ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Secret Key Sharing Mechanism for Data Security in Cloud

Anmol Bhatia[1], Gaurav Garg[2]

M. Tech, Dept. of CSE, Advanced Institute of Technology and Management, Palwal, India[1]

Assistant Professor, Dept. of CSE, Advanced Institute of Technology and Management, Palwal, India[2]

ABSTRACT: Cloud computing becomes very woeful in the era of internet. Because we are generating peta bytes or more of data day by day. And developing new tools and technologies. In this scenario, we need to work more and more from anywhere with full ease of access of our personal machines, servers. So, cloud computing help with this. But, security is a biggest threat for cloud while transferring and accessing information over the internet. So, we have proposed a system with secret key sharing technique.Which helps more on fault tolerance against Byzantine attack. Data transmission completely secured by the encryption and decryption keys.

KEYWORDS: Cloud Computing, Security, Byzantine Attack, Secret Key

I. Introduction

Cloud computing could be a globalised construct and there are not any borders among the cloud. Computers would not have anymethod to store user information which is set anyplace on the world counting on wherever the capabilities that are needed within the international pc networks used for cloud computing. Owing to the enticing options of clouds computing several organizations are victim cloud storage for storing their vital information. The info is hold on remotely within the cloud by the users and might be accessed victimisation skinny shoppers as once needed. One among the main issue in cloud these days is information security in cloud computing. Storage of information within the cloud is risky owing to use of net by cloud based mostly services which suggests less management over the hold on data. One among the main concern in cloud is however will grab all the advantages of the cloud whereas maintaining security controls over the organizations assets [2].

Cloud computing could be a model for convenient, on-demand network access to a shared pool of configurable computing resources. Cloud computing provides associate surrounding wherever heterogeneous systems interact over the web. Heterogeneous systems involve totally different environments like one system could use software system for eg. windows,linux and macintosh etc. Cloud computing is that the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the utilization of a cloud-shaped image as associate abstraction for the advanced infrastructure it contains in system diagrams [6].Cloud computing assign the responsibility of remote services with a user's data, software and computation. There are many types of public cloud computing:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Storage as a service (STaaS)
- Security as a service (SECaaS)
- Data as a service (DaaS)

- Business process as a service (BPaaS)
- Test environment as a service (TEaaS)
- Desktop as a service (DaaS)
- API as a service (APIaaS)

Cloud computing can be classified in two diverse ways: -

1. Deployment Model
2. System Model

Based on the readying the cloud may be of following sorts. Diverse types of clouds are delineating below:

1. **Public Cloud:** The cloud merchandiser hosts the computing infrastructure at its own premises and therefore the customers do not have any management on wherever the computing infrastructure is hosted. The computing infrastructure is open to be used by public or totally different organizations share this computing infrastructure [5].
2. **Personal Cloud:**Computing infrastructure is not between the organizations. It is dedicated to a specific organization and is thus safer than public clouds.The 2 sorts of personal clouds are delineating below. Outwardly hosted personal clouds are hosted by same third party that extended sizes in cloud infrastructure and completely utilized by one organization. On premise, personal clouds are hosted by the enterprise itself and are costlier as compared to outwardly hosted personal clouds.
3. **Hybrid Cloud:**The cloud infrastructure in hybrid cloud could be a synthesis of two or a lot of distinctive cloud infrastructures that are delimited along by some standardized technology that empowers application and information movability.
4. **Community cloud:** The cloud infrastructure is only utilised by shoppers from organizations that have connected or imparted considerations. Community cloud is also overseen, managed and worked by 3rd party or one or a bigger quantity of organizations within the community or some consolidation of them.

The design includes of the many loosely coupled cloud parts. Cloud may be computer system is noted as side that consists of the applications and interfaces that square measure required for accessing cloud computing platforms, e.g. application program. Side alludes to cloud itself and includes of each last one in every of resources that square measure obligated to convey cloud computing services [1]. It includes of virtual machines, large information storage, virtual machines, security mechanism, services, servers, readying models so forth. These ends square measures generally connectedthrough a network commonly connected by means that of internet.

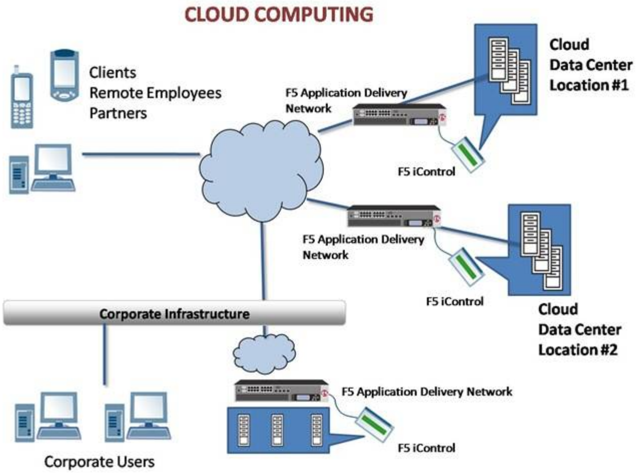

Figure 1. Sample Cloud Computing Infra

In cloud computing six specific areas where substantial security attention isrequired is are as follows [4]:

1.Security of data in transit.

2.Security of data at rest.

3.Cloud legal and regulatory issues.

4.Robust separation between data belonging to different customers.

5.Authentication of users/ applications/ processes.

6. Incident response.

So, we basically work for the security aspect in cloud computing.

II. Related work

Dnyneshwar Supe, Amit Srivastav, Dr. Rajesh S. Prasad [3]have shown various algorithms for secret sharing in cloud computing as well as how secret sharing happens in cloud computing. They also have proposed some security solutions for cloud computing.

Mrs. Komal Kate, Prof. S.D. Potdukhe [7]In this paper they shown that user's information privacy may be central question of cloud storage. Compress secret keys in public-key cryptosystem that support delegation of secret keys for various cipher text categories in cloud storage. Despite that one amongst the facility set categories, the delegate will perceptually get associate degree mixture key of constant size.

In cloud storage, the quantity of cipher texts typically grows chop-chop with none restrictions. Therefore, we've got to order enough cipher text categories for the long run extension. Otherwise, we want to expand the public-key. though the parameter is downloaded with cipher texts, it'd be higher if its size is freelance of the most variety of cipher text categories.

Saria Islam, A.S.M Mahmudul Hasan [10], in this paper they need cantered on a vital scientific discipline primitive – secret sharing theme. A secret sharing theme starts with a secret so devices from inbound shares that square measure distributed to some users. The key could also be recovered solely by bound planned teams that belong to the access structure.

Secret sharing schemes have appeared as a chic resolution for the matter of safeguarding scientific discipline keys however their applications embrace currently scientific discipline protocols and a few e-voting or e-auction protocols.They need reviewed the foremost vital secret sharing schemes for various access structures. Some terribly attention-grabbing and helpful extended capabilities are additionally surveyed in order that the applications are simply fathomable.

III. PROPOSED ALGORITHM

Main objective of this research is to boost the key management and information security in cloud computing supported secret key sharing management algorithmic program.Our projected technique helps to convey higher fault tolerance against Byzantine attacks, server colluding and information modification attack. Byzantine failure is incredibly inclined fault in cloud servers, within which a storage server will fail in arbitrary ways in which. On incidence of a byzantine failure system responds in random means. At the purpose once a Byzantine failure is going on, the framework might react in any erratic means, unless it is meant to process Byzantine fault tolerance.

The cloud is additionally inclined to information modification and server colluding attack within which the storage servers may be compromised by the individual, as a result of that information files may be changes if they are internally consistent. Some important entities are there in our proposed system which is given below:

1. Cloud User: User can create, Update, Delete his/her data.

2. Cloud storage Server: it is a server where the data is stored in encrypted form.

3. Key Management Server: It will split the key in different shares and store them on different share holder servers.

4. Share Holder Server: It will store the keys from different users. It is also responsible for Renewal of shares periodically.

5. Log Editor: It checks the Share Holder Server periodically if the share is not getting modified.

6. Security Server: Does Encryption and Decryption thing [8].

IV. METHODOLOGY

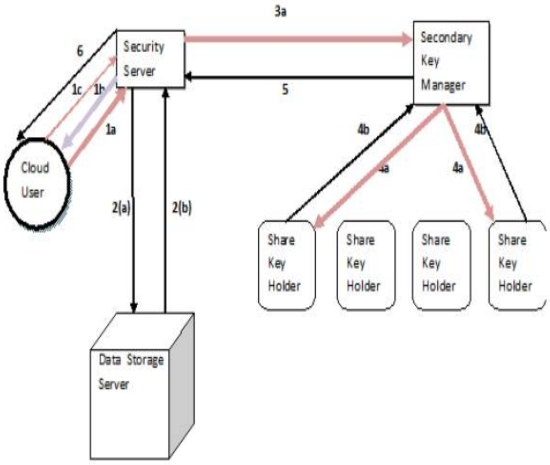

Figure 4.1 Process Diagram

File Upload:

1. When the cloud user wants to submit a file to a cloud first the file is forwarded to the cloud manager.

2. Security module in cloud manager generates the key and encrypts the file using the encryption algorithm as shown and then forwards the key to key management module.

3. Encrypted file is forwarded to the cloud data storage centre.

4. Key management module divides the key into number of shares. Sends a master key to the cloud user and distributes all theremaining keys to the Share Holder Servers.

All the primary shareholders and secondary shareholders are monitored from time to time to ensure that their values are not modified by attacker.

File Download:

1(a) Request to the security server for file downloading.

1(b) Request to cloud user to provide master key that was given in the encryption process.

1(c)Master Key provided by cloud user.

2(a) Request to data storage server to send the encrypted key as requested by user.

2(b) Data storage server sends encrypted file to cloud storage server.

3(a)Security server enquires the secondary key from the key manager.

4(a)Key Manager requests the share from the different shareholders.

4(b) Share holder servers forward their shares corresponding to the user to the key manager.

5. Key manager combines all the shares and sends it to security server.

6. Security server combines the master key provided by the user and the secondary key provided by key management server and generates the actual key. Then, it decrypts the user file stored in cloud and send it to the user. Our proposed system has advantages over the existing systems:

   1. Existing techniques are centralized in nature. We try to provide to provide a distributed approach for key management.

   2. Our technique provides fault tolerance to byzantine attacks, data modification and server colluding attacks.

   3. Reliability of the system is increased by using the voting technique to ensure that the shares do not get modified by the attacker.

   4. After a pre-decided crypto time, the shares are renewed to ensure the security of user data if in case some of the shares get compromised.

DOI: 10.15680/IJIRCCE.2017. 0505006

V. SIMULATION AND RESULTS

To simulate our work we used CloudSim machine with Amazon Internet Services and Web beans IDE. CloudSim could be an internet app that runs on amazon virtual machine(AWS). It permits users to launch, terminate and monitor the virtual machines with the AWS Cloud. Every CloudSim configuration maps to a constellation, that square measures collection of multiple virtual machines running along.

Proposed technique is implemented with different file size ranges from 100KB to 50MB and we try to find out performance comparison between an existing technique and the proposed technique. The key provided from AWS is the token that allow CloudSim to access AWS on behalf of the AWS user.

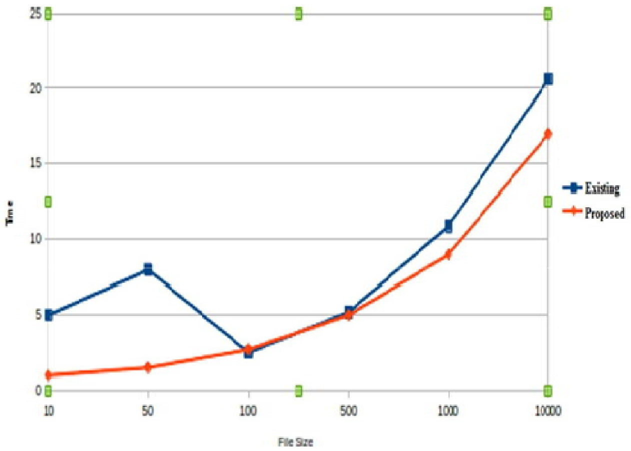

Figure 5.1 Size Vs Time for File Upload

File Transfer Time: It includes the time to encipher the file as requested by the consumer. It is the time between the points once user requests the cloud system to transfer the file and therefore the time once tasks of secret writing and generating key shares truly finishes and therefore the encrypted file is really keep within the cloud knowledge storage. Figure 5.1 shows the time taken for file uploading for various file sizes.

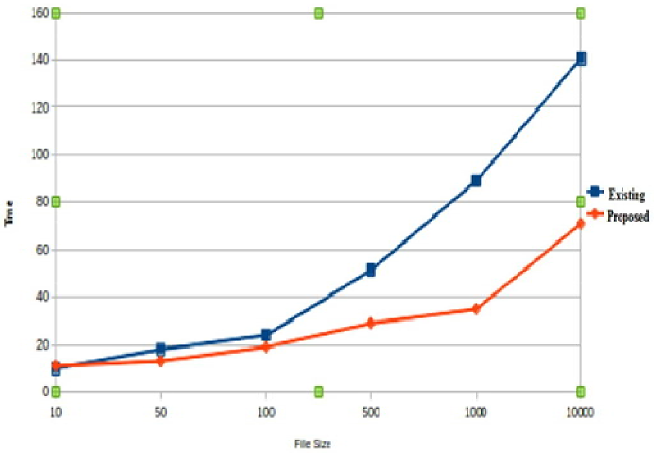

Figure 5.2 Size Vs Time for File Download

File Transfer Time: It includes time to gather the share, generate the secondary key, and merge the key and therefore the secondary key and time to rewrite the input data. It is the time between the 2 points once the user makes an invitation to transfer a file and user really receives his file. Figure 5.2 shows the time taken for file downloading for various file sizes.

VI. Conclusion and Future Work

We conclude that it is an efficient scheme where the secret is shared in a group because the unauthorised or outside entity cannot get the access to the information shared in a group without having at least threshold number of shares of the decryption key used to encrypt the information.

Within the cloud platform, there is continually an opportunity of business executive attack or outsider attack. Key is accessed or purloined by staff while not the data of finish users. Our aim is to produce secrecy to the info yet as keys that are hold on in cloud systems. Our projected technique provides higher knowledge security and key management in cloud systems. This system conjointly provides higher security against byzantine failure, server colluding and knowledge modification attacks.

For future, this work may be extended to use another secret sharing scheme that are a lot of economical so the performance of projected system is any improved. Additionally to the current the projected technique is extended to figure out the uneven cryptography algorithms.

References

1. A.Shamir," How to share a Secret",Comm ACM, Vol.22, no.11, pp. 612-613, 1979.
2. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in IEEE Cloud, June 2012, pp. 295–302.
3. Dnyaneshewar Supe, Amit Srivastav, Dr. Rajesh S. Prasad, "Review of Methods for Secret Sharing in Cloud Computing", International Journal of Advanced Research in Computer Engineering and Technology(IJARCET), Vol. 02, Issue 1, pp. 11-17, January 2013.
4. Fredrik Olsson, "A Lab System for Secret Sharing", 2004
5. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
6. Lein Harn and Changlu Lin, "Authenticated Group Key Transfer Protocol Based on Secret Sharing" IEEE transactions on computers, vol, 59, No.6, June 2010 IEEE.
7. Mrs. Komal Ate, Prof. S. D Potdukhe, "Data Sharing in Cloud Storage with Key-Aggregate Cryptosystem", International Journal of Engineering Research and General Science(IJERGS), Vol. 02, Issue 06, pp. 882-886, October-November 2014.
8. N. Ferguson & B. Schneier, "Practical Cryptography", 2003, pp. 358-360
9. Ranjith. K, P.G. Kathiravan, "A Self-Destructing System for Dynamic Group Data Sharing in Cloud", International Journal of Research in Engineering and Technology(IJRET), Vol. 03, Special Issue 07, pp. 265-270, May 2014.
10. Saria Islam, A. S. M Mahmudul Hasan, "Implementation of Shamir's Secret Sharing on Proactive Network", International Journal of Applied Information Systems(AJAIS) , Foundation of Computer Science FCS, New York, USA, Vol.06, No. 02, pp. 17-22, September 2013.
11. S. Jaya Nirmala, S. Mary Saira Bhanu, Ahtesham Akhtar Patel, "A Comparative Study of Secret Sharing Algorithms for Secure Data in the Cloud", International Journal of Cloud Computing: Services and Architecture(IJCCSA), Vol. 02, No. 04, pp. 63-71, August 2012.
12. Swapnila S. Mirajkar, Santosh Kumar Biradar, "Using Ssecret Sharing Algorithm for Improving Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Technology(IJARCST), Vol 02, Issue 02, Ver. 03, pp. 395-398, April-June 2014.
13. W.G. Tzeng. "A Secure Fault-Tolerant Conference Key Agreement Protocol," IEEE Trans. Computer, Vol.51, no.4, pp. 373-379, Apr.2002
14. Yamini Indla, M. Sampat Kumar, "Extended Group Key Transfer Protocol for Authentication Using DES based on Secret Sharing in Cloud" International Journal of Emerging Technology and Advanced Engineering(IJETAE), Vol. 02, Issue 11, pp. 541-551, November 2012.