ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

Review of Cloud computing Security and data sharing challenges

1. A.Manimuthu, 2.P.Peter Jose 3.Dr. G.Murugaboopathi

#1Research Scholar, Department of Computer Science, Bharathiyar University, Coimbatore, Tamilnadu

#2Research Scholar, Department of Computer Science, Bharathiyar University, Coimbatore, Tamilnadu

#3Associate Professor, Department of Computer Science and Enginering, Kalasalingam University, Krishnankoil, Tamilnadu

Abstract

Cloud computing is a type of computing that relies on *sharing computing* Computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machineCloud computing has quickly developed and spreadin the previous couple of years, with constantly new administrations and functionalities being offered by suppliers keeping in mind the end goal to increase bigger market divisions. This has brought on as a rule a great deal of trouble and perplexity to clients who have been regularly subjected to the ”vendor lock-in”phenomenon,because of interoperability and portability issues frequently emerging among various Cloud suppliers. In this paper we give a brief prologue to the essential definitions of Cloud Computing, portability and interoperability and we additionally
portray an arrangement of built up utilize cases. Every one of these ideas are mapped to a multi-dimensional space, which is utilized to order both definitions and utilize cases

resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid

Introduction

The term “cloud”, as used in this white paper, appears to have its origins in network diagrams that represented the

internet, or various parts of it, as schematic clouds. “Cloud computing” was coined for what happens when applications and services are moved into the internet “cloud.” Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Many companies are delivering

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

services from the cloud. Some notable examples as of 2010 include the following:

• **Google** — Has a private cloud that it uses for delivering many different services to its users, including email access, document applications, text translations, maps, web analytics, and much more.

• **Microsoft** — Has Microsoft® Sharepoint® online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud. • Salesforce.com — Runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services. But, what is cloud computing? The following sections note cloud and cloud computing characteristics, services models, deployment models, benefits, and challenges

General Cloud Computing Challenges

Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. Some common challenges are:

1. **Data Protection**
   Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them. Cloud Computing Page 6 of 6
2. **Data Recovery and Availability**
   All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support Appropriate clustering and Fail over Data Replication System monitoring (Transactions monitoring, logs monitoring and others) Maintenance (Runtime Governance) Disaster recovery Capacity and performance management If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.
3. **Management Capabilities**
   Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling" for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

4. **Regulatory and Compliance**
Restrictions In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers. With cloud computing, the action moves to the interface — that is, to the interface between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation — areas that many enterprises are only modestly equipped to handle

The Challenges of Secure Cloud Storage

Many big name cloud storage services have been under scrutiny of late; they don't seem to be able to provide the secure cloud storage and privacy they promise (one of the most recent big offenders under fire is Dropbox). Investigations and studies are being performed to test just how effective these sites are at ensuring our data safety in various situations, and many have been found sorely lacking when it comes to privacy, data leaks, and encryption

Data Leak Issues

Bring Your Own Device, or BYOD, is a popular strategy to bring business up to speed today and allow for a versatile, flexible enterprise, and we all understand the importance of using this technology effectively yet securely. The latest revelation with regard to Dropbox or similar programs and BYOD is that files deleted from mobile devices aren't always truly gone. Researchers found that documents, audio files, images, and more were able to be recovered even though they were thought to be permanently deleted both from the device and from the cloud. Another disconcerting discovery was that metadata such as user activity history could also be found with a little digging. In addition to these findings there have always been issues of hackers, and the fact that your data is stored on a shared server with other customers using these "secure cloud storage" companies. Encryption is their answer to this charge, but even that isn't fool proof. There are just too many chances that your data will leak when you go with one of these public server storage cloud options. The only way to know just how protected you are is to have your own cloud storage under your security measures and protectionPublic Server Storage Means No Data Privacy

When it comes to using a cloud storage service, you have no control over where they are storing your data. They own the servers and they will distribute your files however it is convenient, which can be a big security hazard. You might be using strong encryption for everything you send, but what about your account credentials?

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

When you share server space, your credentials could be shared with others on this server, or vulnerable to theft. Then, while they probably couldn't un-encrypt your data, they could start deleting things. Other malicious people might nose in on your data transmission and watch your activity. None of us wants to be spied on or have malicious strangers manipulating our data. This is another issue which can be solved by having your own cloud on a company server, where you can be in charge. Then your files will never be out of your own control and management.

Encryption Isn't Guaranteed

Another problem which has recently been discovered with some of the popular cloud storage companies is a flaw in encryption protection. Many businesses like to use the cloud not only for secure storage but also as a safe sharing and collaboration method. It was discovered, however, that when data is shared between two or more users in the cloud, it is vulnerable to attack by employees of the cloud storage company itself. They can use a fake key to unlock the data when it is sent for sharing and view it before re-encrypting it and sending it to the intended viewer. While no actual instances of this have been found as of yet, the possibility is discomfiting. Secure cloud storage companies can no longer boast of a "zero-knowledge environment" for your data. You simply have to trust that the cloud service won't peek into your files. This is just another inherent danger of public server cloud storage. Control Your Own Secure Cloud Storage Rather than putting the safety and security of your files outside of your domain, you can have your own cloud on a server within your company. This means that your IT department handles security and your data safety is protected behind your own firewalls and privacy policies. You shouldn't have to be at the mercy of your storage provider for protection which they can't quite guarantee. Take a look at how own Cloud can help you control your own secure cloud storage today.

THE SECURITY SCHEMES FOR DATA SHARING

This section discusses the state of the art schemes for data sharing over untrusted cloud providers. We classify the schemes into three categories, which are encryption and key management techniques, efficient searching methods over encrypted data, and data access control schemes.

Data Integrity

Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen.

Data integrity is easily achieved in a standalone system with a single database. Data integrity in the standalone system is maintained via database constraints and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

transactions, which is usually finished by a database management system (DBMS). Transactions should follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity.Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.Owing to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third party supervision mechanism besides users and cloud service providers.

Verifying the integrity of data in the cloud remotely is the perquisite to deploy applications. Bowers et al. proposed a theoretical framework "Proofs of Retrievability" to realize the remote data integrity checking by combining error correction code and spot-checking .The HAIL system uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realize the availability and integrity checking .Schiffman et al. proposed trusted platform module (TPM) remote checking to check the data integrity remotely

Data Confidentiality

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness .Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

complex requirements such as query, parallel modification, and fine-grained authorization.

Distributive Storage

Distributive storage of data is also a promising approach in the cloud environment. AlZain et al. discussed the security issues related to data privacy in the cloud computing including integrity of data, intrusion, and availability of service in the cloud. To ensure the data integrity, one option could be to store data in multiple clouds or cloud databases. The data to be protected from internal or external unauthorized access are divided into chunks and Shamir's secret algorithm is used to generate a polynomial function against each chunk. Ram and Sreenivaasan.have proposed a technique known as security as a service for securing cloud data. The proposed technique can achieve maximum security by dividing the user's data into pieces. These data chunks are then encrypted and stored in separated databases which follow the concept of data distribution over cloud. Because each segment of data is encrypted and separately distributed in databases over cloud, this provides enhanced security against different types of attacks.Arfeen et al. describe the distribution of resources for cloud computing based on the tailored active measurement. The tailored measurement technique is based on the network design and the specific routes for the incoming and outgoing traffic and gradually changing the resources according to the user needs. Tailored measurement depends on the computing resources and storage resources. Because of the variable nature of networks, the allocation of resources at a particular time based on the tailored active method does not remain optimal. The resources may increase or decrease, so the system has to optimize changes in the user requirement either offline or on-line and the resource connectivity

Conclusion:

In This paper discussed about the challenges in the cloud storage and cloud data sharing in the modemera. this review help to know the issue facing int the current cloud trend in feature research may solve these problem and make cloud as more efficient to the cloud user

Reference

[1]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.

[2] N. Sengupta and R. Chinnasamy.'Contriving hybrid DESCAST algorithm for cloud security.'Elsevier, pp 47-56, 2015.

[3] S.K. Sood. 'Hybrid data security model for cloud.'International Journal of Cloud Applications and Computing, pp 50-59,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

2013.[4] J.J. Hwang, Taoyuan, Taiwan, Y.C. Hsu and C.H. Wu.'A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service.'International Conference on Information Science and Applications (ICISA), pp 1-7, 2011.

[5] J. Lai, R H Deng, C. Guan and J. Weng.'Attribute-Based Encryption with Verifiable Outsourced Decryption.' IEEE Trans. Inf. Forens. Security, vol 8, pp 1343-1354, 2013.

[6] F. Moghaddam F, Karimi O and Alrashdan M T. 'A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments.' Proceedings IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, USA, pp 185-189, 2013.

[7] W. Liu. 'Research on cloud computing security problem and strategy.'IEEE, pp 1216-1219, 2012.

[8] A. Behl and K. Behl.'An analysis of cloud computing security issues.'IEEE World Congress on Information and Communication Technologies, pp 109-114, 20122011.[10] J.K. Wang and X. Jia. 'Data security and authentication in hybrid cloud computing