IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 59-62
www.iosrjournals.org

Survey on Data Security and Integrity Issues in Cloud Computing

Sudhir Juare
sudhir.juare@raisoni.net, Coordinator & Assit. Prof.,
G. H. Raisoni Institute of Information Technology,
RTM Nagpur University, Nagpur(MS),India

Abstract *: Cloud Computing is scalable, fast, flexible, and cost effective technology platform for IT enabled services over the internet. There are various advantages of cloud computing but ultimately cloud service users have to put their data over the cloud i.e., third party servers which are not directly controlled by the data owner. But security and integrity of data is the major concern in cloud computing. So in this paper focuses on various issues regarding data security and integrity such as How cloud provides authentication and integrity over user's data?, How data stored over cloud storage servers will be protected from attackers? And many more such issue.*

Keywords *- Cloud Computing, Iaas, PaaS, SaaS, Secaas*

I. INTRODUCTION

Cloud Computing is a recent advancement wherein IT infrastructure and applications are provided as "Services" to end-users under a usage based payment model. There are many application areas of the cloud computing as the technology. The evolution of cloud computing enables organizations to reduce their expenditure on IT infrastructure and is advantageous to both the serving and served organizations. Various examples of cloud computing service providers are Google App Engine, IBM, Amazon, Microsoft Azure and many more.

Cloud Computing however suffers from various security issues as data owners store their data on external servers, there have been increasing demand and concerns for data confidentiality, authentication and access control. Cloud security is becoming a key differentiator and competitive edge between cloud providers. In spite of various benefits that are provided by the cloud computing services, cloud computing service users are very much afraid about the security of their data once it is over the cloud under the control of third party vendors.

II. CLOUD COMPUTING MODELS

There are three fundamental models are provided by Cloud computing providers:

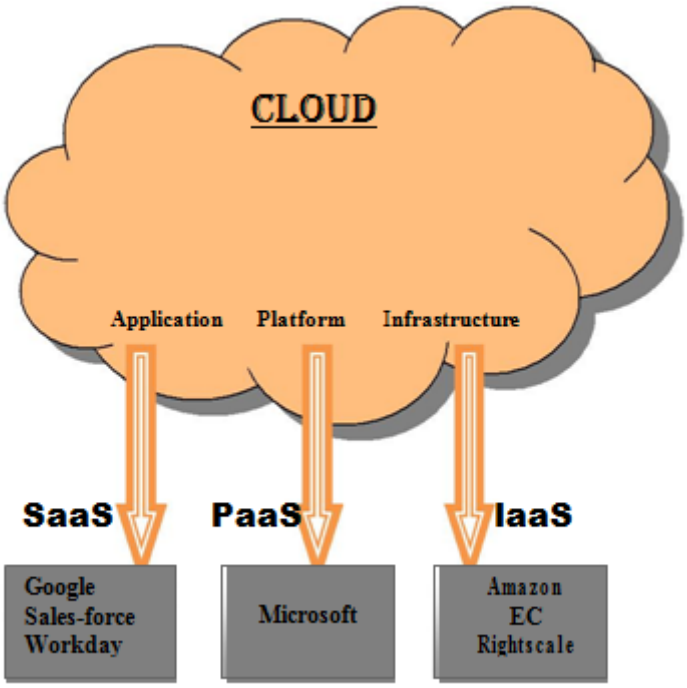
Infrastructure-as-a-Service(IaaS): Whole infrastructure to customer for processing, networking, storing and other computing services in which the customer can ran various software as well as operating systems or application based software is provided under this service model. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except selection of the some network component like host firewalls.

Software-as-a-Service(SaaS): Different types of application provided by service provider on a cloud environment under this service model**.** Clients are able to access these applications with the help of interfaces like web browsers or application interfaces. Cloud application services or "Software as a service" provide the function of software as a service over internet. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the some configuration setting for the application.

Platform-as-a-Service(PaaS): This service model provides the ability to the customer to deploy their application at the cloud environment with the use of programming and there is no need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the some configuration settings for the application where it is going to host. It also provide all the facility without the purchasing, managing and other cost of software and hardware[1].

Thus, cloud computing is advantageous to the enterprise and cost effective with the help of SaaS, PaaS and Iaas. However, one of the biggest in adoption of cloud is the lack of security. So to fulfill this security gap SecaaS has been introduced in the cloud computing.

Security-as-a-Service(SecaaS): The service model provides the management of security services across the internet but can provide some specialized information security service. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the selection services. By using this service the customer can access different set of services to address security[18].



III. DEPLOYMENT MODELS FOR CLOUD INFRASTRUCTURE

Cloud infrastructure can also be classified into different categories on basis of their deployment methods and scope of usage:

1. Private Cloud: private cloud (or internal cloud) is dedicated to the single organization comprising multiple customers and not shared with any other organizations. It is managed within the organization data centre and operated by internal employees.

2. *Public Cloud:* Public cloud (or external Clod) is open to use by multiple customer in the common environment. Public cloud is managed and operated by other organizations where the data will be shared among many organization s like academics, Government, Business organization or others.

3. *Hybrid Cloud:* A Hybrid Cloud environment is the combination of different private or/and public cloud providers. With the hybrid cloud, the organizations run their desensitize applications in the private cloud while the normal applications in the public cloud.

IV. DATA SECURITY AND INTEGRITY RISKS IN CLOUD COMPUTING

Data Integrity

Data integrity affects the accuracy of information maintained in the system. In a cloud computing model data validity, quality and security affect's the system's operations and desired outcomes. The program efficiency and performance are addressed by the integrity. An apt example for this would be that of a mobile phone service provider who stored all the customer's data including messages, contact lists etc in a Microsoft subsidiary [4]. The Provider lost the data and the cloud was unavailable. The customers had to wait until they got the necessary information from the cloud and the data was restored.

Data Security

Another key criterion in a cloud is the data security. Data has to be appropriately secured from the outside world. This is necessary to ensure that data is protected and is less prone to corruption. With cloud computing becoming an upcoming trend, a number of vulnerabilities could arise when the data is being

indiscriminately shared among the varied systems in cloud computing. Trust is an important factor which is missing in the present models as the service providers use diversified mechanisms which do not have proper security measures. The following sub section describes the risks factors in cloud environments

V. VARIOUS DATA SECURITY ISSUES

Many cloud service providers provide storage as a form of service. They take the data from the users and store them on large data centre, hence providing users a means of storage. Although these cloud service providers say that the data stored in the cloud is utmost safe but there have been cases when the data stored in these clouds have been modified or lost may be due to some security breach or some human error.

Various cloud service providers adopt different technologies to safeguard the data stored in their cloud. But the question is: Whether the data stored in these clouds is secure enough against any sort of security breach?

Various issues regarding security of data are as follows:

1. How data will be secure the data in transit and security of transmitted data can be achieved through various encryption and decryption schemes.
2. Another major issue that is mostly neglected is of Data-Eminences. It refers to the data left out in case of data transfer or data removal. It causes minimal security threats in private cloud computing offerings, however severe security issues may emerge out in case of public cloud offerings as a result of data-eminence.
3. How cloud provider will provides authentication and integrity over user's data.
4. How cloud provider able to protect stored users data in cloud storage servers form attackers. And how to protect private data from access of hackers whose aim is to hack the servers for access over private data.
5. How cloud users able to change cloud provider and transfer stored data from one cloud provider to another

The virtualized nature of cloud storage makes the traditional mechanisms unsuitable for handling the security issues. These service providers use different encryption techniques like public key encryption and private key encryption to secure the data resting in the cloud.

VI. VARIOUS DATA INTEGRITY ISSUES

Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other mali- cious users, and that any incorrect computing will be detected.

In Cloud Computing, the data required by the users are not stored on their own computers; instead they are stored on remote servers which are under the control of other hosts. To maintain our data in cloud, it may not be fully trustworthy because client doesn't have copy of all stored data. Thus cloud service provider must provide data integrity before and after the data update in cloud. For maintaining data integrity over cloud Digital Signatures can be used.

Various issues regarding data integrity are as follows:

1. *Data loss/manipulation:* One of the service of cloud computing is storage as a service. User keep heir large amount of data on the cloud servers, that data can be accessed on rare occasions. The cloud servers are distrusted in terms of both security and reliability [6], which means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss (e.g., backup and restore, data migration[2]). Additionally, adversaries may initiate attacks by taking advantage of data owners' loss of control over their own data[2].

Dishonest computation in remote servers: With outsourced computation, it is difficult to judge whether the computation is executed with high integrity. Since the computation details are not transparent enough to cloud customers, cloud servers may behave unfaithfully and return incorrect computing results.[2] .

3. Another issue regarding data integrity security is if during transmission attackers changes information i.e. a risk to integrity of data [13].

4. In case of cloud computing the location of data is unknown thus in case of any disaster the data can be lost thus there must be means to recover the data.

VII. CONCLUSION

With the increase in the growth of cloud computing, security needs to be analyzed frequently. The Users should be aware of the risks and vulnerabilities present in the current cloud computing environment before being a part of the environment. In This Paper We Have Identified The Most Data Security and Data Integrity Issues, Which May Be Considered In Cloud Computing Both By Users And Providers. Such As Maintaining Data Security And Integrity While Transmitting Data, Data Reminisce Problem, How To Protect Data Stored On The Cloud From Attackers, How User Of Cloud Can Change The Cloud Provider Etc.

.

REFERENCES

[1]. ”A Survey of Cloud Computing Security,Challenges and threats”,International Journal On Compuetr Science and Engineering(IJCSE) ISSN: 0975-3397 Vol.3 No.3 March2011.

[2]. XIAO and XIAO: Security and Privacy in Cloud Computing IEEE Communications Surveys & tutorials,1553-877X/12/$31.00 c2 012 IEEE [3].Security and Privacy policies of Sales-Force.com. http://trust.salesforce.com/trust/security/best_practices/http://trust.salesforce.c om/trust/privacy/tools/.

[3]. Cubrilovic N,“Letting Data die a natural death”, International Journal of electronic Government Research 2009Securing Your Data In Cloud- www.memset.com.

[4]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” SecureComm, 2008

[5]. “Cloud Computing Security Issues and Challenges” Kuyoro S. O.,

[6]. Ibikunle F. & Awodele O International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 247

[7]. “Data Security Model for Cloud Computing “ ISBN 978-952-5726-06-0 Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) © 2009 ACADEMY PUBLISHER 141 AP-PROC-CS-09CN004

[8]. ” A Survey on Security Issues in Cloud Computing”- Rohit Bhadauria(School of Electronics and Communications Engineering,Vellore Institute of Technology, Vellore, India), Rituparna Chaki, arxiv.org/pdf/1109.5388, 2011

[9]. Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessicca Staddon, Ryusuke Masuoka, Jesus Molina, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control,” Proc. of the ACM Workshop on Cloud Computing

[10]. Security, pp. 85-90, USA, November, 2009. ISBN: 978-1-60558-784-4. “Data Security over Cloud”, by D.H. patil, Rakesh R. Bhavsar, Akshay S.

[11]. Thorve, Emerging Trends in Computer Science and Information Technology-2012(ETCSIT2012),proceedings published in International Journal of Computer Aplications(IJCA).

[12]. ”Enabling public Auditability for Cloud Data Storage Security”, By Abirami G, Dhana sundari m, linda Joseph, International Journal of Computer Information systems, Vol. 3,No. 2,2012

[13]. ”Security issues occur in cloud computing and there security”, by Karamjit Singh et al.,International Journal on Computer science and Engineering(IJCSE), ISSN: 0975-3397,Vol.4 No.05, May 2012 Williams Stallings, Cryptography and Network security

[14]. A. Juels and B. S. Kaliski, “PORs: Proofs of retrievability for large files,” In ACM CCS, pages 584-597, 2007.

[15]. Z. Xiao and Y. Xiao, “Accountable MapReduce in Cloud Computing,” Proc. The IEEE International Workshop on Security in Computers, Networking and Communications (SCNC 2011) in conjunction with IEEE INFOCOM 2011.

[16]. http://elastic-security.com/2010/01/07/data-remanence-in-the-cloud/

[17]. ”A Novel Open Security Framework for Cloud Computing”, by Devki G. pal, ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh, International Journal of Cloud Computing and Services Sciences(IJ-CLOSER), Vol.1, No.2,June 2012, pp. 45~52, ISSN:2089-3337. [19]http://www.zapthink.com/2011/05/19/data-remanence-cloud-computing- shell-game/