Efficient and Secure Group Data Sharing Model Using Cloud Computing

Mohit Kabadi[1], Gitesh Ghorpade[2], Munot Sarode[3], Sameer Sagar[4], Amol Dumbare[5]
[1,2,3,4]*B.E (Computer Engineering), Pimpri Chinchwad College Of Engineering And Research, Ravet, Pune, Maharashtra, India*
[5]*Professor, Department of Computer Engineering, Pimpri Chinchwad College Of Engineering And Research, Ravet, Pune, Maharashtra, India,*
[1]*Email: mohigk06@gmail.com* [2]*Email: ghorpadegitesh25@gmail.com*
[3]*Email: munotsarode333@gmail.com* [4]*Email: rathoresameer67@gmail.com*
[5]*Email: amol.dumbare@pccoer.in*

Abstract: *Cloud computing is alleged to be the servicehomeward-bound computing technology, that ar reasonable andversatile over the web. In past few years the cloud has becomemore experienced and provided several services, one in allthe first service is knowledge sharing in cluster, wherever theinformation are often simply shared from one member to adifferent. However, whereas sharing the information security isone in all the first concern. In past many methodology has beenplanned. However, these strategies lacked from the feasibleness.Hence, during this paper we've propose methodology relies onthe choice theme. Here General cluster secret's generated andwhat is more General Key agreement protocol is redistributedprimarily based model wherever the information ar controlledby the owner inside constant cluster. Moreover, the plannedmethodology is evaluated by analyzing the comparative analysissupported the assorted range of parameter. Result Analysiscounsel that our methodology merely outperforms the presentone.*

Keywords:Cloud Computing, security, Group data shar-ing

1. INTRODUCTION

IN recent times as the concept of cloud computing rises,cloud storage is said to be the one of the hotspots of thestorage of informationIt basically refers to a model, that provides the datastorage. Here, CSP (cloud service provider) is directly re-sponsible for making data available as well as accessibleaccording to the requirement of use r.Storage capacity is either bought or leased from providerto store the data by the individual or organization. Thisservice can easily be accessed through the the application,which utilizes the API such as cloud storage gatewayMoreover, in the past few years, it has been observed thatthe demand of cloud storage has been increased phenomenalin accordance with the use of personal as well as businesspurpose, since it is highly based on the virtualized infras-tructure and much more flexible in terms of multi-tenancy,scalability and availability. Since the cloud, computing provides USA the feature ofpay as you go service, the organization needs to pay just forthe service they use, and cloud service provides precisely thesame. Business exploitation the caesium will truly scale backup to seventy p.c of energy consumption. CSP is completelyliable for the upkeep of the info and still because thealternative tasks like shopping for the extra storage capability.Since the backup of the info area unit settled in many placeswithin the globe, it can even be applicable because the proofbackup of natural disaster. Meanwhile, cloud storage is oneservice, that isn't mentioned the physical device, however it'sthe aggregation of the many server and storage for its users.

2. LITERATURE REVIEW

1.Efficient and Secure Group Data Sharing Model basedon Selection scheme in Cloud environment.

Description: Cloud computing is aforementioned to bethe serviceoriented computing technology, that area unitreasonable andflexible over the web. In past few years thecloud hasbecome additional matured and provided severalservices, one ofthe primary service is knowledge sharingin cluster, wherever the datacan be simply shared fromone member to another. How-ever, whereas sharing theknowledge security is one of the primaryconcern. In pastmany methodology has been projected.However, these wayslacked from the practicableness. Hence,in this paper we've vepropose methodology relies on theselection theme. HereGeneral cluster key's generated andmoreover General Keyagreement protocol is decentralizedbased model wherever theknowledge area unit controlled by the ownerwithin identicalcluster. Moreover, the projected methodologyis evaluatedby analyzing the comparative analysis based mostly onthenumerous range of parameter. Result Analysis suggestthatour methodology merely outperforms the existing one. Key-words: cloud Computing, security, cluster knowledge sharing

2. Panda: Public Auditing for Shared Data with EfficientUser Revocation in the Cloud

Description: With info storage and sharing servicesamong the cloud, users will just modify and share infoas a bunch. to substantiate shared data integrity ar verifiedpublically, users among the cluster got to be compelled tocypher signatures on all the blocks in shared info. fully fullytotally different blocks in shared info ar sometimes signedby different—totally fully fully totally different—completelydifferent users as a result of info modifications performed bydifferent users. For security reasons, once a user is revokedfrom the cluster, the blocks that were antecedently signedby this revoked user got to be re-signed by associate degreeexisting user. The straightforward methodology, that enablesassociate degree existing user to transfer the correspondinga district of shared info and re-sign it throughout user revo-cation, is inefficient as a result of the massive size of sharedinfo among the cloud. throughout this paper, we've a bent topropose a completely unique public auditing mechanism forthe integrity of shared info with economical user revocationin mind. By utilizing the thought of proxy re-signatures,we've a bent to permit the cloud to re-sign blocks on behalfof existing users throughout user revocation, therefore as thatexisting users haven't have to be compelled to be compelledto transfer and re-sign blocks by themselves. additionally,a public voucher is usually able to audit the integrity ofshared info whereas not retrieving the complete info from thecloud, although some a district of shared info has been re-signed by the cloud. Moreover, our mechanism is in associatedegree passing position to support batch auditing by verifyingmultiple auditing tasks at a similar time.

3. NPP: A New Privacy-Aware Public Auditing Schemefor Cloud DataSharing with Group Users

Description : Today, cloud storage becomes one of thecrit-ical services, as a result of users will simply modify and shareinformation with others in cloud. However, the integrity ofsharedcloud information is vulnerable to inevitable hardwarefaults, soft-ware failures or human errors. To guaranteethe integrity ofthe shared information, some schemes aredesigned to allowpublic verifiers (i.e., third party auditors)to expeditiously auditdata integrity while not retrieving theentire users' information fromcloud. sadly, public auditing onthe integrity ofshared information could reveal informationowners' sensitive informationto the third party auditor. In thispaper, we tend to propose afresh privacy-aware public audit-ing mechanism for sharedcloud information by constructing ahomomorphic verifiable groupsignature. not like the prevail-ing solutions, our theme requiresat least t cluster managersto recover a trace key hand and glove,which eliminates theabuse of

single-authority power andprovides nonframeability.Moreover, our theme ensures thatgroup users will traceinformation changes through selected binarytree; and willrecover the latest correct information block whenthe currentinformation block is broken. In addition, the formalsecurityanalysis and experimental results indicate that ourscheme isincontrovertibly secure and economical.

4.Enabling Efficient and Protected Sharing of Data in Cloud Computing
Description : Cloud storage plays a very important rolesignificantly in applications like medical files transfer and in-experienced computing where in-house data storage systemssquare measure established. In case of group-shared data,the data face every cloud-specific and conventional executivethreats. Secure data sharing among a gaggle that counters ex-ecutive threats of legitimate notwithstanding malicious usersis an important analysis issue in cloud. Protected Sharingof knowledge in cloud got to maintain: data confidential-ity and integrity; access control; data sharing (forwarding)whereas not victimization computeintensive re-encryption;executive threat security; and forward and backward accessmanagement .The PrSDC methodology encrypts a file withone coding key. a pair of wholly completely different keyshares for each of the users square measure generated, withthe user only getting one share. The possession of 1 share of akey permits the PrSDC methodology to counter the executivethreats and prevents stealing of medical files or simply justin case of inexperienced computing on-line credit paymentdetails. the alternative key share is keep by a sure third party,that's termed the scientific discipline server.

3. EXISTING SYSTEM

In Existing system data is share through the social media, Email , and centralized system but there is no security provided by the system who can recover the data changed by the hacker . In existing system use end to end communication of computers which does not have any security system for data transaction.

4. PROPOSED SYSTEM

Since the structure and overall arrangement of optical access networks is complicated and meantime, the quantity of operational fiber is big, failures of optical fibre links occur a lot of oftentimes, and thus, the price and operation administration and maintenance (OAM) stays at a high level. The period on-line fiber-fault detection and site within the optical access network with ancient optical domain reflector (OTDR) is complicated and dear, and has low resolution of the fault location .

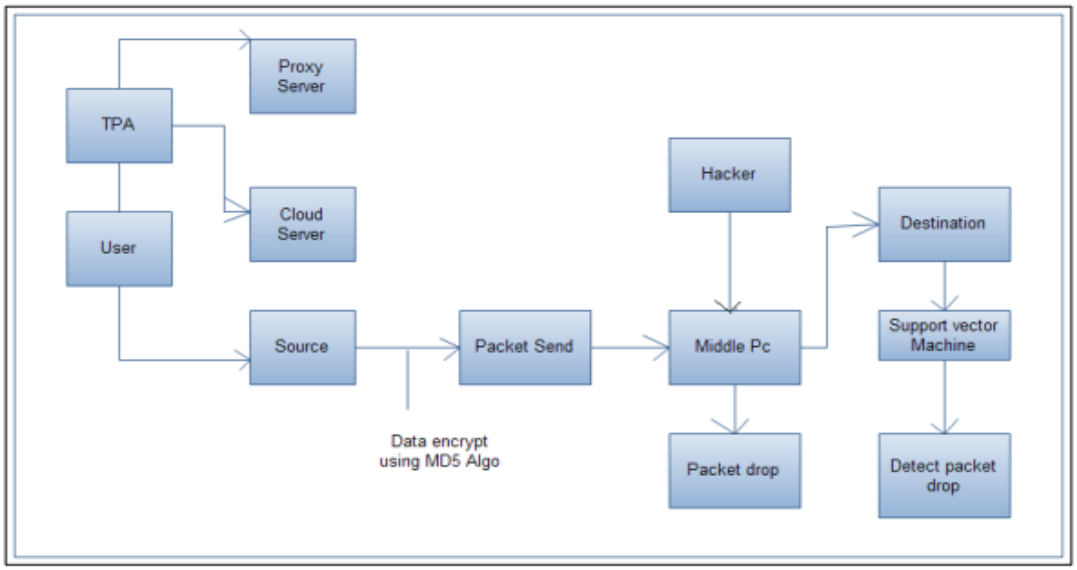

Fig. 1: Architecture Diagram

We transferred data between manager and the employees who are shared data between two system. When data is upload on system then we are stored in cloud server as well as proxy server for security purpose.

• If hacker change data between transaction then we are traces them and recover data using support vector machine (machine learning algorithm).

• So we are securely share and transferred data between multiple users on cloud computing.

Advantages of Proposed System 1) Secure data transaction
2) Data in encrypted through transaction
3) Data store in cloud server
4) Effective and efficient system for data transaction

5. CONCLUSION

Group data sharing in the cloud plays an important role when the data has to be distributed among the others. Moreover, security is one of the big concern when it comes to preserving the privacy. In this research work, we have developed a method based on the selection scheme, which helps in securing the data. We are provide cloud base encryption system for database for security purpose. Data is encrypted during the transaction which never decrypt

REFERENCES

[1]Giuseppe Aceto, Valerio Persico, Antonio Pescape, “The role of Information and Communication Technologies in Healthcare: Taxonomies, Perspectives, and Challenges”

[2] Rui Zhang and Ling Liu,” Security Models and Re-quirements for Healthcare Application Clouds”.

[3]ANSI, ISO/TS 18308 “Health Informatics- Requirements for an Electronic Health Record Architecture”, ISO 2003.

[4] R. Bakker, B. Barber, R. Tervo-Pellikka, A.Treacher,(eds.),“Communicating Health Information in an Insecure World” in: Proceedings of the Helsinki Working Conference. 43:1, 1995.

[5] B. Barber, D. Garwood, P. Skerman, In: Security in Hospital Information Systems, Security and data protection programme presented at the IMIA

♦♦♦