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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Secure Data Distribution over Multiple Cloud Server using DROPS and Bloom Filter

Swarada Narayan Deshpande

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India

ABSTRACT: Cloud acts as a backbone to the number of emerging technology such as Internet of Things, business enterprises, mobile applications. Cloud schema that can be used to provide a privacy preserving mechanism while considering the importance of Service Level Agreement between cloud consumer and provider. Developing secure systems so as to preserve identity of user which is crucial responsibility. Preventing Trusted Third Party from sharing secure outsourced data is requirement that has to be ensured. Intelligent data backup recovery system can avoid loss of confidential data. Replication mechanism will increase the availability of the data on cloud. Motive is to secure the sensitive data and preserve privacy policy. Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information. In cloud computing security of the assets does not solely depend upon an individual's security measures however the neighboring entities may provide an opportunity to an attacker to bypass the user's defenses. The defined system will try to mitigate the security risks and improve the computing environment.

KEYWORDS: Privacy Preserving, Cloud Security, Bloom Filter, Replication, SHA-1

I. INTRODUCTION

The cloud's roots date back to early mainframe processing, when users connected to a shared computing resource through terminals to solve their computing needs. The advent of faster and cheaper microprocessors, RAM and storage brought computing into the client-server model, which grouped sets of users into networks sharing computing power on decentralized commodity servers. As bandwidth became more ubiquitous, speedier, and less costly, these networks interconnected to form the Internet. IT departments typically provisioned their datacenters in house, protected inside a firewall. However security remained as a concern regarding cloud user. Confidential data uploaded to the cloud if outsourced should not be shared, modified, deleted or lost unless user grants permission. Cloud collaboration has become popular as is immensely helpful to build enterprise business model. Mining data for predicting user behavior so as to enhance the business is obvious nowadays. Alongside the differences of the application necessities, clients might need to get to and share each other's approved information fields to accomplish profitable advantages which bring new security and privacy challenges for the cloud storage. Shared Authority in cloud computing short-come for key revoking. While implementing bloom filters at the cloud server avoid duplication consuming space.

II. RELATED WORK

Existing work done by the researchers for cloud storage and privacy is studied.
Hong Liu, Huansheng Ning, Qingxu Xiong, and Laurence T. Yang proposed a Shared Authority Privacy Preserving Protocol States a new protocol to provide data anonymity.

L.A. Dunning and R. Kresman, [2] developed system for Privacy Preserving Data Sharing with Anonymous ID in which Newtons identities and theorem is used for data mining a distributed solution on certain polynomials over finite fields Enhances algorithms scalability.

X. Liu, Y. Zhang, B. Wang, and J. Yan [3] proposed a system named Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud which decryption policy are developed in which user can decrypt data without pre-contacting the data owner and hence avoiding frequent up gradation hence proposed scheme here supports privacy preserving and traceability.

S. Grzonkowski and P.M. Corcoran [4] developed Sharing Cloud Services that authenticates User for Social Enhancement of Home Networking here ZKP zero knowledge proof is used for authentication. Here attempt is made to

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

use more User Centric approach in line with current trends in mobile network services. When ZKP techniques are combined with cloud services they provide dynamically adjusting increasing number of authentication challenges from the server.

Andrei Brodery and Michael Mitzenmacherz studied all the applications of Bloom Filter in Computer Network can be used in replica location; query routing has number of advantages while building a good cloud storage.

In this paper Cloud schema is proposed which has Number of various users is connected with a continuous association and applied with independent authorities over some data fields.

Cloud server that is controlled by particular cloud provider for giving the data storage as well as computing services. In this system user has ability to store the information separately through the online system, platforms or software.

III. PROPOSED SYSTEM ARCHITECTURE

The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be illegally accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the users privacy no matter whether or not it can obtain the data access permissions. There is also a problem of system overhead due to communication with TPA and encrypted file storage on cloud server. To overcome this problem, schema is proposed also bloom filters help us to avoid DE duplication and provide rapid response.

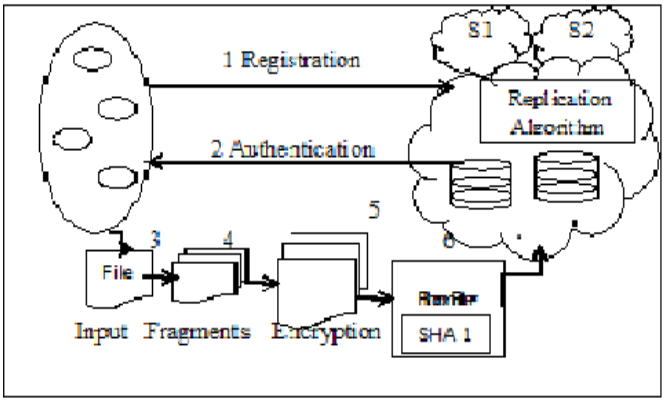

Fig 1: Proposed System Architecture

In this system user has ability to store the information separately through the online system, platforms or software. This facility for cloud services will be worked in the proper way as well as same and cooperative modes. In proposed system the user or group of user has to register itself initially with cloud server and after that login to the system. At the time of login user is going process of the authentication which is performed by cloud service provider and if the user has authentication then user will login successfully in the system and executes its operations. This system takes the file and it splits into number of segments and after that it creates the hash of file as well as uploads the segments on the cloud server. In the process of uploading, Division and Replication approach is executed. In DROPS approach each node preserves a single segment of the information and all the nodes are physically divided in several distance.

IV. ALGORITHM

Fragments Replication Algorithm

Input: Cloud Server (CS1, CS2, CS3, CS4), fragments (f1, f2, f3, f4)

Output: Fragments Replication

1. While the replication of each fragment is not completed do
2. Receive a fragment fm and lookup its fingerprint in CSn.
3. If (CSn.size)!=2 and !(CSn.contains(fm))

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

4. Then place fm in CSn
5. Remove fm from fragment list and increase size of CSn by 1
6. Else
7. Change the CSn.
8. End while.

V. RESULTS

In Proposed system architecture, when user registers on cloud until data get equally distributed on cloud intelligently and replicated the data availability and storage comparison graphs are discussed below.

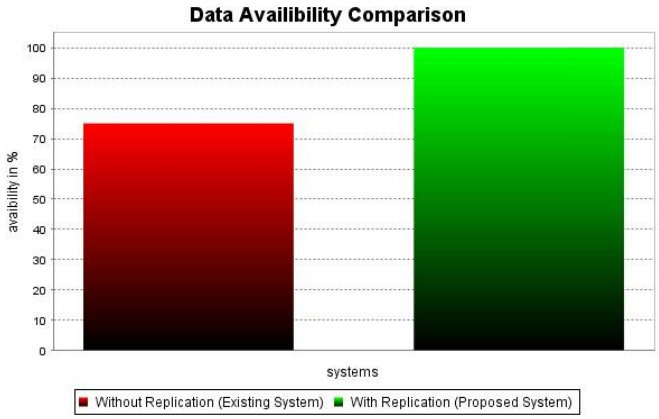

Fig 5.1: Data Availability Comparison

Data availability in proposed system is better than existing system, because proposed system makes use of DROPS algorithm. According to this algorithm, file is divided into blocks and that blocks are stored at more than one server individually. X-axis represents the systems and Y-axis represents the availability in percentage.

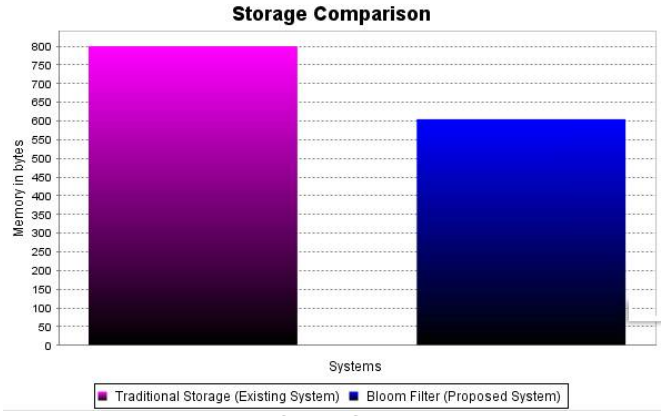

Fig 5.2: Storage Comparison

Storage require in proposed system is less than existing System, because proposed system makes use bloom filter approach. Bloom filter requires less memory to store the hash values of file blocks. X-axis represents the systems and Y-axis Represent the memory required in bytes. The X-axis shows various file size from 10 kb to 10000 kb while Y-axis shows time required in seconds to run the algorithms.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

VI. CONCLUSION

Proposed a cloud architecture that can distribute data over cloud intelligently and can provide greater throughput rather than traditional cloud on Internet. Cloud schema ensures intelligent data distribution, enhances cloud security mitigate Privacy Preserving Challenges, future scope includes consideration of attacks on cloud server. Evaluating the distance the nodes are divided. If the attack is successful the fragmentation and scattering guaranteed that no important information was accessible by an adversary. In each node only single fragmented file is stored. Experimental results demonstrate that our constructions are efficient and practical. The experimental result also shows that our proposed system required less time and memory compared to existing system.

REFERENCES

1. Hong Liu, HuanshengNing, QingxuXiong, and Laurence T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing IEEE transactions on parallel and distributed systems, vol. 26, no. 1, January 2015
2. L.A. Dunning and R. Kresman, "Privacy Preserving Data Sharing with Anonymous ID As-signment," IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 402-413, Feb. 2013.
3. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dy-namic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, http:// ieeexplore.ieee.org/stamp/stamp.jsp-tp=arnumber=6374615, June 2013.
4. S. Grzonkowski and P.M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Trans. Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, Aug. 2011.
5. M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614, http://ieeexplore.ieee.org/stamp/stamp.jsptp= arnumber=6298891, Nov. 2013.
6. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.
7. S. Sundareswaran, A.C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, July/Aug. 2012.
8. Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan IEEE DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security.

BIOGRAPHY

Swarada N. Deshpande completed B.E. from Dr. Babasaheb Ambedkar Marathwada University and pursuing Masters in Computer Engineering from Savitribai Phule Pune University. Her Area of Interest includes Internet of Things, Cloud Security and Privacy Preserving in Cloud.