ORIGINAL RESEARCH PAPER

Computer Science

DATA SECURITY IN CLOUD COMPUTING: A CHALLENGING TASK

KEY WORDS: Cloud Computing, Security, Data-at-rest, Data-in-transit

Dr. Geeta Dalal Asst. Professor in Computer Science, Pt. N.R.S. Govt. College, Rohtak (Haryana).

Seema Sangwan Asst. Professor in Computer Science, Pt. N.R.S. Govt. College, Rohtak (Haryana).

Suman Asst. Professor in Computer Science, Govt. PG College for Women, Rohtak (Haryana).

ABSTRACT

In this paper we have elaborate and discusses about cloud data security which is really a challenging task. It is a study of data in the cloud and aspects related to it concerning major security. Cloud computing is used by many of the organizations for storing the huge amount of data on the clouds and using over the networks. Therefore, there is need to secure the data which may in the form of text, audio, video, etc. There are numerous algorithms designed by the researchers for securing the data on the cloud. Cloud Computing domain is so wide that it is impossible to deal with all of its aspects. In this paper, we focus on aspects related to Cloud computing security and more particularly, we are interested in the security of data hosted on Cloud infrastructures. As more and more information from individuals and organizations are placed on the Cloud, the issue regarding data security and user privacy becomes an important concern, especially when data is sensitive.

INTRODUCTION

The word Cloud Computing has appeared newly and it is not is common use of the several of definitions are exists on the existing scenario, one of the simplest is, "a network solution for providing inexpensive, reliable, easy and simple access to IT resources". Cloud Computing is not think as application oriented but service oriented. This service oriented character of Cloud Computing is not only cuts the overhead of infrastructure and charge of ownership but also provides elasticity and enhanced performance to the end user.

A main concern of cloud data is security and privacy. It is extremely vital for the cloud service to make sure the data integrity, privacy and protection. For this purpose, several service providers are using diverse policies and mechanism that depends upon the nature, type and also size of data. One of the main question while using cloud for storing data is whether to use a third party cloud service or create an internal organizational cloud. So, the data is additional sensitive to be stored on a public cloud, like, defense and national security data or more confidential future product details etc. This type of data can be extremely sensitive and the consequences of exposing this data on a public cloud can be severe. So, it is suggested to store data using internal organizational cloud. This approach can facilitate in securing data by enforcing on premises data usage policy. However, it still does not guarantee full data security and privacy,

DATA SECURITY ISSUES CLASSIFICATION

Data security is a common concern to all technologies. However, it becomes a major challenge when applied to an uncontrolled environment like Cloud Computing. It is important to distinguish between the security risks associated with all IT infrastructures and those introduced by the use of Cloud Computing. These risks are generally associated with open, shared and distributed environments. Therefore, when analyzing the risks, it is important to separate existing problems from those raised by Cloud Computing.

In this paper, we deal only with issues introduced by the Cloud, and related to data. Data outsourced to Cloud infrastructure is more vulnerable than that stored on a traditional infrastructure, mainly for these reasons:

- Data is stored on the service provider's infrastructure
- Data of different users shares the same physical infrastructure
- Data is accessible via internet.

DATA SECURITY IN CLOUD COMPUTING

Data security in cloud computing involves more than data encryption. Requirements for data security depend upon on the three service models SaaS, PaaS, and IaaS. Two states of data normally have threat to its security in clouds; Data at Rest which means the data stored in the cloud and Data in Transit which means data that is moving in and out of the cloud. Confidentiality and Integrity of data is based upon the nature of data protection mechanisms, procedures, and processes. The most significant matter is the exposure of data in above mentioned two states.

DATA AT REST

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

DATA IN TRANSIT

Data in transit normally refers to data which is moving in and out of the cloud. This data can be in the form of a file or database stored on the cloud and can be requested for use at some other location. Whenever, data is uploaded to the cloud, the data at time of being uploaded is called data in transit. Data in transit can be very sensitive data like user names and passwords and can be encrypted at times. However, data in unencrypted form is also data in transit

DATA-IN-USE

Data-in-use refers to any reading or processing (creation, transformation or deletion) of data. When processing take place in the Cloud, the risks of misuse increase, due to the large number of users involved in Cloud

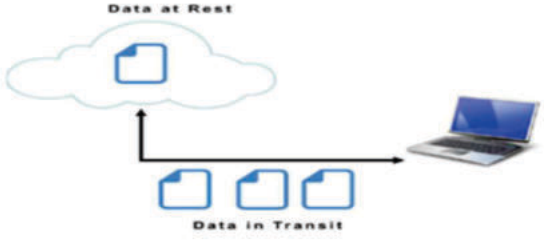

Fig 1: Data At Rest And In Transit.

DATA ISSUES ACCORDING TO CLOUD DATA LIFE CYCLE

Calculation and storage are the two basic services provided by Cloud Computing. Data storage is distributed over a number of Datacenters around the world. Data calculation is carried out by virtual machines. Users can create different virtual machines, with different capacities and numbers to suit their needs. The transfer of data calculation and storage to a third part involves the transfer of responsibility associated with their security and compliance to this third part.

The calculation in the Cloud takes place as follows: the user first submits his data to the datacenter that is stored and managed by storage service. This data is then sent to the virtual machines for parallel processing using the corresponding distributed technology. After the end of processing, users can download and view the results. During this process, all private or confidential data may be disclosed.

RISKS ASSOCIATED AND DATA SECURITY ATTRIBUTES

The first risk concerns the sharing of physical infrastructure between different users. Given, multiple users share the same physical storage space, data security risks increase and affect many users. Unauthorized access by a service provider or its customers (other users) is therefore a serious problem, especially, when data is sensitive

Although the security requirements differ from one data type to another (data-at-rest, data-in-transit, data-at-use). They all share a basic concept that is CIA trio: Confidentiality, Integrity, and Availability, but applied to a distributed, virtualized and dynamic architecture. These three principles are used by all security measures that are intended to protect one or more aspects of this trio. The majority of literature papers dealing with data security discuss these three points.

CONFIDENTIALITY

Confidentiality refers to data protection from unauthorized access. These problems occur when sensitive data is outsourced to the Cloud server. In a decentralized Computing context, the issues of confidentiality are much more important since the server hosting the data does not necessarily belong to the user. Confidentiality in Cloud systems is a major barrier to his adoption. Currently, Cloud offers are mainly public and therefore exposed to more attacks, compared to those hosted on private data centers

INTEGRITY

Integrity refers to data protection from unauthorized changes, whether intentional or accidental. These changes include creating, deleting, and writing. Data integrity is one of the critical elements in most information systems. It can be simple to perform in a centralized system, but becomes a complex task in a distributed environment such as Cloud Computing

AVAILABILITY

Data availability means that information must be available when authorized persons need it. Data availability is one of the biggest concerns of service providers. If for some reason a Cloud service is interrupted, many clients will be affected. Service providers contractually undertake to ensure an availability level of 99.9%. In addition, the duplication of data and physical resources and their distribution on different locations increases the level of availability

CONCLUSION AND FUTURE SCOPE

Data security in cloud computing a headache for now the days because of mostly work to be done online and the data also keep online on cloud, so the above facts cloud computing become a popular field in 21st century cloud users.

REFERENCES

1. Sharma Anjali and Sinha Garima, An Efficient Approach on Data Security with Cloud Computing Environment: A Comprehensive Research, *Turkish Journal of Computer and Mathematics Education Vol.12 No.14 (2021), 1372 – 1382*
2. J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," *Build. Infrastructure. Cloud Secur.*, vol. 1, no. September 2011, pp. 3–22, 2014.
3. An, Y.Z., Zaaba, Z.F., Samsudin, N.F.: Reviews on security issues and challenges in cloud computing. In: IOP Conference Series: Materials Science and Engineering, vol. 160, p. 012106. IOP Publishing (2016)
4. Arjun, U., Vinay, S.: A short review on data security and privacy issues in cloud computing. In: IEEE International Conference on Current Trends in Advanced Computing, pp. 1–5. IEEE (2016)
5. J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.
6. Balogh, Z., Turčáni, M.: Modeling of data security in cloud computing. In: IEEE Annual Systems Conference, pp. 1–6. IEEE (2016)
7. Bhabad, A.V., Heda, J.R., Dhatrak, V.N., Shahane, G.P., Shirole, B.S: Data confidentiality and security in Cloud Computing using KIST algorithm. Int. J. Emerg. Trends Sci. Technol. 1 (2016). 2456-0006