International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

"Enhancement of Security And Availability of Data In Cloud Storage"

Ms. Bhandwalkar Priyanka[1], Ms. Parkhe Tejal[2], Mr. Sonwalkar Sandip[3], Mr. Saste Makarand[4], Ms. A. A.Pathan[5]
[1, 2, 3, 4, 5]UG Student, Computer Science and Engineering, College Of Engineering Phaltan, Satara, India [1-4]

Abstract: ***The cloud computing term describes a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network. Cloud computing relies on sharing various resources (e.g. networks, storage and services) to achieve coherence and economies of scale and gives the highest interest, how to maximize the effectiveness of utilization of the shared resources. We used efficient AES encryption and decryption algorithms. The AES encryption is used to store secure data on cloud and AES decryption algorithm is used to retrieve data securely from cloud. Here we have used efficient data fragment algorithms based on IDA (Information Dispersal Algorithm), with which we can partition a file into a designated number of pieces and reform by part of the pieces efficiently. We also used a Cloud Storage Application Programming Interface (CSAPI) for users, a method of accessing and utilizing a multi-Cloud storage, ignoring difference between various cloud servers.***

Keywords: Cloud storage, File Fragment Algorithm (FFA), Security Cloud Storage Gateway (SCSG), Advanced Encryption Standard (AES).

I. INTRODUCTION

Cloud computing, is a large-scale distributed and virtual machine computing infrastructure. The increasing network bandwidth and reliable yet flexible network connections even make it possible that clients can now subscribe to high quality services from data and software that reside solely on remote data center [1]. Cloud computing provides a new way of services by organizing various resources and providing them to users based on their demands [2]. Cloud computing is an innovative model to give beneficial, an on-demand access to a typical configurable handling resources [3]. Increased flexibility and budgetary savings drive companies to store data on Cloud storage for archiving, backup, and even primary storage of files [1]. Cloud computing and storage solutions provide users and enterprises with various strengths to store and process their data in third-party data centers that may be situated far from the user ranging in distance from across a city to across the world. Firstly, a third-party auditor (TPA), which user safely delegates to integrity checking tasks to, has proposed to guarantee data possession. Secondly, data encryption can guarantee data security and availability; however, reconstruction of the data usually requires more computational capabilities.

Storing data onto the cloud greatly decreases storage load with users and brings them access comfort, thus it has become one of the most important cloud services [1], [2].The benefit of data storage in the cloud is becoming increasingly attractive to both individuals and businesses. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provision and released with minimal management effort or service provider interaction [3], [4].

Cloud computing provide a scalability atmosphere for rising amounts of data and process that work on a mixture of applications and services by means of on-demand self-services.

One primary characteristic of this standard shifting is that data is being centralized and out-sourced into clouds. Users access data from cloud storage servers directly and then demand for data security from either cloud storage providers or via a third party auditor where third party auditor acts as an intermediary between the users and the providers. Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security [2].

A. Problem Definition

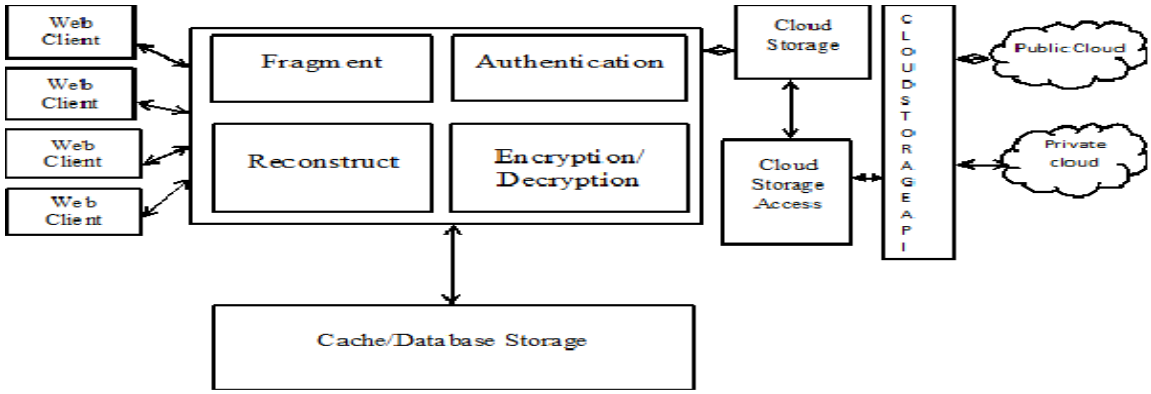
Enterprise and individual end users moves more and more important information to outsourced data centers, where the data may be misappropriated in the malicious model,

Security and availability become the main concerns of cloud storage. Our main objective is to preserve sender's authentication, receiver's authentication, message integrity and confidentiality of data in the cloud environment.

.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

II. PROPOSED SYSTEM



The term cloud is refers to Internet.Cloud computing is the delivery of computing services over the internet. E.g. Server, Networking etc. The cloud storage used to store secure information and access any time, anywhere by using internet. The multiple web client can request to access of information that store in cloud. The web client that can access the information of private cloud, only when they are authorized client of that private cloud. Authentication is the process of determining the identity of a client. The details of authentication vary depending on how you are accessing Cloud Storage. Authentication identifies the client, and authorization determines what client can do. The AES (Advanced Encryption Standard) algorithm is used for security, encryption and decryption purpose. The file fragmentation algorithm is used for the information availability. The cache database used for the recently access information. A cloud storage API (Application Program Interface) that connects a locally-based application to a cloud-based storage system, so that a user can send data to it and access and work with data stored in it. It enables users to access cloud application services written in the programming language across different storage platforms. The public and private clouds are used for large storage space to client and business enterprise.

III. LITERATURE SURVEY

The [1] paper author presented new architecture of distributed cloud storage gateway that is secure. The scheme provides a uniform storage interface for end user and third party application to visit public and private cloud storage service. The method makes full use of information dispersal algorithm (IDA) to design of file fragment algorithm which is used for file encoding and decoding. It is beneficial for less storage space and solves single point of failure. But in this paper uses 64 bit block size algorithm which is smaller for file security, it does not guarantee security of communication and services provided by cloud storage via internet which is highly latent.

The [2] paper was cloud computing with ECC is a completely new domain and has tremendous scope of research. The concern here is to provide data security with elliptic curve cryptography and also confidentiality with authentication of data between clouds. This paper proved the same level of security rendered by an RSA based system. But the ECC uses smaller key size which effects in faster calculations, saving memory and bandwidth. scheme which is used to generate key values. Private and public key is generated based on the partially generated private key by the KGC and to check the cloud data reliability of the user uploads the data in server and then during the auditing of the reliability of data is checked. Once after checking it then sends the report to the users. To confirm the data reliability during the auditing process and the server generates the proof and randomly selects the blocks. It is beneficial for key Generation Center (KGC) will generate only the partial key so that at any case it will not compromise user's private key. But it required storage space is large. The paper [4] proposes an access management system frame work that allows the user to use external cloud storage resources, requiring only a minimum level of trust but guaranteeing high availability confidentiality, integrity, of data. The main objective of this work is to seamlessly integration of cloud storage resources by highly scalable, easily accessible, and durable external storage services as they are widely offered by current cloud computing providers. The systems core component is a proxy server which is responsible for encryption, data distribution, and the unification of the different cloud storage localities and services. It provides high level of data security, availability, confidentiality and integrity. In this paper Complexity is more for secure data storage and retrieval of the relevant information.

This [5] paper public-key crypto system is planned which create constant-size cipher texts such that efficient allocation of decryption rights for any set of cipher texts are achievable. Users encrypt a file with single key using KAC, that means every file have each file, also there will be aggregate keys for two or more files, which formed by using the tree structure. Through this, the user can share more files with a single key at a time. But it not required more keys for shared more files because user used a single key for sharing file. This approach reduces the workload on the storage servers. It provides less security. If key is share, then whole data is shared. This [6] paper proposes a private key cryptography can be used to provide confidentiality. RSA is used to maximize the efficiency of public key cryptographic. In this paper error localization Algorithm is also used to determine the error and the localization of error while storing data considering the dynamic operations on data blocks like update, delete and append and to provide efficiency and resilience. The RSA Algorithm is based on modulo arithmetic. It selects two large prime numbers and then calculates public and private keys on the basis of a mathematical formula for encryption and decryption respectively. RSA is secure. RSA does not distribute the key. RSA is not efficient for large data. It involves large computations and CPU will be busy all the time. RSA very slow due to large number of mathematical computations involved.

IV. CONCLUSION

We have presented a new architecture of distributed cloud storage data which is secure. This paper provides more enhanced result in the cloud storage, which provides more security and Availability. The method makes full use of the AES algorithm to design a file fragment algorithm, which is used for file encryption and decryption. It costs less storage space and bandwidth to solve a single point of failures and data faults. SCSG achieves the design objectives; meanwhile, files partition storage can improve traditional cloud storage access efficiency. The concern here is data security to provide confidentiality and authentication of data between clouds. In future we wish be focused on more security issues of cloud computing.

V. ACKNOWLEDGMENT

Today on completion of this preliminary project report, the persons we need to thank the most that have helped us throughout the making of this report and without whose help it would not have seen the light of the day. Primarily, we submit us gratitude and sincere thanks to Prof. Ms. A. A. Pathan, for their constant motivation and support during the work in the last six month. We truly appreciate and value their esteemed guidance and encouragement from the beginning to the end of this work. We are thankful to our Head of the Department Prof. R. P. Bagawade for their unwavering moral support and motivation during the entire work. We would also like to thank our Principal Dr. M. K. Phadatare who encouraged us and created a healthy environment for all of us to learn in the best.

Miss PriyankaDhananjayBhandwalkar
Miss Tejal Bharat Parkhe
Mrs Sandip Laxman Sonwalkar
Mrs Makarand Rajendrakumar Saste

BE Computer Engg.

PES's COE, Phaltan.

REFERENCES

[1] Shenlingliu, Chunyuan Zhang, Le Bo "Improve security and availability for cloud storage," IEEE 2016.
[2] S. R. Pardeshi, V. J. Pawar, K. D. Kharat "Enhancing Information Security in Cloud Computing Environment Using Cryptographic techniques," IEEE 2016.
[3] R. Swathi, T. Shubha, "Enhancing data storage security in cloud using certificate public auditing," IEEE 2017.
[4] R. K. Banyal, V. K. Jain, Pragya Jain, "Data Management System to improve security and availability in cloud storage," 2015 IEEE (ICCIN).
[5] V. Swathy, K. Sudha, R. Aruna, C. Sangeetha, R. Janani, "Providing Advanced Security Mechanism for Scalable Data Sharing In Cloud Storage," IEEE 2016.
[6] A. Bhandri, A. Gupta, D. Das, "A Framework for data security and storage in cloud computing," 2016 IEEE (ICCTICT).