A New Framework for Cloud Computing security using Secret Sharing Algorithm over Single to Multi-Clouds.

Venkatarao Matte[1], L. Ravi Kumar[2]

[1]pursuing M.Tech(CSE) from Holy Mary Institute of Technology and Science(HITS), Keesara, A.P. affiliated to JNTU Hyderabad.

[2] working as an Assistant Professor in Department of CSE at Holy Mary Institute of Technology and Science(HITS), Keesara, A.P. affiliated to JNTU Hyderabad.

Abstract: **Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for the Internet, so the phrase-- are delivered to an organization's computers cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications and devices through the Internet. Presently implementation of cloud computing has increased rapidly in IT industry and in other organization also. Cloud is a collection of distributed database. It provides number of benefit such that low cost and accessibility of data. If a data is store only at single place and unfortunately that data has been lost then there is no recovery of data. Cloud computing gives us a solution to store a number of copy of data, in this manner if a data is going to be loss at one place that can be retrieved from other place. The problem of service unavailability has been solved by using cloud computing, which was a major concern in single cloud. In recently days use of multi cloud becoming popular because its provide the major benefit of service availability. As much of benefit coming with multi- cloud computing, that much security issues also coming with it. A cloud user is storing their information in clouds, those cloud provider can be untrusted, the information stored by user can be sensitive and in cloud there may be a chances of availability of malicious and anomaly which can harm user sensitive data. So security of data in multi-cloud computing is a major concern. In this paper we are going to discuss about functionality of single and multi cloud computing and security threats. In several researches on fact is coming out that the work done for maintainability of multi cloud security concern is less than the cost and work dome for single cloud. This research promotes the use of multiclouds due to ability of reducing security threats that affect the sensitive data of user.**

In this paper we will give a solution for security concern of data in multiclouds. Here we will show that in respect of storing user actual data , we are going to store encrypted data in cloud for which we will use plain cipher encryption algorithm of cryptography.

Keyword- **Cloud computing, single cloud, mutli-cloud, security, cryptography.**

I-INTRODUCTION

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

To do this, cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Cloud computing become a big invention of internet in today's world. By using cloud computing a user can access his service any where any time. The flexibility of storing and retrieving data becoming so fast. In traditionally approach of storing data , user string his data at single place which is not accessible from all where ,and once if that data is loss from that place its impossible to take that back. This issue known as service unavailability. Solution of this come as a cloud computing. A cloud is pool of number of distributed database which are linked together in a distributed environment. There is cloud owner or cloud manager which having control over all databases , these databases known as cloud. Cloud computing provide a huge benefit to user. Cloud computing provides facilities for user to develop and manage their own applications on the cloud ,this enhance the concept of virtualization of resources. Through virtualization resources are managed by themselves. The implementation of cloud computer increased widely in organization. Cloud computing has started to obtain mass appeal in corporate data centers as it enables the data center to operate like the Internet through the

process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner. For a small and medium size business , the benefits of cloud computing is currently driving adoption. In the SMB sector there is often a lack of time and financial resources to purchase, deploy and maintain an infrastructure. In cloud computing, small businesses can access these resources and expand or shrink services as business needs change. The common pay-as-you-go subscription model is designed to let SMBs easily add or remove services and you typically will only pay for what you do use.

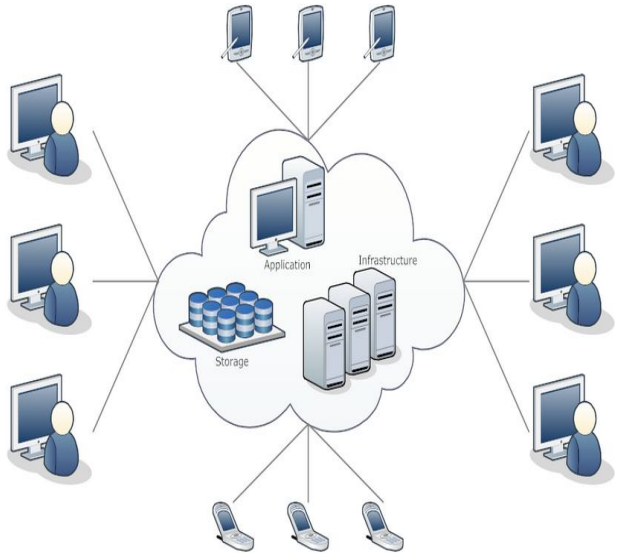

Fig 1-Cloud Computing

As the use of cloud computing increased widely, the resposiblity of cloud provider also increases. Cloud provider should focus on privacy and security issues as a matter of high concern. When a user using a single cloud, the issue of service unavailability and potential coming front and there is a possibility of malicious attack in single cloud. In recent time it has been viewed that the use of multi cloud in respect of using single cloud becoming popular. Multi cloud also known as intercloud or cloud of clouds. In fig-1 we have shown an architecture of multiclouds.

Normally in cloud computing user of cloud give their data to cloud manager and also give the information that in how many cloud data should have to store. Cloud manager having communication with numerous of clouds , he store the information given by user to some of those clouds and also give the accessibility control to user. Whenever user want to retrieve his data he can retrieve from any of those cloud which increases the potential and availability of data.

The information or data which are store inside clouds can contain sensitive information. The cloud provider all the time not trusted, they can be untrusted which make a security threat to user data. Hence security become a major concern in cloud computing. In this paper we are presenting a technique by using which we can assure sensitivity of data will not loose. For making security from single to multi cloud we are going to use cryptographic technique. In coming section we will explain about how we can implement cryptography techniques for providing security in cloud computing from single to multi clouds.

II- SECURITY RISK

In this section we will discuss about security risk in cloud computing. There is number of security threats in cloud computing. For example-

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems

Above explained security threats can be handle by cloud manager responsibility. Here mainly we will discuss about threats in single clouds which are Data Integrity,Data Intrusion and Service availability.

A.Data Integrity- In computing, data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle and is an important feature of a database or RDBMS system. Data integrity means that the data contained in the database is accurate and reliable. Data warehousing and business intelligence in general demand the accuracy, validity and correctness of data despite hardware failures, software bugs or human error. Data that has integrity is identically maintained during any operation, such as transfer, storage or retrieval. All characteristics of data, including business rules, rules for how pieces of data relate dates, definitions and lineage must be correct for its data integrity to be complete. When functions operate on the data, the functions must ensure integrity. Examples include transforming the data, storing history and storing metadata. Data integrity contains guidelines for data retention, specifying or guaranteeing the length of time of data can be retained in a particular database. It specifies what can be done with data values when its validity or usefulness expires. In order to achieve data integrity, these rules are consistently and routinely applied to all data entering the system, and any relaxation of enforcement could cause errors in the data. Implementing checks on the data as close as possible to the source of input (such as human data entry), causes less erroneous data to enter the system. Strict enforcement of data integrity rules causes the error rates to be lower, resulting in time saved troubleshooting and tracing erroneous data and the errors it causes algorithms.

B.Data Intrusion-Attacks on systems and data are a reality in the world we live in. Detecting and responding to those

attacks has become the norm and is considered due diligence when it comes to security. As a matter of fact, most of the standards and regulations applied in the technology space today have explicit instructions regarding the need for monitoring and alerting, or intrusion detection.

C.Service Availability- An user is storing their data for future use. In future whenever user of that data want to retrieve that information the data should retrieve by user without any disturbance this phenomena is known as service availability. Some time due to limited resources or because of some intruder attack that data will not reach to user on time this is known as service unavailability. In single cloud service unavailability is a major threat , multi cloud computing is a better solution for service availability concern.

In order to reduce the risk in cloud storage,customers can use cryptographic methods to protect the stored data in the cloud . Using a hash function is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data . If the amount of data is large, then a hash tree is the solution . Many storage system prototypes have implemented hash tree functions, such that this is an active area in research on cryptographic
methods for stored data authentication. Although the previous methods allow consumers to ensure the integrity of their data which has been returned by servers, they do not guarantee that the server will answer a query without knowing what that query is and whether the data is stored correctly in the server or not. Proofs of Retrievability (PORs) and Proofs of Data Possession (PDP) are protocols to ensure high probability for the retrieval of the user's data using multiple cloud providers to ensure data integrity in cloud storage and running Byzantine-fault-tolerant protocols on them where each cloud maintains a single replica. Computing resources are required in this approach and not only storage in the cloud, such a service provided in Amazon EC2, whereas if only storage service is available, working with Byzantine Quorum Systems by using Byzantine Disk Paxo and using at least four different clouds in order to ensure users' atomicity operations and to avoid the risk of one cloud failure. As mentioned earlier, the loss of availability of service is considered one of the main limitations in cloud computing and it has been addressed by storing the data on several clouds. The loss of customer data has caused many problems for many users such as the problem that occurred in October 2009 when the contacts, photos, etc. of many users of the Sidekick service in Microsoft were lost for several days. Data encryption is considered the solution to address the problem of the loss of privacy. They argue that to protect the stored data from a malicious insider, users should encrypt data before it is stored in the cloud. As the data will be accessed by distributed applications, the DepSky system stores the cryptographic keys in the cloud by using the secret sharing algorithm to hide the value of the keys from a malicious insider.

Hence we can say that security threat is going to be down as we moving from single to multi cloud.

III- SYSTEM IMPLEMENTATION

In this section we describe our implementation work for making security concern by using multi-clouds computing environment. In this architecture there are multiclouds environment in which there is a cloud owner or cloud manager who making communication and control all clouds. A cloud user or cloud consumer want to store his information to cloud and also want to store his data in number of cloud for service availability concern and potential purpose. An user will give his data with the information regarding number of storage to cloud manager , cloud manager will check his data and also check his metadata and store that information to clouds according to consumer need, because all clouds are not trustworthy , there may be a chance to attack on information and that information can be sensitive, for security of that we user here cryptography technique to secure our data in cloud. Here we used encryption and decryption technique of cryptography. Cryptography is a tool to secure our data from attacker, in this technique the original data is change into another form by using some keys ,and that form can not be understand by anyone. When that data needed in original form by using keys we can decrypt that data in original data. So if any attacker taking user data in clouds he cannot use that data and data will be in secured way. Here we used plain cipher encryption technology of cryptography for encryption and decryption techniques.

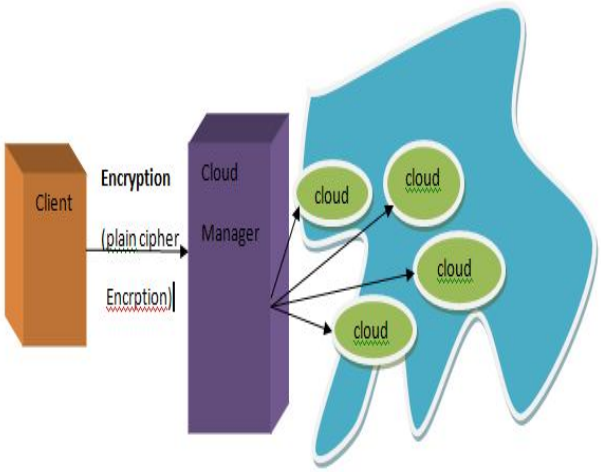

Fig 2-Multi cloud system architecture using plain cipher encryption

A. *Plain Cipher Algorithm*-Plain cipher encryption technique is an implementation of cryptography. It is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

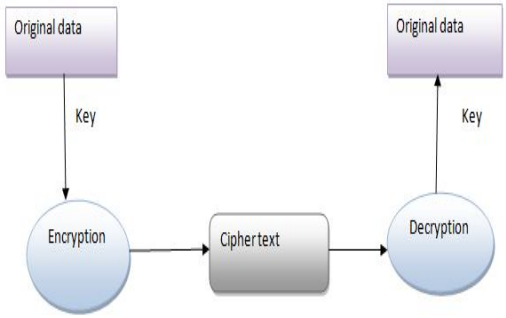

Fig 3-Plain cipher cryptography

Algorithm- Plain cipher

INPUT- original data,key

Step 1-convert original data in corresponding byte format by using ASCII value of each letter.

For ex- let original data is-'hello' and key is 'A'.

ASCII value-104,101,108,108,111

Step 2-convert key to corresponding ASCII value and subtract this value to each letter corresponding ASCII value.

Ex- key ASCII-64

Adding to original -40,37,44,44,47

Step 3-change resultant data into corresponding original format which will be known as cipher text

Ex-

Original value will be- (% ' ' /(cipher text).

Step 4-Store this data to cloud

Step 5-For decryption follow vice versa process.

Ex-

Key value is-A(64)

Cipher text is-(% ' ' / (40,37,44,44,47)

Add key ASCII to cipher ASCII –

104,101,108,108,111.

Convert into character- hello(original data).

IV-EXPERIMENTAL EVALUATION

In this section we are going to compare different related work which we did in implementation of our project. Here we are going to show the security related work for cloud computing from single to multi cloud.

Year	Cloud Security	Addressed Security Risks: Data integrity	Addressed Security Risks: Data intrusion	Addressed Security Risks: Service availability	Privacy/ Security Mechanism	Type of cloud: Single cloud	Type of cloud: Multi clouds	Type of service: Cloud storage	Type of service: Cloud database
2011	√	√			Multi shares+ secret sharing algorithm				
2011	√	√	√	√	DepSky,(Byzantine + secret sharing + cryptography)		√	√	
2011	√ survey	√				√		√	
2010	√				RAID-like techniques+ introduced RACS		√	√	
2010	√	√			ICStore ,(client-centric distributed protocols)		√	√	
2010	√			√	SPORC, (fork)	√			
2010	√								
2010	√				cryptography	√		√	
2010					Depot, (FJC)	√		√	

Fig 4-Experimental evaluation

The problem of the malicious insider in the cloud infrastructure which is the base of cloud . IaaS cloud providers provide the users with a set of virtual machines from which the user can benefit by running software on them. The traditional solution to ensure data confidentiality by data encryption is not sufficient due to the fact that the user's data needs to be manipulated in the virtual machines of cloud

providers which cannot happen if the data has been encrypted . Administrators manage the infrastructure and as they have remote access to servers, if the administrator is a malicious insider, then he can gain access to the user's data present some negative aspects of data encryption in cloud computing. In addition, they assume that if the data is processed from different clients, data encryption cannot ensure privacy in the cloud.

V-CONCLUSION

It is totally clear from above discussion that the use of cloud computing is increasing very widely in current world. Most of the organization starts using cloud services for storing their information. Security also becomes a major concern in cloud computing environment. Customer does not want to lose their private information as a result of malicious intruder inside cloud. Service unavailability was also a big concern due to which multi clouds phenomena has came. Security also was a concern in multi-cloud environment. But potential of multi cloud is better than single cloud. For giving security to user sensitive data we proposed here Plain cipher cryptographic technique in multi-cloud computing. We also showed the experimental evaluation of proposed system from existing one. Hence we can assume that this proposed system will be very useful in multi-cloud computing environment for providing security to user information with potential service availability.

REFFERENCES

K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.

K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.

C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.

M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.

G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.

Clavister, "Security in the cloud", Clavister White Paper, 2008.

A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp. 1-14.

S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.

AUTHORS PROFILE

Venkatarao Matte, Pursuing M.Tech(CSE) from Holy Mary Institute of Technology and Science(HITS) Keesara A.P. affiliated with JNTU Hyderabad.

L. Ravi Kumar , is working as a Assistant Professor of CSE department at Holy Mary Institute of Technology and Science(HITS) Keesara A.P. affiliated with JNTU Hyderabad.