Shared Authority Based Privacy Preserving Authentication for Data Partitioning Cloud Storage

Mr. Prashant Alkunte[1], Prof. D. M. Jadhav[2]
[1, 2] Department of Computer Engineering
[1, 2] Trinity College of Engineering and Research, Pune-48, Maharashtra, India.

Abstract- *Cloud computing has introduced from distributed computing which helps users to use their resources according to their operational requirements. Cloud is based on various service models which include pay per service and pay per use models. Cloud computing with data partition and shared authority protocol is one of the emerging trends. Shared authority has its group each group owns its users which are allowed to access the valid or legal data fields and different users have independent access policies it means that any two users from dissimilar groups should access different data fields of the same datasets and protect user requests of different user by anonymity. shared authority introduced with data partitioning is in vertical and horizontal direction takes place. It store portioned data into bucket and use slicing technique for data storage error correction and data constraint checking is used to detect the availability of data. Load balancing in the cloud computing has an important affect on the speed & performance load balancing makes cloud computing more effective and improves satisfaction.*

Keywords- Cloud Computing, Shared authority protocol, Data partitioning, Trusted Third Party, Load balancing.

I. INTRODUCTION

Cloud computing is an emerging technology which provides IT services and resources to the customers through public network specifically internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offers an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure.[1] Our goal is to build an application for improving cloud security using partition and encryption method which will help to improve the cloud security. The main Moto of this dissertation is Shared Authority Based Privacy Preserving Authentication [1] for Data Partitioning Cloud Storage for the storage [2], which focuses on authentication and authorization without disclosing a user's private information. This technique addresses security and privacy issue for cloud storage. In this shared authority is implemented by anonymous access challenge mechanism with some privacy conditions like authentication, anonymity, privacy and forward security. [1]

Shared authority with this highlights the concept of how dynamic partitioning technique can improve the performance of Cloud Computing Environment. Existing solutions that use wholesome cryptographic techniques to tone down security and access control problems. In this paper, the proposed data partitioning technique with cryptography which ensure cloud storage security, integrity [3]. Cloud storage constraint checking method is used to enhance the integrity and security of cloud storage. System model constitutes of three layers namely client machine, trusted Third Party (TTP) and cloud storage servers. Partitioning method implemented at trusted third party. TTP performs operation like partition data, , Public key generation for each partition, Encrypt each partition using particular keys, storing each partition sequence of respective data, signature key and file attributes on its own server, sending partition at appropriate cloud server, retrieve as well merging of partitions, Decryption and integrity checking of data. Load balancing in the cloud computing has an important affect on the speed & performance load balancing makes cloud computing more effective and improves satisfaction. Load balancing is the work of distributing the task among various resources in any other system. Thus task need to be distributed over the resources in cloud so that each resource does to provide some techniques to balance requests to provide the answer of the software application faster.[4]

II. LITERATURE SURVEY

Access the information using GPS and find out the present location of users like restaurants, cafess, ongoing events etc. Users are interested about point of interest (POI) in their physical proximity and data owner only allow to paying customer. When user query to cloud provider request itself reveal the physical location information of the data owner which stored on cloud. Location based service uses current coordinate of user and use them for other purpose such as profiling, unsolicited, advertisement. Storage of data and query must do in encrypted form. At the end, paper concludes a promising future of this area of research by Sunoh choi. [5]

Decentralized information accountability framework to keep track of the actual usage of the users data in the cloud. Proposed object oriented approach that enables enclosing our

logging mechanism together with user's data and policies. Users need to be able to ensure that their data are handled according to the service level agreements made at time when they sign. CIA-Cloud Information Accountability framework which gives powerful accountability that combines aspect of access control, usage control and authentication. Propose by Smitha Sundareswaran, [6]

With decentralized erasure code from that secure distributed storage system is formulated. Proxy encryption supports encoding operation over encrypted message as well as forwarding operation. Erasure code is stored in one server and data owner encrypt the message first and requesting for code and then use erasure code to encode again and forward to the next server or user. Proxy reencryption message encrypted first by the owner then stored in storage server when user want to share his message he sends a reencryption key to the storage server re encrypt the encrypted message for authorized user by Hsiao-Ying Lin [7]

Proposed by Kai Hwang, Trust and security prevented business accepting platform. Data coloring and software watermarking technique protect shared data objects and massively distributed software modules enable single sign on and authentication. Forward and backward color generation process is used to add the cloud drops or data colors into the input images and when you want to decrypt the original data remove the data color from the original part and restore it. [8]

Anonymous ID generation for different users to share their data securely and which is involved in cloud computing. These assignments of anonymous id gives befit of communication identities received are unknown to the other users of the group. Confusion among different members is identified when private communication channels are used. This assignment of serial numbers allows complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access and this all the communication is going through trusted third party. Proposed by Larry A. Dunning [9]

Proposed by X. Liu, Y. Zhang From this paper we got information related to multi owner data sharing secure scheme for different groups in the cloud application. There is implementation of anonymity for different user to securely contact with data owner resources. In this scheme users are operated in un-trusted environment but it support dynamic interaction with other member in group. In this user is requesting to cloud server for data owner data and cloud server granting data access to user and users are getting data without pre-contacting to data owner. [10]

Proposed a zero-knowledge proof based authentication scheme for sharing data within cloud services and based on the social home networks, a user centric approach is applied to enable the sharing of personalized content and dishonest network services through TCP/IP infrastructures, in which a trusted third party is introduced for decentralized interactions. When you want to authenticate with network device the traditional method was username and password but the new technique is to use trusted third party or smart card or biometric machines to increase the security for the users. In this paper they use TCP/IP protocol for data sharing and that is dishonest protocol or not secured protocol for communication. Proposed by S. Grzonkowski [11]

Decentralized access scheme is for to provide security with anonymous authentication which prevents actual data about user. Cloud verifies the authenticity without knowing the details of user before data storing and also added feature of access control which controls and maintains the security only valid user can decrypt the data from cloud. This scheme prevents replay attacks and this is fully centralized control. All the communication between cloud server and users are in encrypted form. [12]

III. PROPOSED SYSTEM ARCHITECTURE

3.1 Data Owner and User

Users which own its data stored in the cloud for online data storage and computing. Users fears of losing control of their own data particularly, financial and health data and research data can become a significant barrier to the wide adoption of cloud services data owners do not have the technical means to support processing queries on a large scale because of this they outsource data storage and handling quires from cloud service provider.

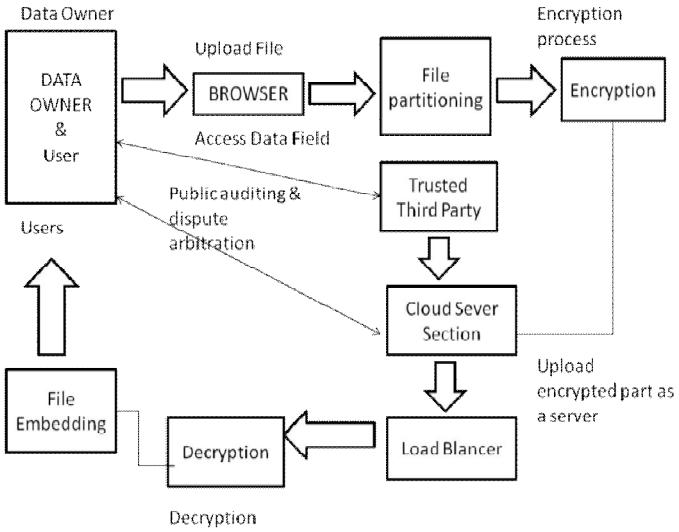

Figure1:- Proposed System Architecture

3.2 Trusted Third party

Trusted third party who has advanced capabilities on behalf of the users, to perform data public checking and security problem arbitration in the cloud storage, a user remotely stores its data through online infrastructures, platforms, or software for cloud services, which are operated in the distributed and cooperative modes. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other members, and is of very importance to assure the private information during the users' data access requests.

3.3 Cloud server

The cloud server is regarded as an entity with secured storage and unlimited computational resources. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offers an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure.

3.4 Uploading Files to Server

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. That is, the cloud server will not maliciously delete or modify user data due to the protection of data checking schemes. This uploading of data which is done by data owner with trusted third party and store their confidential data on cloud server.

3.5 File Partitioning

A partition is a division of a logical database or its element into distinct non related parts. Database partitioning is normally done for easy manageability, effective performance. A popular and favorable application of partitioning is in a distributed database management system. Each partition may be loaded over multiple terminals, and users at the node/terminal can perform local transactions/manipulations on the partition. This increases performance for site that has regular transactions involving certain views of data, at the same time as maintaining availability and security

3.6 Encryption-Decryption Algorithm

Encryption technique is used to encrypt the partitions of files for security and Integrity purpose. To encrypt data partitions using encryption algorithm is used. Using Clients public key data is encrypted, stored on the cloud servers. At the time data retrieval client is going to request data. Trusted third party will search for the respective data partition and will return data to the client.

3.7 Load Balancer

Load balancing in the cloud computing has an important affect on the speed & performance load balancing makes cloud computing more effective and improves satisfaction.

V. CONCLUSION

Achieve privacy-preserving access authority sharing using trusted third party and shared authority to establish Authentication, Data anonymity, User privacy, Forward Security. Implemented load balancing with file partition is aimed at the public cloud using partitioning technique which increases speed of uploading and downloading files.

ACKNOWLEDGMENT

I am highly indebted to Prof. D. M. JADHAV for their guidance and constant supervision as well as for providing necessary information regarding the Dissertation and also for their support.

REFERENCES

[1] Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE, "Shared Authority Based Privacy Preserving Authentication Protocol in Cloud computing",Year-2015 IEEE

[2] G.Jeeva Rathanam Department of Information Technology Anna University, Chennai Tamil Nadu, INDIA."Dynamic Secure Storage System in Cloud Services", Year 2014, IEEE

[3] C. Selvakumar Department of Information Technology MIT Campus, Anna University Chennai, Tamil Nadu, Indian "PDDS – Improving Cloud Data Storage Security Using Data Partitioning Technique", Year-2012, IEEE

[4] Suchita Khare1, Abhishek Chauhan Department of Computer Science, NRIIST, Bhopal, India"A Review on Load Balancing Model Based on Cloud Partitioning for the Public Cloud", Year-2014, International Journal of Emerging Technology and Advanced Engineering

[5] Sunoh Choi, Gabriel Ghinita, Hyo Sang Lim and Elisa Bertino "Secure kNN query processing in untrusted cloud environments" Year 2014 IEEE

[6] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin Ensuring Distributed accountability for data sharing in the cloud" Year 2012 IEEE

[7] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE"A secure Erasure code based cloud storage system with secure data forwarding " Year 2012, IEEE

[8] Kai Hwang University of Southern California Deyi Li Tsinghua University, China "Trusted cloud computing with Secure resources and data coloring" Year 2010, IEEE

[9] Larry A. Dunning, Member, IEEE, and Ray Kresman" Privacy Preserving Data Sharing With Anonymous ID Assignment" Year-2013, IEEE Transaction

[10] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems" Year- 2013, IEEE Transaction.

[11] S. Grzonkowski and P. M. Corcoran, Fellow, IEEE, "Sharing Cloud Services: "User Authentication for Social Enhancement of Home Networking," Year- 2011 IEEE Transactions

[12] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, andAmiya Nayak, Senior Member, IEEE," Decentralized Access Control withAnonymous Authentication of Data Stored in Clouds" Year-2014,IEEE

AUTHORS DETAILS

First author :- Mr.Prashant Alkunte, M.E. (Computer Engineering), Trinity college of engineering and research,Pune,alkunteprashant@gmail.com

Second author:-Prof..Mr.Jadhav D. M. (SemanticWeb, Cyber Security, Hadoop, Data Mining),Trinity college of engineering and research,dadaramjadhav@gmail.com