ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

A Survey on Access Control of Cloud Data

Ms Reshma Sadasivan, Mrs K.Sangeetha, Dr S.Karthik

***Abstract*-Among the emerging technologies, cloud computing provides a flexible, on-demand computing infrastructure for a number of applications. Cloud computing is about moving computing from the single desktop pc/data centres to internet. In cloud computing, user's data can be put it in the cloud storage and it can be access from the cloud, by the users whenever and wherever they needed. The major feature of the cloud is that user's data are processed in remote machines, which are unknown to the data owners. Here the security problems are raised. Users fear about their data control, so that they needed to account their data, which are stored in cloud. It can provide accountability for cloud data by using a framework called Cloud Information Accountability (CIA). Here it uses Java Archives (JAR) files for automatically log the usage of user's data. To strengthen user's control, it can provide distributed auditing mechanism and also can provide authentication of JAR, it allows the developer to develop powerful application even after they modify the code and the code of the copied code by the attacker.**

***Index Terms*- Accountability; Cloud Security; Data Sharing, JAR File**

I. INTRODUCTION

Cloud Computing is a subscription-based service where you can obtain networked storage space and computer resources. In cloud computing model customers plug into the cloud to access IT resources which are priced and provided on-demand services. This cloud model composed of five essential characteristics, three service models and four deployment models. Users can store their data in cloud and there is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. Here we must ensure the security of user's data, which is in cloud. Users prefer only the cloud which can be trusted. In order to increase the trust in cloud storage, the concept of accountability can be used.

Manuscript received Sep 15, 2012.

Reshma Sadasivan, Computer Science and Engineering, Anna University, Chennai, SNS College of Technology,.kollam,India,09489822889

***Mrs K.Sangeetha**, Computer Science and Engineering, Anna University, Chennai, SNS College of Technology.,Coimbatore,India,09976288435*

***Dr.S.Karthik**, Computer Science and Engineering, Anna University, Chennai, SNS College of Technology., Coimbatore,India,0422-2666264*

Accountability is likely to become a core concept in cloud that increase the trust in cloud computing. It helps to trace the user's data, protecting sensitive and confidential information, enhancing user's trust in cloud computing.

II. ESSENTIAL CHARACTERISTICS

a. **On-demand service**-consumers can use web services to accesscomputing resources on-demand as needed automatically
b. **Broad network access-can access** Services from any internet connected device
c. **Resource Pooling**-customers can share a pool of computing resources with other customers
d. **Rapid Elasticity**-enables computing resources or user account to be rapidly and elastically provisioned
e. **Measured Service**-control and optimize services based on metering and automatically monitor the resources

III. SERVICE MODELS

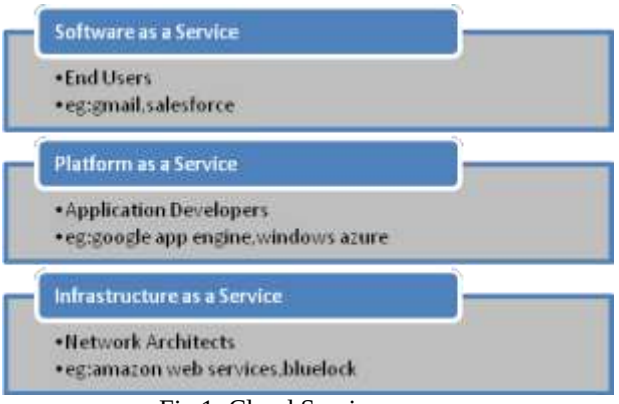

Fig 1: Cloud Services

i. *Software as a service (SaaS):* The capacity provided to the consumer is to use the provider's applications running on a cloud infrastructure. The application is accessible from client devices through web browser
ii. *Platform as a service (PaaS):* The capability provided to the consumer is to deploy onto the cloud infrastructure

consumer created or acquired application created using programming language and tools supported by the provider

iii. **Infrastructure as a service (IaaS):** The capability provided to the consumer is to provision processing, storage, network and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating system and application

IV.DEPOLYMENT MODELS

a. Public Clouds**:** Public cloud computing services are provided off-premise to the general public and the computing resources are shared with the provider's other customers.

b. Community Clouds: Cloud infrastructure shared by several organisation that have shared concern, managed by organisation or third party.

c. Private Clouds: Cloud infrastructure for single organisation only, may be managed by the organisation or third party, on or off premise.

d. Hybrid Clouds**:** It use public clouds for general computing while customer data is kept within a private cloud.

V. CLOUD SECURITY

Cloud stores mass amount of user's data, there is a critical need to be secured that data. The owner of the data does not aware about where their data is stored and they do not have control of where data is placed. Here it explores the security challenges in cloud. Some of the security risks include secure data transfer, secure software interface, secure stored data, user access control, data separation. To promote privacy and security concern of end users accountability mechanism is used. Here the basic concept is that user's private data are sent to the cloud in an encrypted form, and then with the encrypted data processing is carried out.

VI. ACCOUNTABILITY IN CLOUD

Accountability become a core concept in cloud that helps to increase trust in cloud computing. The term Accountability[1] refers to a narrow and imprecise requirement that met by reporting and auditing mechanisms. Accountability is the agreement to act as a responsible proctor of the personal information of others, totake responsibility for protection and appropriate use of that information beyond legal requirements, and to be accountable for misuse of that information. Prospective accountability use preventive controls. Preventive controls for the cloud include risk analysis and decision support tools, policy enforcement, trust assessment, obfuscation techniques, identity management. Retrospective accountability use detective controls. Detective controls for the cloud include auditing, tracking, reporting and monitoring. Accountability in cloud focuses on keeping the data usage transparent and track able.

VII. RELATED WORKS

i. DATA STORAGE SECURITY IN CLOUD

In cloud data storage, user's data are stored in cloud. There third party maintains everything from running the cloud to storing data. Outsourcing of data into the cloud reduces the cost and complexity of long term large scale data storage, but it does not offer guarantee on data integrity and availability[10]. So that here proposed a trusted computing environment that provides secure cross platform. It includes the security services authentication, encryption and decryption and compression.

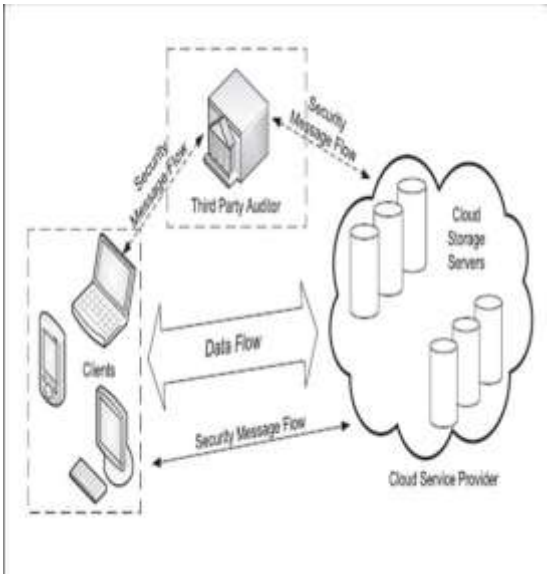

Fig 2: Architecture of cloud data storage

The network consists of three backup sites that can be useful for recovery after disaster. Backup site placed at remote location from the main server. During backup sites the encrypted files are created and data are compressed. And the data will be decrypted during recovery operation. In cloud must ensure authentication for data for security.

ii. DATA SECURITY IN CLOUD COMPUTING WITH ELLIPTIC CURVE CRYPTOGRAPHY

In cloud, the stored data must be secured. There are many security risks that include data location, data segregation, and recovery etc. Cloud data are usually transferring between cloud storage and users. The user doesn't know the exact location where the data are storing. Here authentication and encryption can be provided to the data with elliptic curve cryptography[5]. Authentication is needed when sending data from one cloud to other. To provide message authentication digital signature is used. Elliptic curve cryptography can provide confidentiality and authentication of data between clouds.

iii. ACCESS CONTROL BASED SECURITY IN CLOUD

Cloud storage has several merits over traditional data storage. Cloud storage can able to get access from any location that has internet access. While storing data in cloud there is a possibility for leakage of data loss. Here hybrid cloud infrastructure is used with cryptographic approach [2]. In this, confidential data are encrypted and uploaded on cloud from client. It can provide an encryption solution to protect files and allow users to view and edit the encrypted file stored in cloud[4].

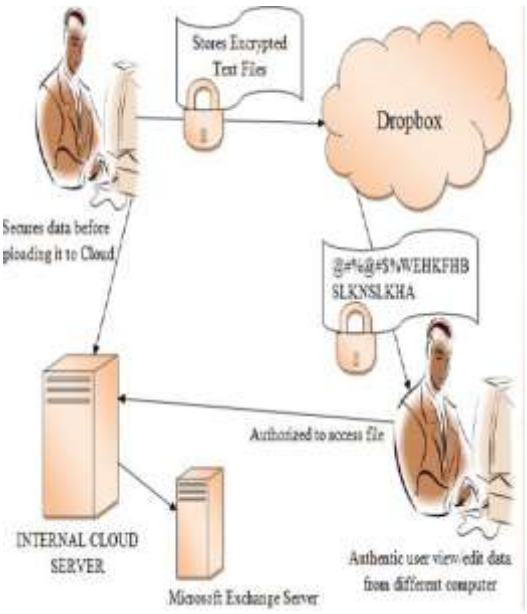

Fig 3: Design of hybrid cloud infrastructure

Here public cloud acts as a storage cloud. For this it use Drop box that can provide a cloud based service. Private cloud is used for the authentication, key management and access control.

iv. A FRAMEWORK FOR ACCOUNTABILITY TRUST IN CLOUD

In cloud storage there is no assurance for security of data. Customers prefer only cloud storage which can be trust. Here it introduced user rights for user agreement that can ensure trust in cloud storage, so that it can avoid cluster authentication method. For auditing purpose Third Party Auditor (TPA) is used[7]. Security can be provided by using encrypting the password and also can hack the entrusted users IP address and TPA stores the IP in restricted IP table.

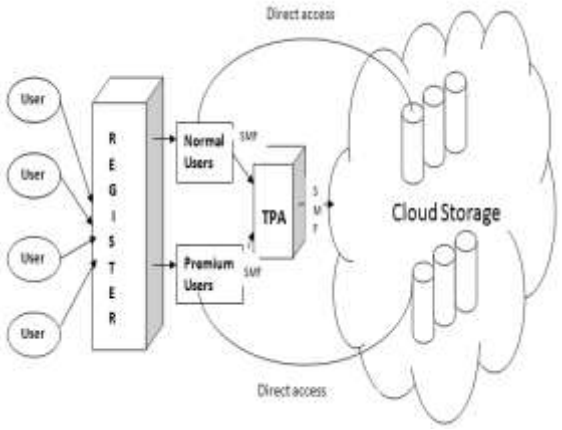

Fig 4: Architecture of proposed cloud storage

In cluster group tag authentication, same amount should be paid for even limited usage. Here in the proposed system client need to pay for they use. It can allow increasing the speed of the data transmission and trust in cloud and also can reducing expense.

v. SECURE ROLE BASED DATA ACCESS CONTROL IN CLOUD

To be kept cloud as secure here cryptographic techniques are used. By using these techniques secure, scalable and fine grained access control on outsourced data can be achieved. Cryptographic techniques included are Key Policy Attribute-Based Encryption (KP-ABE), Proxy Re- Encryption (PRE) and Lazy Re encryption[6]. KP- ABE can enforce access control and it can protect data encryption key of data file. PRE combines with KP-ABE and then enable data owner to delegate the computation operation to cloud server without relieving the file contents. Lazy re encryption techniques is used for reducing the computation overhead on cloud server and also to aggregate multiple secret key file re encryption into one.

vi. DISTRIBUTE ACCOUNTABILITY FOR DATA SHARING IN CLOUD

As the data owners are unaware of

the location where their data are stored, they want to keep track their data for knowing whether data is secure or not. Here a framework is used know as Cloud Information Accountability (CIA). It can provide end to end accountability in distributed fashion and also it combines with access control,usage control and authentication. For auditing two modes are included. Push mode refers to logs being periodically sent to the data owners. Pull mode refers to logs that can retrieve by the user.

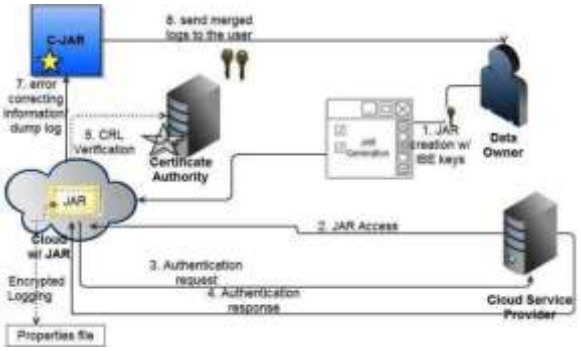

Fig 5: CIA frame work

Here Java Archives (JAR) files are used for automatically log the usage of the user data. JAR file includes user's data and their policies such as access control policies and logging policies. By using this framework it helps to increase the trustiness of cloud.

VIII. EXISTING SYSTEM

Cloud storage must be handling with full care of security. Cloud security can include access control, usage control and authentication. Considering the above related works cloud security can be provided by using many methods. Among that the most efficient mechanism is providing accountability for cloud data.By using CIA framework it trace the control of data by the data owner. Here the user, who subscribed to a certain cloud service, usually needs to send his data as well associated access control policies to the service provider after the data are received by the cloud service provider, the service provider will have granted access right, such as read, write and copy on the data.

Using conventional access control mechanisms, once the access right are granted, the data will be fully available at the service provider. In order to track the actual usage of the data, logging and auditing technique is developed. The most intuitive attack is that the attacker copies entire JAR files. The attacker may assume that allow accessing the data in the JAR file without being noticed by the data owner. such attacks will be detected by our auditing mechanism. But it does not enable the data owner to audit even those copies of its data that were made without his knowledge.

IX. PROPOSED SYSTEM

Generally many security schemes have been implemented to address the security issues. This is based on the restricted access to all portable applications to a system of authentication in which different levels of permission will be given based on whether the application can be authenticated as having come from the trusted source. In existing scheme they have used X.509 certificate to denote the authentication instead here implementing the signed Application Descriptor File (ADF) which is used to authenticate a portable application code.

This allows the developer to develop powerful applications even they can modify the code and audit the code of the copied code by the attacker because the application have more access to the computer resources of the client machine. This work is relates in general to portable code transfer, such as java technology, and more particularly to provide security and authentication of portable code for use by mobile device or other computing devices relatively limited computing resources and limited communication bandwidth.

X.CONCLUSION

In cloud computing, we can ensure the trustiness of cloud by using accountability. CIA can provide access and usage control with authentication. Accountability is used for tacking the data that means tracing the control of data. We can use JAR files that contain user's data and their policies.

JAR file can be authenticated; so that it allows the developer to develop more powerful applications even modify the code and audit the code of the copied code by the attacker. It includes advantages are can able to distribute applications to many different mobile devices, information gathering capabilities is high and portability.

REFERENCE

[1] Andreas Haeberlen,"A case for accountable cloud", Max Planck Institute for Software Systems (MPI-SWS) Cloud Security Alliance. (2010). CloudAudit .The Automated Audit, Assertion,

Assessment, and Assurance API)
Available: http://cloudaudit.org/

[2] Sonam Chugh and Sateesh Kumar Peddoju, "AccessControlBased Data Security in Cloud Computing", Vol. 2, Issue 3, May-Jun 2012, pp.2589-2593

[3] Eric Keller, Ruby B. Lee and Jennifer Rexford," Accountability in Hosted Virtual Networks",

[4] Jinhui Yao and Chen Wang,"Accountability as a service for data

[5] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi " Data Security in Cloud Computing with Elliptic Curve Cryptography ", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[6] V Sathya Preiya, R.Pavithra, Joshi, "SECURE ROLE BASED DATA ACCESS CONTROL IN CLOUD COMPUTING", International Journal of Computer Trends and Technology May to June 2011

[7] Ms P.M Kiruthika, Ms T.Amirtha and Mrs R.Deepa,"Aframework for accountability and trust in cloud computing", International Journal of Communications and Engineering Volume 01-NO.1,Issue 03 March 2012

[8] Kyriacos E.Payolu and Richard T.Snodgrass," Achieving database information accountability in the cloud computing", Arizon

[9] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray Siani Pearson,"TrustCloud:A framework for Accountability and trust in cloud computing"

[10] S.Sajithabanu and E.Geogre Prakesh Raj,"Data storage security in cloud ", IJCST vol 2, issue 4, oct dec 2011

[11] Q.Wang, C. Wang, J.Li, K.Ren and W.Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing 14th European symp. Research in computer security (ESORICS'09),pp.355-370,2009

[12] D.J Weitzner, H .Abekson, T.Berners-Lee, J. Feigenbaum, J.Hendler and G.J sussman,"Information accountability" communication of the ACM,vol 51, no 6,pp 82-87,junew 2008

[13] A.R Yumerefendi, J.S Chase strong accountability for network storage. ACM Transaction on storage, volume 3,issue 3,article no 11,2007

[14] Y.Zhang, K.J Lin, T.Yu. Accountability in service-oriented architecture:computing with reasoning and reputation . In proc IEEE International conference on e-Business Engineering,pp 123-131,2006.

[15] 104th United stated congress, Health insurance probability and accountability act of 1996 (HIPPA)"

Ms Reshma Sadasivan is doing 11nd year Masters of Engineering in Computer Science and E ngineering, SNS College of Technology, affiliated to Anna University Chennai, Tamilnadu, India. She received the B.E degree from The Raajas Engineering College affiliated to Anna University Thirunelveli. Her research interest includes cloud computing and its security. She is an active member of ISTE

Mrs. K.Sangeetha is presently Assistant Professor at Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University-Chennai, Tamilnadu, India. She received the B.E degree from Sasuri College of Engineering and M.E degree from Nandha Engineering college. Currently she is pursuing her doctoral degree in Anna University Chennai. Her research interests includes datamining and networking. She published papers in international journals , nationa and international l conference.

Professor Dr.S.Karthik is presently Professor & Dean in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University-Coimbatore, Tamilnadu, India. He received the M.E degree from the Anna University Chennai and Ph.D degree from Ann University of Technology, Coimbatore. His research interests include network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.