Data Security in Cloud Computing

Sarika Dutta[1] Shaloo Kumari[2] Kirti Pandey[3] Pallab Banerjee[4] Biresh Kumar[5]
[1,2,3,4,5]Department of Computer Science and Engineering
[1,2,3,4,5]Amity University, Jharkhand, Ranchi, India

Abstract— Cloud computing is a latest technology that has evolved the IT industry. Cloud Computing provides the right to the user to access and store the data over internet. It also provides the right of using resources that are demanded through a computer network such as databases, email, file services etc. over the internet on a pay for use basis. It is a new concept that provides various digital and virtualized resources, hardware and software to the users. But it has different security issues. This paper discusses the various data security issues and techniques in cloud computing. There are various techniques which are used for data protection in cloud computing but there are various types of threats in this area. The main aim of this paper is to estimate and resolve the best security technique for protecting the data in cloud computing.

Keywords: Cloud Computing, Cloud Security, User Authentication

I. Introduction

Cloud computing is a term that originates from the telecommunication world. It provides the user a virtual computing environment that fulfill user's requirement. Cloud computing helps its consumer to get free from installing any type of application in their PC's. It's main motive is to use internet based service on behalf of the application that are installed in the user's computer. The users are charged whenever the use that service. There are various actions such as developing new application, storage, backup, recovery of data, delivery of software, hosting websites, video and audio streaming performed in cloud computing.

A. *Software as a service (SaaS):*

SaaS, or Software as a Service, is the uppermost layer of the Cloud. It is on top of both IaaS and PaaS. This layer offers applications, programs, software and web tools to end users and the end users have to pay for the time they have used. Microsoft is the best example of SaaS which provides us software like Microsoft office. Google is also the example of SaaS because it provides us software like Google chrome. CRMs, email and other office applications come under SaaS. Some services are free while some are billed monthly or per usage. To access the software, the end users should have a high-speed internet and no need to install the software on PC. Backend, resources and servers are managed by vendor. The end user does not need to maintain the software or handle the issues with security risk. SaaS is platform independence. The end user need not to be worry about the backend. Backend is handled by the vendor. Access to operating system, physical machine, virtual machine and virtual storage is not given to end users.

B. *Platform as a service (PaaS):*

PaaS, or Platform as a Service is basically the middle layer of the Cloud. This layer is mostly used by web developers, programmers, and coders for development. Vendors provides tools, runtime environment and programming language, by using this application is developed and deployed. PaaS works by developers renting raw hardware from an IaaS provider, no need to purchase expensive hardware and software. The customers create the applications by using the programming language. They don't manage the virtual server. They host the programs on the platform service they pay for. The management and maintenance of the operating. System and other hardware done by providers. Access to operating system, virtual machine, physical storage, data storage and virtual storage is not given to developer, only access to user interface, data related applications are given to developers. Only the developer should have high speed internet to create the applications. Access in PaaS in comparatively less as compared to IaaS but more in compare to SaaS. Only the developers has to pay for the resources they have used.

C. *Infrastructure as service (IaaS):*

IaaS is an important component of cloud computing along with software as a service (SaaS) and platform as a service (PaaS) Infrastructure as a service(IaaS) is a cloud computing that offers the vendors to provide the users to access the computing resources such as servers, storage and networking..

1) Key Features-

– Users pay for IaaS on demand instead of purchasing hardware.
– As data is present on the cloud so there is no chance of failure.
– It saves the cost of buying and maintaining their own hardware.
– It provides the virtualization of administrative tasks and frees up the time for other work.

IaaS is also known as Hardware as a Service (HaaS).IaaS cloud computing platform layer removes the requirement for every organization to maintain the IT infrastructure. IaaS is provided in three models: public, private and hybrid cloud. The private cloud states that the infrastructure is present at the customer premise. The public cloud states that the infrastructure is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which customer chooses the best between private cloud or public cloud. IaaS examples-Amazon Web services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE), Joyent.

II. Issues in the Security of Cloud Data

There are also some kind of risks challenging the security system of data in cloud computing. They are -

A. *Virtualization*

Virtualization is used in cloud computing to make a virtual platform of server operating system. It separates compute environments from physical devices setup and thus helps us to run multiple operating systems and other applications in the same device. Hypervisor is a part of it which can run a guest operating system making it work as virtual machine in the host operating system. The hypervisor but creates risks in data security when any damage occur to it because it can affect the whole system and data. There is also another risk associated with the virtualization is in the terms of allocating and de-allocating of the resources. If we want to reallocate memory next to a VM operation then the previous VM data operation must be cleared because if not done it would lead to data exposure next VM which would be not desirable. To solve these problems we should design proper virtualization where we use all the data carefully and authenticate data before de allocating the resources.

B. Data stored in the public cloud

The data stored in public cloud is a big risk because we keep data in a centralized manner of storing which can be easily accessed by the hackers. The storage resources are combinational outcome of the hardware and software devices that can expose the whole data even if there is a slight breach in the public cloud.

Therefore it is better to use private cloud in case of the extremely sensitive data to avoid the risks involved in public cloud.

C. Shared access

Shared access is a major risk to data in cloud computing because multiple users share the computing resources just like in case of CPU. Storage of data is a big problem for all users as it is common for all users in multitenancy. In this kind of situation there is always a bigger risk of data leak accidently even if there is fault in any one of the systems which can lead to access of all the data to another user or hacker causing a big problem for the whole system.

D. Privilege user access

Sometimes we have to share our private data to third party for improvement of data. Which is a major risk. We should ask providers to give us information about such that if any problem occurs we can contact them. Giving access to our data is risk so we should have knowledge that who are managing our data.

E. Regulatory compliance

Cloud is not responsible if any modification in data occurs, even when it is held by service providers. Customers are responsible for securing their private data from intruders. If any event occurs in the cloud then service provider will not take any responsibility.

F. Data location

When we use the cloud, we actually don’t know where our data is located. We don’t know in which country our data is hosted. So we should ask the providers to give us information about our data where it is kept and also make a contractual commitment to obey local privacy requirements on behalf of their customers.

G. Data segregation

Data in the cloud is in shared mode with data of others customers so there is a chance of mixing of data. The service providers should take assurity that encryption mechanism were designed and tested by experienced specialist. So the service provider should take responsibility that the data is encrypted and will not be mix with others data.

H. Recovery

We don’t know where our data is, so the cloud provider should tell us what will happen to our data in case if it is lost. The provider should take assurity that our data will be recovered. We should ask them how much duration will it take to restore the data.

I. Investigate support

Investigating illegal activity is not possible in cloud computing because there are billions of customers in cloud. It is not possible to find out who has deleted or modified our data. This is the main issue of security in clod computing.

J. Long term viability

Cloud computing provider will never go broke and consumed up by a larger company. But we must be sure that our data will be available even if any event occurs. So we should ask service providers how we will get our data back. So the trusted company should have data.

ISSUES	THREAT	SOLUTION
DATA CONFIDENTIALITY	In data confidentiality, the client never has a physical data so the privacy and confidentiality of the cloud data are at risk. The unauthorized party can access data due to which the data can be lost before receiving and it is not possible to investigate who has accessed the data. In this, someone can gain access to information who shouldn’t have access to it.	Data owner protects the data with a secret key and grants permission only to authorized receiver of the cloud and the data can be accessible by that secret key by the receiver if and only if it is known by the receiver. Data send by the sender will be divided into bits along with dummy bits such that if the intruder attacks the data then he will be confused which is the original data and also, they will not able to access the data without that secret key.
DATA INTEGRITY	In data integrity, the data is present in cloud so it can be read and altered by the unauthorized person who is an attacker. Due to this the actual data is changed and modified and the receiver receives the changed data and the actual data is lost which is a risk.	The sender will attach the check value with the message data and sends it to the receiver. The sender will continuously change the path of the message such that it cannot be tracked by the attacker and when it is received by the receiver, the receiver will check the check

		value send by the sender and then the receiver will also find the check value of the received message data and he will compare both the check values,if the check values are same ,it means that the data is not modified by any third party and the data is safe.
VIRTUALIZATION	Virtualization is used in cloud computing to make a virtual platform of server operating system. It separates compute environments from physical devices setup and thus helps us to run multiple operating systems and other applications in the same device. Hypervisor is a part of it which can run a guest operating system making it work as virtual machine in the host operating system. The hypervisor but creates risks in data security when any damage occur to it because it can affect the whole system and data. There is also another risk associated with the virtualization is in the terms of allocating and de-allocating of the resources. If we want to reallocate memory next to a VM operation then the previous VM data operation must be cleared because if not done it would lead to data exposure next VM which would be not desirable. To solve these problems we should design proper virtualization where we use all the data carefully and authenticate data before de allocating the resources.	The risk of virtualization can be minimized by having a proper and arranged management of policies, processes and all the possible guidelines in the meanwhile of the steps and management done to maintain the VM lifecycle by having secured self-services and automated scripts. There should be strict rules in the storage, creation and application of VM images and even any kind of alteration in previous format should be minimized and done only when there is a special requirement. The hypervisor can be made less prone to risks by making small changes in the whole configuration like we should look out for the unused physical devices and disconnect them and try to disable clipboard or file sharing services. There should be restricted access to the layers of virtualization, specially the hypervisor and APIs / CLIs in such sensitive operating system through firewalls which is capable to restrict console access.

Table 1: Threats and solution for cloud computing security

III. Conclusion

Cloud Computing is an emerging technology and it provides easy access to computing resources and storage infrastructure. It is a combination of various technologies that provides great possibilities and great abilities. Cloud computing is being defined a talked across various IT industry under various situations and with different definitions connected to it. Though it has come into existence at present but the future of the IT industry is going to be completely dependent on this concept. But with the increase in the cloud computing environment there are several risks present in it. There are many problems that need to be solved with the growth of cloud computing. The current obligations in the cloud model will increase the risk from the attackers. The threats in privacy protection is sharing data while protecting personal data. The capability to decide which information to reveal and who can access the information over the internet has become a burden. These burden consist whether the personal information can be stored or read by the third parties without authorization, or third parties can track the web sites someone has visited. One of the major concern of this paper is about data security and challenges and its solution in the cloud computing. There are various security issues discussed in this paper. To provide a secure and safe data access in the cloud various encryption techniques are used for storing and retrieving data from the cloud. This paper also tells us about the cloud concept and it's models and services which gives idea about the cloud abilities such as scalability, elasticity, platform independent, reliability and low cost. This paper has highlighted all the data security issues of cloud computing. So new security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture.

References

[1] Cloud Standards Customer Council (2016). Cloud Security Standards: What to Expect and What to Negotiate. http://www.cloud-council.org/deliverables/cloud-security-standards-what-to-expect- and-what- to-negotiate.htm

[2] L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas and F. AlDosari. 'A secure cloud computing model based on data classification.'Elsevier, pp 1153-1158, 2015.

[3] Cloud Standards Customer Council (2015). Practical Guide to Cloud Service Agreements. http://www.cloud council.org/deliverables/practical-guide-to- cloud-service-agreements.htm

[4] Rao, Leena. "Critical Skills Education SaaSEverFi Raises $10M From Jeff Bezos, Eric Schmidt, Ev Williams And Others." www.techcrunch.com.Techcrunch, 14 Aug 2012. Web. 26 Nov 2012.

[5] <http://techcrunch.com/2012/08/14/critical-skills-education-saas-everfi-raises-10m-from-jeff- bezos-ericschmidt-ev-williams-and-others/>.

[6] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.

[7] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, “Building safe PaaS clouds: A survey on security in multitenant software platforms,” Comput. Secur., vol. 31, no. 1, pp. 96–108, 2012.

[8] U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, “Security risks and their management in cloud computing,” 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.

[9] T. Mather, S. Kumaraswamy, and S. Latif, “Cloud Security and Privacy,” p. 299, 2009.

[10] F. Yahya, V. Chang, J. Walters, and B. Wills, “Security Challenges in Cloud Storage,” pp. 1–6, 2014.

[11] Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM

[12] Lipinski, T. A. (2013, September). Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements. In International Symposium on Information Management in a Changing