International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

DATA SHARING PROTOCOL TO MINIMIZE THE SECURITY AND PRIVACY RISKS OF CLOUD STORAGE IN BIG DATA

Kalla Swathi[1], M.Shelcy Moses[2], Dereddy Hemalatha[3],Chokkakula Jagadhish[4]

[1234]*Final Year B.Tech, CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam, A.P, India*
Guided by**: Mrs. Gudiwaka Vijayalakshmi, Assistant Professor,** *SVPEC, Visakhapatnam, A.P, India*

ABSTRACT:

A cloud based enormous information sharing framework uses storage space from a cloud specialist co-op to impart information to the real clients. As opposed to customary arrangements, cloud supplier stores the common information in the huge server farms outside the trust area of the information proprietor which might set off the issue of information privacy. This paper proposes a Secret Sharing Group Key Management Protocol (SSGK) and key re-encryption to safeguard the correspondence cycle and shared information from unapproved access. Not quite the same as the earlier works, group key is utilized to encode the common information and mystery sharing plan is utilized to circulate the gathering key in SSGK. Broad security and execution examinations show that our convention exceptionally limits the security and protection dangers of sharing information in distributed storage and recoveries around 12% of extra room.

INTRODUCTION:

Arising advances about huge information like Cloud Processing, Business Intelligence, Data Mining, Modern Information Integration Engineering (IIIE) what's more, Internet-of Things have opened another time for future Enterprise Systems (ES). Distributed computing is a new registering model, in which all assets on Web frames a cloud asset pool and can be allotted to various applications and administrations powerfully. Contrasted and conventional disseminate framework, a lot of venture saved, what's more, it brings remarkable flexibility, versatility, and productivity for task execution. By using Cloud Processing administrations, the various endeavour interests in building andkeeping a supercomputing or framework registering climate for shrewd applications can be successfully diminished. Building security component for distributed storage is definitely not a simple undertaking. Since shared information on the cloud is outside the control area ofauthentic members, making the common information usable upon the request of the real clients ought to be settled. Furthermore, expanding number of gatherings, gadgets what's more, applications engaged with the cloud prompts the dangerous developmentof quantities of passageways, which makes it more challenging to take appropriate access control. In conclusion, shared information on the cloud are defense less against lost or on the other hand mistakenly adjusted by the cloud supplier or network aggressors. Online reinforcement frameworks are traditionally constructed a client programming application that sudden spike in demand for not entirely settled by the buy phase of administration. Cloud reinforcements containthe product and equipment part to keep an association's information, incorporateapplications Exchange what's more, SQL Server. Online reinforcement is utilized by littleand medium estimated organizations (SMBs) and bigger ventures to back up theinformation. For bigger association, cloud information reinforcement as a correlative type of reinforcement. The distributed storage suppliers give a stage as a help, is one of the foundation administrations on distributedstorage to abbreviate capacity the executives for ventures and character clients. Executing cloud information reinforcement can help support association informationinsurance without raising the responsibility on data innovation.

EXISTING SYSTEM:

A secure sharing schemes of non public health records in cloud computing supported cipher text policy attributed-based(CP-ABE) sign-encryption. It focuses on limiting unauthorized users on access to the confidential information. Liu et al, planned an access management policy supported CP-ABE for private records in cloud computing additionally. Huang et al, introduced a unique public key coding with licensed equality warrants on all of its cipher text or a such that cipher text.

PROPOSED SYSTEM:

To address the protection downside of sharing information on the cloud storage, a secret sharing cluster key management protocol is planned within the paper and therefore the following means that square measure taken by our protocol to assist find or stop frauds.

Firstly, so as to form the shared information usable upon demand by the legitimate users, bilaterally symmetric coding algorithms square measure wont code the shared information. Once one information owner desires to share information with others, the decipherment key's is distributed to the legitimate sharers by the information owner.

Secondly, the key wont rewrite the shared information controls the access permission for shared information. Uneven coding algorithms square measure wont code the interactive message and makes solely legitimate participants have the flexibility to rewrite the key. Thirdly, just in case of shared information being familiar by unauthorized users. This protocol uses secret sharing theme to assign key to the legitimate participants.

By adding security mechanism to standard service familiarized clouds, we tend to acquire a security aware cloud and guarantee the privacy of knowledge sharing on cloud storage.

Building security mechanism on cloud storage could accelerate the readying .

METHODOLOGY:

1. CLOUD STORAGE FOR LARGE DATA:

The design of cloud based mostly massive information is illustrated.It consists of three parts: supply information, cloud center and services. Between supply information and cloud center layer, unstructured or semi-structured supply information is structured. They embody process ways like information assortment, data processing and information aggregation .

The processed supply information is kept on cloud in relative or No SQL databases .Lastly, service layer answers data requests submitted by shoppers by desegregation data kept in cloud.

Beyond permitting customers to place all information into cloud, cloud storage provides every kinds of knowledge services for patrons.

Because scale horizontally runs on low cost trade goods exhausting in a very distributed configuration and there is no would like for patrons to get and maintain their own IT facilities. Cloud based mostly massive information stores brings in inherent availableness, measure ability, and value effectiveness.

AN EXAMPLE OF HEALTHCARE INFORMATION SYSTEM:

Cloud storage provides not simply low price, however high quantifiability and availableness. It should be a natural answer to a number of issues in storing and analyzing the increasing patients' medical records. For attention suppliers, supported the aggregation of all patients' medical records, might correct diagnosing be created Reference planned a cloud-based platform for attention.

Cloud storage provides a typical place for storing medical records that overcome the delay of transferring medical records between totally different attention suppliers and build diagnostic method additional economical . The e-healthcare cloud provides several blessings unitedly an information sharing among attention suppliers . Nonetheless, in contemplate of the extremely privacy of medical information it comes with important risks of medical records.

Firstly, medical records square measure shared on the general public channel wherever several attackers on the channel to listen the medical records. To boot, because of the increasing range of parties, devices and applications concerned in cloud, unauthorized parties or cloud suppliers could have the flexibility to access shared medical records. Last however not the smallest amount, some approved parties may go along to urge some unauthorized medical records lawlessly.

E-healthcare services need a security mechanism to shield the privacy of medical records. During this section we tend to describe additional regarding the planned protocol model and rule of SSGK.

PROTOCOL MODEL:

1) INFORMATION SHARING MODEL:

Consider a cloud storage information sharing system with multiple entities and therefore the information sharing model.

The protocol model consists of three sorts of entities: cloud supplier, information owner and cluster members. The cloud supplier provides a public platform for information house owners to store and share their encrypted information.

The cloud supplier doesn't conduct information access management for house owners. The encrypted information is downloading freely by any users.

Data owner: defines the access policy and encrypts its information with a bilaterally symmetrical secret writing rule employing a cluster key. The cluster members un agency glad the access policy represent a sharing cluster. Then secret sharing theme is employed by the owner to distribute the secret writing key to the sharing cluster.

Group members: each cluster member together with the information owner is alloted with a novel and a try of keys. The cluster members will freely get any interested encrypted information from the general public cloud. However, the user will rewrite the information if and as long as it gets the information coding key from the information owner.

2) SECURITY MODEL In SSGK: we've the subsequent assumptions:

The data owner is completely trusty and can wont be corrupted by any adversaries. Cloud supplier is semi-trusted, it properly executes the task alloted to them for protests, however they might try and out the maximum amount secret data as doable supported knowledge house owners uploaded.

We currently describe the safety model of SSGK by listing doable attacks. The cluster secret's is distributed by running the key sharing theme. Components of the cluster members will gather their sub-secret shares to reconstruct the cluster key.

Moreover, the communicating of our protocol is outlined as: Each try of participants have a point-to-point channel to send messages. In additionally, all the participants access to a broadcast channel, once a participant puts a message m on this channel. All the opposite participants receive m. The cluster secret's distributed on the general public channel and also the key is also tempered by adversaries.

Verify: A verification formula that, on input a sub-share and v, output whether or not the sub-share tempered throughout distribution.

Secret Reconstructed: For any t sub-shares, the safety parameter K is reconstructed.

Equity and Availability: Verified secret sharing theme guaranteeing equity and convenience with 2 conditions:

Any participant set within the share cluster, wherever the scale of the set is a smaller amount than the entire amount. The participants within the set cannot get only data concerning K. Solely with cooperation of all the legitimate participants, K may be reconstructed.

Confidentiality: Verified secret sharing theme guarantees confidentiality if any users outside the sharing cluster cannot get any data of K even with the data of enough interactive messages.

Integrity: Once the interactive messages are tempered throughout VSS, any data concerning K may be gotten by participants.

We aforementioned that verified secret sharing theme guarantees integrity. There are certain notations are used throughout the rest of this paper.

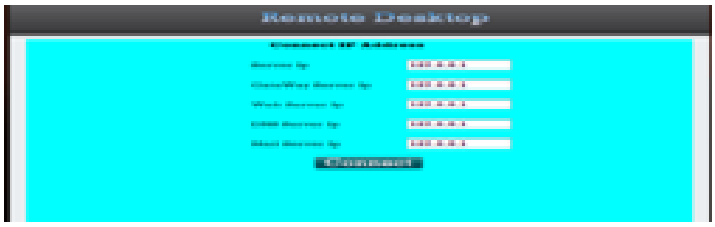
In this paper, we tend to propose a unique cluster key management protocol for the information sharing with the cloud storage. In SSGK, we tend to use RSA and verified secret sharing to form knowledge owner deliver the goods negrained control over the out-sourced data while not looking forward to any third party. Additionally, we tend to offer elaborated analysis of doable attacks and corresponding defences, that demonstrates that GKMP is secure below weaker assumptions.

Encryption secures the trans-mission on the general public channel; verified security theme build the grids information solely accessed by approved parties. The higher performance in terms of storage and computation build our theme additional sensible.

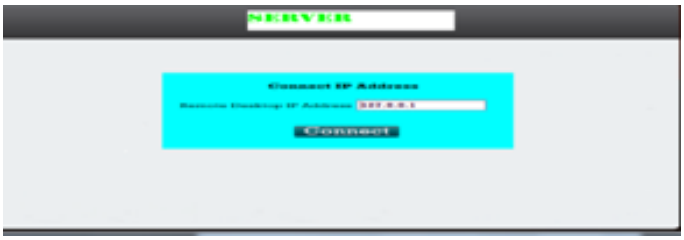
The problem of forward and backward security in cluster key management could need some additions to our protocol.

RESULT AND ANALYSIS:

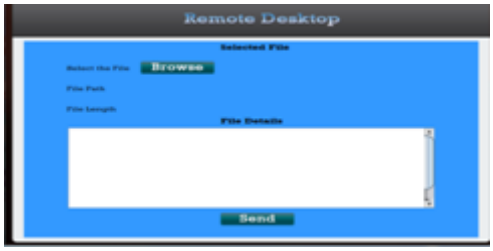
Client connecting interface:



Cloud interface:

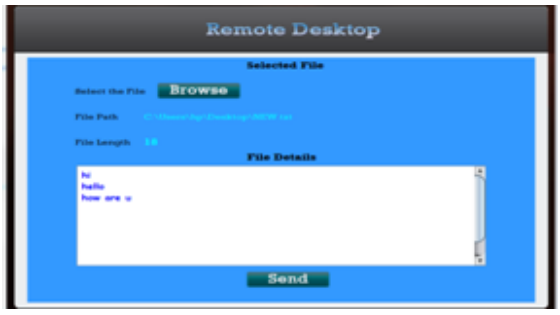


Client Dash board:

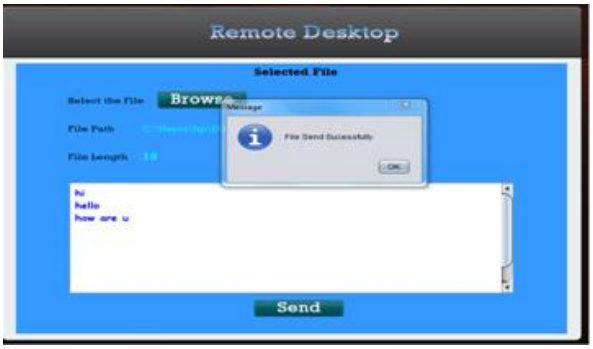


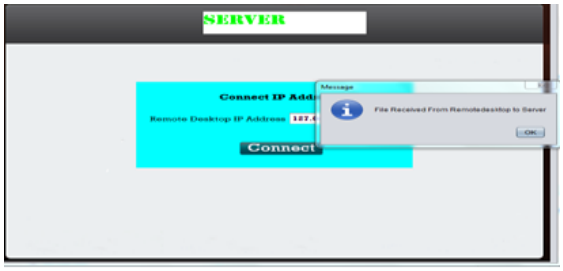
In client sending files to cloud:

File contents:

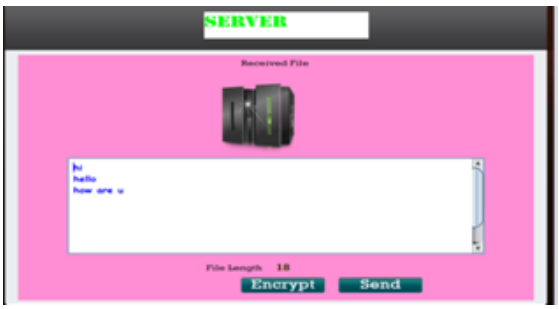


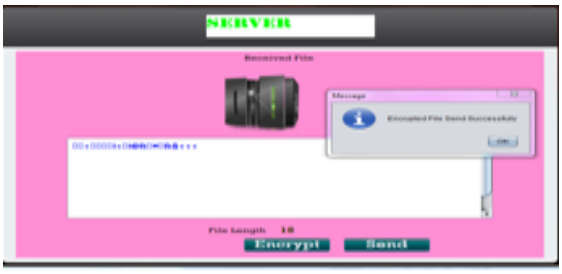
File uploaded to Cloud:

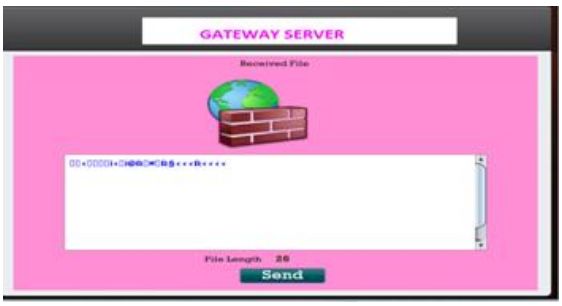


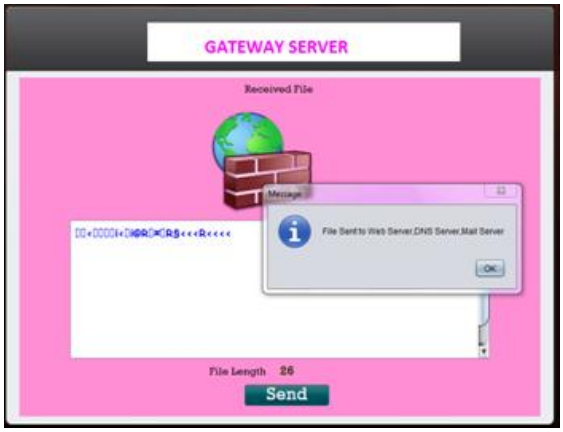


Encryption screen in cloud:









CONCLUSION:

Common worker secret's shared to scale back the knowledge discharge from cloud storage in huge data. To attenuate security and privacy risks some limits were provided that are deadline, size limit, and credit purpose limit. Data was encrypted to supply additional security (AES, DES algorithm).The worker key may be employed by one that requests to retrieve data for once. If aside from the request person tries to use worker key, then that secrets removed, and alert notifications are going to be sent to knowledge owner.

Temp key supplier sends the key to request person by mail victimisation SMTP protocol. The most advantage of planned system is to separate space for storing into module and every module is secured with worker secret. This makes additional economical constructions. This key may be used just one occasion. We have a tendency to propose a new secret sharing theme that's computationally secure and may scale back the quantity reduce the of shares worker key helps data retrieval additional secured with low price. Solely request person will use worker key. Coding standards create info troublesome to thievery. Limitations of worker key provides high security.

REFERENCES:

[1]Future of cloud computing - 2nd annual survey results. http://goo.gl/fyrZFD, 2012.

[2]S3FS-FUSE-based file system backed by Amazon S3.

[3]http://code.google.com/p/s3fs/.

[4]S3QL - a full-featured file system for online data storage.

[5]http://searchcloudstorage.techtarget.com/definiti on

[6]Krishna P.N. Puttaswamy, Thyaga Nandagopal and Murli kodialam "Frugal storage for cloud file system," in proceeding EuroSys'12 of the 7th ACM European conference on computer Systems, 2015 pages 71-84.

[7]P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish "Depot: Cloud Storage with Minimal Trust," In Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI), Oct. 2010.

[8]J. Howard "Scale and performance in a distributed file system" ACM Trans.Computer Systems, 1988.

[9]P. Hunt, M. Konar, F. Junqueira, and B. Reed. "Zookeeper: Waitfree coordination for internetscale services," In USENIX ATC, 2010.

[10]A. Bessani, E. P. Alchieri, M. Correia, and J. S. Fraga "DepSpace: A Byzantine fault- tolerant coordination service," in EuroSys, 2008.

[11]StorSimple. StorSimple. http://www.storsimple. com/.

[12]Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando Andr´e, and Paulo Sousa "DEPSKY: Dependable and Secure Storage in a Cloud-of-clouds," EuroSys 11-April

[13]Ricardo Mendes, Tiago Oliveira, Vinicius Cogo, Alysson Bessani "The SSGK PROTOCOL file system,"

[14]Idilio Drago, Marco Mellia, Maurizio M. Munafò, Anna Sperotto and Aiko Pras "Inside Drop box: Understanding Personal Cloud Storage Services," in Proceeding of IMC -12 of ACM conference on internet measurement conference,2012 PP.481- 494.

BIOGRAPHIES

MRS.GUDIWAKA VIJAYALAKSHMI

Currently working as assistant professor from department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College

KALLA SWATHI

Pursuing B. Tech from department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College

M.SHELCY MOSES

Pursuing B. Tech from department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College

DEREDDY HEMALATHA

Pursuing B. Tech from department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College

CHOKKAKULA JAGADISH

Pursuing B. Tech from department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College