A FRAMEWORK TO ENSURE DATA STORAGE SECURITY IN CLOUD COMPUTING TO PROVIDE ERROR LOCALIZATION AND REDUCE THE COMMUNICATION DELAY

[1] *UJVAL GADHAVI,* [2] *DR. VIPUL VEKARIYA*

[1] Student of M.E. (CE), Noble group of institutions, Junagadh, Gujarat, India
[2] Associate professor, Computer engineering, Noble group of institutions, Junagadh,

ujval.gadhavi@ngivbt.edu.in, vp@ngivbt.edu.in

Abstract— Cloud Computing is a future age innovation for IT undertaking. It has diverse qualities like virtualization, multi-client, versatility and some more. It likewise gives on request computational foundation which has the ability to decrease the cost to manufacture the IT based administrations. It can give different sorts of administration over the web. One of the imperative administrations is given by the cloud is capacity where clients can keep their information according to the necessity. In this way, it is a testing issue for the client as every one of the information are put away in some between associated asset pool yet this asset pool are arranged over better places of the world. Unapproved clients might may be got to this information through virtual machines. Along these lines, it is an extremely dim side of cloud information stockpiling; this weakness makes a major issue for clients. Cloud computing information security is a noteworthy issue. With a specific end goal to understand the information security in cloud computing, we have proposed a structure which provide error localization and reduce the communication delay.

Keywords— Cloud computing, Infrastructure as a Service, Error Localization, Latency, Communication Delay

1.INTRODUCTION

Cloud computing has been defined as a model of enabling Ubiquitous, convenient, cheapest, on-demand network access to a shared pool of configurable computing resources (like: networks, servers, storage devices and services) that can be rapidly provisioned and it needs minimal management effort or service provider interaction [1]. Users have the provision to use such type of environment without investing the capital in such infrastructure. Even, recourses can be accessible from any part of the world using any computing devices by any authorized user. It can manage the recourses such as allocate or reallocate resources dynamically and has the ability to monitor their performance continuously [1].

Though there are several types of services are providing the cloud but Data store is one of the latest features which is providing by the cloud to the client companies or any other users. But due to the lack of proper security control policy and weakness in protection, many clients are not ready to implement cloud computing technology. The superior of cloud computing providers are Amazon Simple Storage services (S3) and Amazon Elastic Compute Cloud (EC2) [2]. Amazon S3 is providing a simple web services interface and, at any time, from any location it can store and retrieve large amount of data using the web. Amazon uses to run its own global network web services which can be access as it is highly scalable, reliable, fast, inexpensive infrastructure. So, data security is a very important aspect of good quality of services and cloud computing faces the challenge of security threats for number of reasons. Firstly adopting the traditional cryptographic approach for the aim of data security in cloud computing is a threat as the data are stored in remote location and users do not have any control on it. So, it requires a data verification approach and it has no explicit knowledge about the whole data. So, it is very tough to verify the actual data. It is very difficult to verify the correctness of data storage in the cloud as it is located in third party's location. Secondly, the data are stored in third-party data warehouse and the data may be frequently updated by the user, including modification, deletion, insertion, appending, recovering and other operation. So, we need a more dynamic advanced technology operation to prevent data loss from the cloud storage. Lastly, but it is not the last as data centers which are running in simultaneously in distributed manner[1] and all data are stored in different physical locations, so it is very important to give correctness assurance in the distributed protocols. The following aspects are summarized as our contributions on: Firstly, an error localization schemes based framework is proposed to check whether the error in data or not in the cloud. It is generating a linear combination of selected data. These should check the error in data from cloud storage. These schemes incorporate check the data correctness in cloud. Secondly, a latency aware scheduling policy based framework is proposed to check latency in data in the cloud.

2.LITERATURE REVIEW

A. Cloud Computing: Preliminary

Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics and more—over the Internet ("the cloud"). Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage, similar to how you are billed for water or electricity at home. There is mainly four Deployment models: 1) Public Cloud, 2) Private Cloud, 3) Hybrid Cloud and 4) Community Cloud. In cloud computing mainly three service models: 1) Infrastructure as a Service, 2) Platform as a Service and 3) Software as a Service.[1]

B. Security Concern in Cloud

Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

C. Latency in Cloud

Cloud service latency is the delay between a client request and a cloud service provider's response. Latency is a networking term to describe the total time it takes a data packet to travel from one node to another. In other contexts, when a data packet is transmitted and returned back to its source, the total time for the round trip is known as latency. Latency refers to time interval or delay when a system component is waiting for another system component to do something. This duration of time is called latency.

3.PROPOSED WROK

Here in our system we take Error Localization and Latency Aware Scheduling algorithm. Our system architecture for error localization is shown in bellow fig. 1.

D. Error Localization

Error localization is a key prerequisite for eliminating errors in storage systems. However, many previous schemes do not explicitly consider the problem of data error localization, thus only provide binary results for the storage verification. Our scheme outperforms those by integrating the correctness verification and error localization in our challenge-response protocol: the response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate potential data error(s).

.

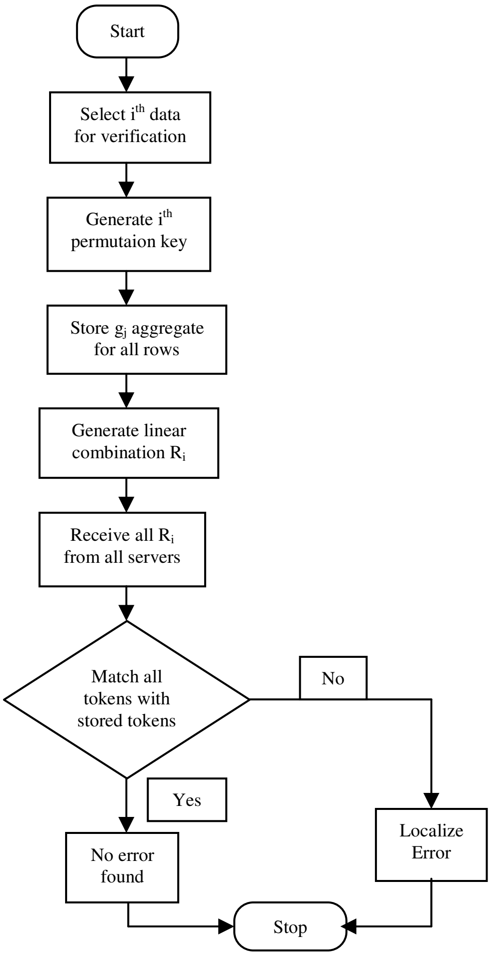
Start
Select ith data for verification
Generate ith permutaion key
Store g_j aggregate for all rows
Generate linear combination R_i
Receive all R_i from all servers
Match all tokens with stored tokens
No
Yes
No error found
Localize Error
Stop

Fig.1. System Architecture for error localization

E. Latency

It is a research issue on the Internet. Any performance in the cloud is undergoing the same meaning of the performance of the result on the client. The latency is compressed back to get clarity as to how and where they are running with both smartly-written applications and an intelligently planned infrastructure.

The latency in a cloud introduces not to be tedious. In future, cloud computing capacity and cloud based applications are bound to increase at a very rapid rate, and thus increase in latency. Cloud latency must be improved in the desktop PC, which is the largest bottleneck in the memory and storage.

Sonam Srivastava and Sarv Pal Singh are discussed about a survey on latency reduction approaches for performance optimization in cloud computing. It proposes a key performance factors and approaches to reduce latency for performance optimization

Our system architecture for error localization is shown in bellow fig. 2

.

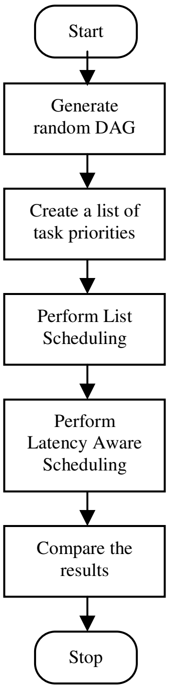

Fig.2. System Architecture for latency aware scheduling policy

4.CONCLUSION

In this paper, we reviewed on data security by error localization in cloud and also review on latency in cloud. There are different techniques are used to secure data in cloud. Here these paper focus to create secure cloud system with the benefits of latency aware scheduling policy.

5.REFERENCES

[1] Peter Mell, Timothy Grance, “The NIST Definatin of Cloud Computing”, Jan, 2011.http://docs. ismgcorp. com/files/external/Draft-SP-800-145_cloud-definition.pdf.

[2] Amazon.com, “Amazon Web Services (AWS)”, Online at hppt://aws.amazon.com, 2008.

[3] Vinayak R. Kankate, Varshapriya J. N, “Assuring Secured Data Storage in Cloud Computing”, 2013, IJESIT

[4] Dzmitry Kliazovich, Johnatan E. Pecero, Andrei Tchernykh, Pascal Bouvry, Samee U. Khan, Albert Y. Zomaya, “CA-DAG: Communication-Aware Directed Acyclic Graphs for Modeling Cloud Computing Applications”, 2013 IEEE

[5] Deepitha K R, Animesh Giri, “Ensuring Correctness and Error Localisation In Cloud”, 2013 IJCSIT

[6] Sowndarya Sundar and Ben Liang, “Communication Augmented Latest Possible Scheduling for Cloud Computing with Delay Constraint and Task Dependency”, 2016, IEEE

[7] Gang Sheng, Chunming Tang, Hongyan Han, Ying Yin, “Correctness Verification of Outsourced Inner Product of Vectors with Error Localization”, 2016, IEEE

[8] Sonam Srivastava, Sarv Pal Singh, “A Survey on Latency Reduction Approaches for Performance Optimization in Cloud Computing”, 2016, IEEE

[9] Teena Mathew, K. Chandra Sekaran, John Jose, “Study and Analysis of Various Task Scheduling Algorithms in the Cloud Computing Environment”,2014,IEE