International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 2 193 - 196

Single Cloud Security Enhancement using key Sharing Algorithm

Mrs. Vijaya Pinjarkar
University of Mumbai,
Information Technology Dept,
K.J.S.I.E.I.T.,
Mumbai, India
vkhirodkar@somaiya.edu

Mr. Neeraj Raja
University of Mumbai,
Information Technology Dept,
K.J.S.I.E.I.T.,
Mumbai, India
neeraj.raja@somaiya.edu

Mr. Krunal Jha
University of Mumbai,
Information Technology Dept,
K.J.S.I.E.I.T
Mumbai, India
krunal.jha@somaiya.edu

Mr. Ankeet Dalvi
University of Mumbai,
Faculty of Information Tech.Dept,
K.J.S.I.E.I.T.,
Mumbai, India
ankeet.dalvi@somaiya.edu

Abstract- The use of Cloud Computing (CC) has increased rapidly in many institutions. Few of the advantages of CC is cloud data storage, where the customers do not have to store their data on their remote servers, but the data is stored on the cloud service provider's (CSP) side. To this end, security in Cloud computing is taken to be one of the most important aspects due to the sensitive and confidential information stored in the remote database(cloud) by the users. Our paper signifies a model to securely store information into the cloud in a manner that preserves data confidentiality, integrity and ensures availability. Our approach ensures the security and privacy of client sensitive information by storing data across single cloud, using a secret sharing approach that uses Shamir's secret sharing key algorithm. The model avoids an unauthorized access and reduces the consequences of encryption techniques.

*****

I. INTRODUCTION

The cloud computing is a cost-effective, service which is, flexible, highly available and on demand service delivery platform for providing business through the internet. Cloud computing resources can be quickly extracted and processed easily. Services and applications provisioned on demand service despite the user location or device. Hence, the opportunity for an organization is to enhance their delivery of services efficiently is achieved through cloud computing. The issues in cloud security series forms substantial security of the cloud fixing through the architectural security of function and data deployed, to the security of the cloud framework implemented in the presence of peripheral attacks and the mechanisms accessible to, respond to these attacks. Privacy and security must be addressed by cloud computing providers for higher and urgent priorities.

1. AIMS AND OBJECTIVES

Aim: The data security aspect of cloud computing, data and information will be shared with a third party without any hacks. Every cloud users will avoid use of untrusted cloud service provider for use of debit/credit cards details or medical report from hackers or malicious insiders.

Secret key algorithm provides secure cloud database that will prevent security risks. We apply Shamir's Secret Sharing algorithm in cloud that helps to reduce risk of data intrusion and service availability for ensuring data.

OBJECTIVE:
While making a cloud secure, the following objectives are to be met:

Aware ourself's, the cloud computing environment provided by the cloud service provider. The cloud computing solution must meet the basic security and privacy needs of any firm deploying it.

The privacy of the cloud and data security of applications must be maintained as that are deployed in cloud computing environment. Cloud services has to maintain data Integrity and service Availability. The user runs customer applications using the service provider's resources.

II. LITERATURE REVIEW

NIST describes cloud computing as "a model for enabling, on-demand network access to a shared configurable computing resources in a convenient manner(e.g., servers, networks, storage, web service applications) that can be made available and released with minimum management effort or service provider interaction.

EXISTING SYSTEM:
User is an entity, who stores data in the cloud and relies on the cloud for the data storage and computation, can be either personal information or an enterprise. As users data growing in size and importance data redundancy can be employed with a technique of erasure correcting code to further reduce faults or server crash The existing system

users makes use of cloud storage for better communication and cost.

2.1 Existing System V/S Proposed System:

EXISTING SYSTEM	PROPOSED SYSTEM
Existing systems provides simple password authentication.	Proposed system will use authentication as well as Key sharing algorithm for confidentiality.
The existing system does not have proper filtration	The proposed design allows the user to audit the cloud storage with better computation cost and communication
The existing system cannot securely store data.	The proposed system further supports secure and efficient dynamic operation on outsourced data, including manage control such as Block modification. Deletion Append security

LIMITATION

The problem of the malicious insider in the clouding infrastructure which is the base of cloud computing.

A set of virtual machines provided by IaaS cloud providers from which the user can benefit by running software. The existing solutions to ensure data confidentiality by data encryption is not sufficient just because of the fact that if the data has been encrypted the user's information can't be manipulated in the virtual machines of cloud providers. Administrators manage the infrastructure and as they have remote access to servers, if the administrators is a malicious insider, then he can gain access to the user's data[6]. In addition, they assume that if the data is processed and gathered from different client then the data encryption cannot ensure privacy in the cloud. Even though the cloud providers are aware of the malicious insider danger, they assume that they have critical alternative to prevent the problem. For example, the solution is to prevent any physical access to the servers. However, the attackers outlined in their work have remote access and do not need any physical access to the servers. Another solution is to monitor all access to the servers in a cloud where theuser's data is stored. However, this mechanism is beneficial for monitoring employee's behavior in terms of whether they are following the privacy policy of the company or not, but it is not effective because it detects the problem after it has happened[6][8][1].

III. PROBLEM DEFINITION:

3.1 Detailed statement of problem:

Our project accomplishes unique purpose. It is basically an undertaking requiring concerted effort that has defined beginning and end in time.

Security is a necessary service for wired network as well as wireless network communication to improve what was offered in cloud .Simply storing the information on clouds solves the problem is not about data availability, but about security. Having multiple copies of files into multiple clouds it will just create many entries for intruders to see in. Representation of Shamir's secret sharing or secret splitting is away for distributing a secret among a group of n participants, each of the user is given a part of the secret key, in our case, a piece of data. The strong point of this method is that the secret key have to be combined by reconstructing by predefined number of shares; individual shares are of no use on their own, so anyone with less t from n shares has no information about the secret key than someone with 0 shares.

IV. DESCRIPTION OF THE PROJECT

We are going to analyze our proposed database model, which enables storing information on cloud transparently to the user. Furthermore, during this section we are going to examine several security risks such as: data integrity, data intrusion and service availability.

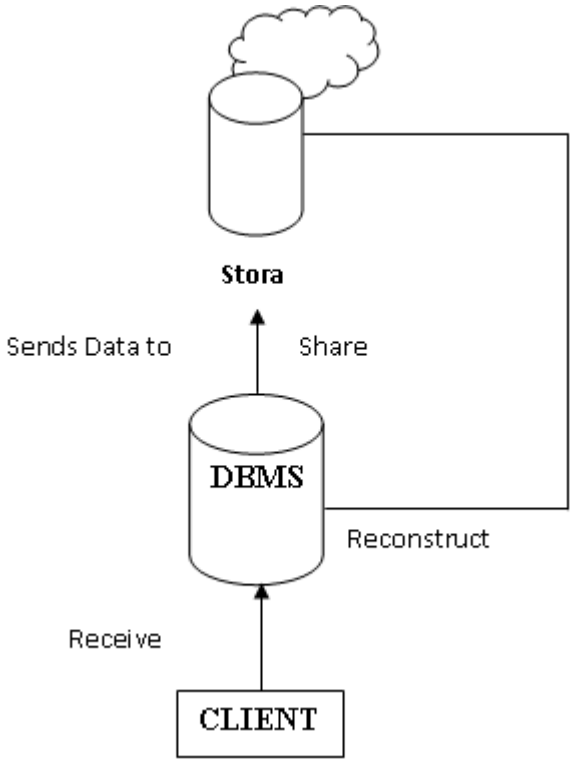

FIG 4.1:-Proposed Architecture

Cloud customers from their expectations based on their past information and needs. Some sort of survey is conducted before selecting a cloud service vendor. Customers are expected to do security checks based on three security concept: confidentiality, integrity and availability. Also cloud service providers may promise a lot to entice a customer to sign a deal, overwhelming barriers to keep their promises but some gaps may manifest later. Many potential cloud customers are well aware of the security, and still

sitting on the sidelines. If all gaps are within acceptable limits then only will not take cloud computing unless they get a clear indication. All relevant information is studied into cloud computing security in a diagram which is presented in following figure. We organized cloud computing security into following sectors: security types, security in service delivery models and also security dimensions. Security in cloud services is based on the following: Security is possible around strong network then there is service delivery platform Data encryption: for data in, and sometimes stored files, but it cannot be applied to data in use. Access controls to see that unauthorized users can't access to applications, data and the processing environment and is the primary means of securing cloud-based services.

Modules of the Project

Admin Module
Admin Login
Manage Users
Upload file and select 3 different keys for encryption
Share File
Select user to whom file have to share
Select file name which have to share
Select database number from which data is share
User will get the 16 digit key for decryption and 10 secret keys for authentication.

User Module
User Login
View Share File names
Try to download
Enter 16 digit key for decryption
Enter 8 digits 6 keys for authentication
If keys matches download the file
Else pop up message "invalid authentication keys".
Change password

ALGORITHM:
SECRET SHARING STRATEGY

Simply storing the information on cloud solves the problem of data availability, but what about security?

Having many copies of data into various clouds it will just create multiple entries for intruders to hack in. Therefore, we need to make sure that the data shipped to cloud is safer. This is when we apply the secret sharing algorithm presented by Adi Shamir[2]. Invented in 1979, the algorithm has occupied a huge place in the area of cryptography. The author discussed the problem of information distributing with the purpose of showing that there is an orthogonal approach which depends on information distribution rather than encryption [3]. The need of a secure communication between two endpoints challenged most of the work on data security. The mathematical evolution behind the algorithm is more complicated, that's where the secret sharing algorithm of Shamir depends – in its simple implementation. Shamir's secret sharing or secret splitting tells a different method for distribute with a secret key among a group of n users, each of whom is allocated a part of the secret, in our case, a piece of data[3]. The strong point of this method is that the secret can be reconstructed only when a all ready defined many shares are merged together; individual shares are of no use on their own, so anyone with fewer than too out of n shared key not has any additional information about the secret than someone with 0 shares. For example, consider a secret sharing scheme in which our information to be protected is "academia". This word is divided into the shares: A person with 0 shares knows that the word consists of eight letters. He would have to guess the word from 268 = 208 billion possible combinations. If he has one share, then the interval is narrowing down to 266 = 308 million combinations, and so on. Thus, an user with fewer than t shares is able to reduce the problem of gaining the inner secret without first requiring to obtain all the necessary shares[1][2].

V. CONCLUSION

The benefits of single cloud are clear, minimizing the risk of physical infrastructure deployment, reducing cost of entry, reducing the execution and response time of applications, Even though CC is extensively researched, security still represents the major issue of it. To this end, this paper focuses on the issues related to the security aspects of cloud and aims at facilitating a new model which uses single cloud service providers (CSP) and Shamir's secret sharing algorithm to prevent and overcome all the shortcomings of a existing cloud model such as data intergrity, user authentication.

REFERENCE

[1] International Data Corporation: IDC's Cloud Computing and Datacenter Roadshow 2013. [online] http:// idc-cema.com/eng/events/52888-idc-s-cloud-computing-and-datacenter-roadshow-2013, 2013.[cited: January-2014].
[2] Multi-Clouds Database: A New Model to Provide Security in Cloud Computing, Ion Morozan, Amsterdam, The Netherlands.
[3] Cloud Computing Security: From Single to Multi-Clouds, Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom*,RMIT University
[4] An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds, Md Kausar Alam, Sharmila Banu K. School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India.
[5] D. Agrawal, A. Abbadi, F. Emekci and, A. Metwally, Database Management as a Service: Challenges and Opportunities., Proceedings of the 2009 IEEE International Conference on Data Engineering, pp 1709–1716, April, 2009.
[6] A. Bessani, M. Correia, B. Quaresma, F. Andr and P.Sousa, DepSky: dependable and secure storage in a cloud-of-clouds, EuroSys, pp. 31–46, 2011.
[7] M. ALzain, and E. Pardede, Using Multi Shares for Ensuring Privacy in Database-as-a-Service, Proceedings of (HICSS), IEEE, pp. 1–9, 2011.