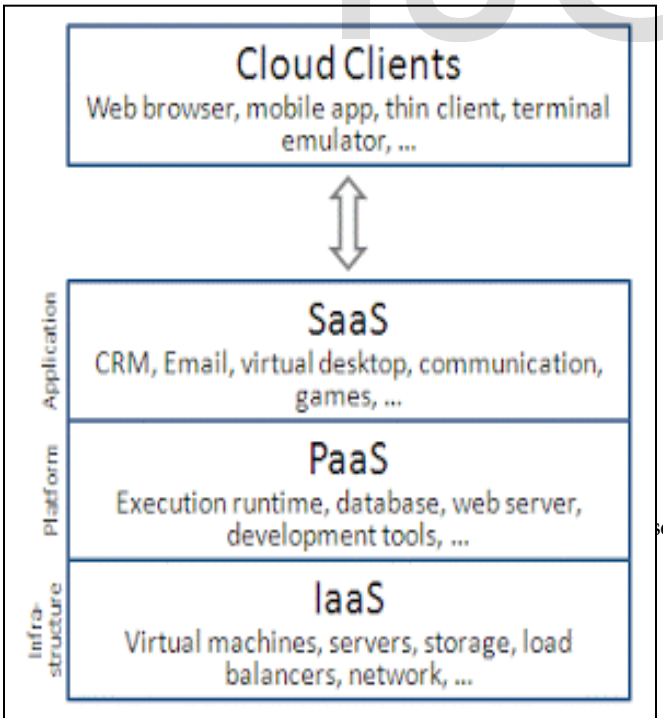

Fig. 1. General architecture of a cloud platform.

secu-

rity". It is an evolving sub-domain of computer security, network security, and information security. It used a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing". Note that cloud computing Security referred to here is not cloud-based security software products such as cloud-based anti-virus, anti-spam, anti-DDoS, and so on.

2.4 Security Issues Associated with the Cloud

There are many security issues related with cloud computing as well as they can be grouped into any number of dimensions. As per to Gartner, before making a choice of cloud vendors, there are seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. In 2009, Forrester Research Inc. evaluated security and privacy practices of some of the leading cloud providers in three major aspects:

1) Security and privacy
2) compliance
3) legal and contractual issues.

Cloud Security Alliance (CSA) is collecting solution providers, loss and single to enter into discussion about the present and future best practices for information in the cloud.

2.5 Data Life Cycle

Data life cycle refers to the entire process from generation to destruction of the data. There are seven data life cycle stages:

1. Data GeneratIion:
   Data generation is included in the data itself. In the traditional IT atmosphere, usually users or organizations own and manage the data. But if data is to be migrated into cloud that it should be considered as how to maintain the data ownership. For private information, data owners are entitled to know what personal information is collected.
2. Transfer:
   Within the boundaries, data transmission usually does not need encryption, or only a simple data encryption measure. For data transmission across enterprise boundaries, both data confidentiality and integrity should be ensured in order is prevent to data from being tapped and tampered by an unauthorized users. In the other words, the data encryption is not enough. Data integrity is also required to be ensured. Hence it should ensure that transport protocols provide both the confidentiality and integrity.
3. Use:
   For the static data using a simple storage service, such as Amazon S3, data encryption is feasible. However, for the static data used by cloud-based applications in PaaS or SaaS model, data encryption in many cases is not feasible. Because data encryption will lead to problems of indexing and query, the static data used by Cloud-based applications is generally not encrypted. Not only in cloud, but also in traditional IT environment, the data being treated is almost not encrypted for any program to deal with. Unencrypted data in the process is a serious threat to data security. According the use of personal data, situations are more complicated. The owners of private data require to focus on and ensure whether the

use of personal information is consistent with the purposes of information collection and whether personal information is being shared with third parties, for example, cloud service providers.

4. Share:
   Nowadays data sharing is important for accesing data it widely use range of the data and renders data permissions more complex. The data owners can authorize the data access to one party. The party can share the data to another party without the consent of the data owners. Hence, at the time of data sharing, specially when shared with the third party, the data owners required to consider whether the third party continues to maintain the original protection measures and usage restrictions. Regarding sharing of private data, in addition to authorization of data sharing.
5. Storage:
   The data in the cloud may be divided into:
   (1) The data in IaaS environment, such as Amazon's Simple Storage Service.
   (2) The data in PaaS or SaaS environment related to cloud based applications. The data stored in the cloud storages is similar with the ones stored in other places and needs to consider three aspects of information security: confidentiality, integrity and availability.
   control, Otherwise, this may result in the availability or privacy threats.
6. Archival:
   Archiving for data focuses on the storage media, to provide off-site storage and storage duration. If the data is stored on portable media then the media is out of control, the data are to take the risk of leakage. If the cloud service providers do not provide off-site archiving, the availability of the data will be threatened. Again, storage duration is consistent with archival requirements otherwise, this may result in the availability or privacy threats.
7. Destruction:
   When the data is no longer needed, it has been completely destroyed. Due to the physical features of storage medium, the data deleted may still exist and can be restored.

4 Current Privacy Protection And Data Security

In June 2009 IBM developed a fully holomorphic encryption scheme. This scheme allows data to be processed without being decrypted. Roy I and Ramadan HE applied decentralized 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.

The system also can prevent privacy leakage without authorization in Map-Reduce computing process. A key problem for the data encryption solutions is key management. The Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) is try to solve 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. 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 a client-based privacy management tool . It provides a user centric trust model to help users to control the storage and use of their sensitive information in the cloud. Munts-Mulerodiscussed the problems that existing privacy protection technologies faced when applied to large data and analyzed current solutions . The challenge of is sharing data while protecting personal data privacy information. RandikeGajanayake 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 appropriate misuse is detect, the agent defines a set of methods to hold the users accountable for misuse. methods of data (destruction) security, but it does not provide any specific requirements for how these two methods are to be achieved. The National Institute of Standards and Technology (NIST) Special Publication .

5 Conclusion

Throughout this paper, studied the security and privacy issues in cloud computing .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

References

[1] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing andgrid computing 360-degree compared," Grid Computing EnvironmentsWorkshop, 2008. GCE'08, 2009, pp. 1-10.

[2] J. Geelan. "Twenty one experts define cloud computing," Virtualization,August 2008. Electronic Mag., article available at http://virtualization.sys-con.com/node/612375.

[3] R. Buyya, C. S. Yeo, and S. Venugopal. "Market-oriented cloud-computing: Vision, hype, and reality for delivering it services as computing utilities," CoRR, (abs/0808.3558), 2008.

[4] P. Mell and T. Grance. The NIST Definition of Cloud Computing(Draft).[Online]Available: www.nist.gov/itl/cloud/upload/cloud-defv15.pdf., Jan. 2011.

[5] Sun Cloud Architecture Introduction White Paper (in Chinese).http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[6] S. Subashini, V.Kavitha. A survey on security issues in service deliverymodels of cloud computing. Journal of Network and ComputerApplications 34(2011)1-11.

[7] Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of TheCloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[8] Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About CloudComputing Security?" Technical Report No.UCB/EECS-2010-5. http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

[9] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_computing_security

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

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

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

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

[14] "IBM Discovers Encryption Scheme That Could Improve CloudSecurity, Spam Filtering," at http://www.eweek.com/c/a/Security/IBMUncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135413/.

[15] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E."Airavat: Security and privacy for MapReduce," In: Castro M, eds. Proc. of the 7th UsenixSymp. on Networked Systems Design andImplementation. San Jose: USENIX Association, 2010. 297.312.

[16] "OASIS Key Management Interoperability Protocol (KMIP)TC",http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip.

[17] Zeng K, "Publicly verifiable remote data integrity," In: Chen LQ, RyanMD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 2008. 419.434.

[18] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, "Ensuring DataStorage Security in Cloud Computing," in Proceedings of the 17thInternational Workshop on Quality of Service.2009:1-9.

[19] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory andimplementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop onCloud Computing Security, CCSW 2009, Co-Located with the 16thACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 43.54. [doi:10.1145/1655008.1655015]

[20] Muntés-Mulero V, Nin J. Privacy and anonymization for very largedatasets. In: Chen P, ed. Proc of the ACM 18th Int'l Conf. onInformation and Knowledge Management, CIKM 2009. New York:Association for Computing Machinery, 2009. 2117.2118. [doi:10.1145/1645953.1646333]

[21] RandikeGajanayake, Renato Iannella, and Tony Sahama, "Sharing withCare An Information Accountability Perspective," Internet Computing, IEEE, vol. 15, pp. 31-38, July-Aug. 2011.

[22] DoD, "National Industrial Security Program Operating Manual",5220.22-M, February 28, 2006.

[23] Richard Kissel, Matthew Scholl, Steven Skolochenko, Xing Li,"Guidelines for Media Sanitization," NIST Special Publication800-88,September2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.