Aggregate Key Sharing Mechanism for Sharing Data in Group via Cloud Storage

R.U. Patil, Prof. A.J. Kadam
M.E, Department of Computer Engineering, All India ShriShivaji Memorial Society's, College of Engineering Pune, SavitribaiPhule University, Pune, India
Professor, Department of Computer Engineering, All India ShriShivaji Memorial Society's, College of Engineering Pune, SavitribaiPhule University, Pune, India

Abstract-In cloud storage data sharing is an important utility. Most of the users attracted by cloud storage because of its numerous benefits. The idea of Key Aggregate Searchable Encryption is build through a concrete KASE scheme. In this scheme data owner distribute single trapdoor to the cloud. In this paper, we used multi cloud for storing & accessing the large amount of data because in cloud environment, large amount of data produced everyday. So, demands for resource is increasing but still clients are worrying about their data is correctly stored & maintained by providers without intact. In this scheme, data owner upload file on multi cloud by splitting files into no. of equal size & store it on multi cloud. User using shared key by data owner, submit single trapdoor to cloud for searching the documents or files. Then after completion of search merge this file parts and then user can download this documents. The security examination and execution evaluation both certify that our propose arrangements are provably secure and basically beneficial. Hence this paper, we are use multi cloud to reduce storage overhead of the customer by compressing the data and reduce computational overhead of the cloud storage server.

Keywords- Searchable encryption, data sharing, cloud storage, data privacy.

I. INTRODUCTION
Distributed storage is an answer for sharing and getting to substantial measure of information. Today, various clients are sharing different sorts of reports, for example, photographs, recordings and archives by means of different long range informal communication construct applications in light of regular routine. Business clients are additionally being pulled in towards utilizing the distributed storage because of its focal points. Be that as it may, while sharing information through distributed storage, clients need to at the same time mindful about the information spillages in the cloud. Commonly business associations need to share the secret information inside the association or to alternate associations. Consider a situation where an administrator needs to impart various classified documents to one of the representative then director will transfer assume n number of records on distributed storage and will give n number of encryption keys to the worker. The representative will store all the keys safely. At that point utilizing these keys, the worker will create the watchword trapdoor for getting to the records. So for n number of documents, it is not productive to give n number of keys, store them safely and afterward create trapdoors for each record. It turns out to be extremely costly at the worker's side server. This pragmatic issue propels to build a plan which will give a solitary accumulated key to the worker and will enable access to the cloud by creating single trapdoor by the representative to get to any number of files. In this paper, we propose the novel idea of key-total searchable encryption (KASE), and instantiating the idea through a solid KASE strategy. The propose KASE conspire identifies with any of the distributed storage that backings the searchable collecting information sharing component, which implies any client may like to appropriate a gathering of documents which are particular with a gathering of chose clients, while allowing the last to do catchphrase seek over the prior. To keep up searchable gathering information sharing the principle requirements for productive key administration are twofold. Essentially, an information proprietor needs to apportion a solitary whole key (rather than a gathering of keys) to the
client to sharing different records. Resulting, the user needs to present a solitary total trapdoor to the cloud for performing watchword look over any amount of shared documents. KASE plan can guarantee both solicitations and security scenarios.

II. REVIEW OF LITERATURE

S. Yu, C. Wang, K. Ren, and W. Lou, proposed dispersed figuring is a creating handling perspective in which resources of the enrolling system are given as organizations over the Internet. As promising as it is by all accounts, this perspective moreover conveys various new challenges for data security and gets the opportunity to control when customers outsource sensitive data for sharing on cloud servers, which are not inside an unclear placed stock in space from data proprietors. To keep fragile customer data private against untrusted servers, existing courses of action generally apply cryptographic methods by revealing data unscrambling keys just to affirmed customers. Regardless, in doing accordingly, these courses of action unavoidably exhibit a mind-boggling figuring overhead on the data proprietor for key flow and data organization when fine grained data get the opportunity to control is needed, and in this way don't scale well. The issue of in the meantime finishing fine-grainedness, versatility, and data mystery of get the chance to control as a general rule still remains unverifiable. This paper addresses this testing open issue by, on one hand, describing and maintaining access game plans in light of data qualities, and, of course, empowering the data proprietor to assign most by far of the computation errands required in fine grained data get the chance to control to untrusted cloud servers without uncovering the key data substance. We achieve this target by mishandling and uncommonly combining strategies of trademark based encryption (ABE), middle person re-encryption, and detached re-encryption. Our propose scheme similarly has eminent properties of customer get the opportunity to profit characterization and customer riddle key obligation. Wide examination exhibits that our propose plan is significantly capable and provably secure under existing security models[1].

X. Liu, Y. Zhang, B. Wang, and J. Yan proposed with the characters of low support and little organization cost, circulated processing offers an intense and calm approach for data sharing in the cloud among social affair people. Regardless, since the cloud is scheming, the security guarantees for the sharing data transform into our stresses. Unfortunately, in light of the progressive change of the enlistment, sharing data while giving security sparing is up 'til now a testing issue. Starting late, Liu et al showed a secured multi-proprietor data sharing arrangement, named Mona, which was ensured that any social affair part could subtly give data to others by abusing bundle signature strategy. Meanwhile, the arrangement could deliver fine-grained get the chance to control, which infers that not only the get-together people could use the sharing data resource at whatever point, moreover the new customers could use the sharing data instantly after their revocations and the revoked customers won't be allowed to use the sharing data again after they are removed from the social event. In any case, through our security examination, the Mona plot still has some security vulnerabilities. It will successfully encounter the evil impacts of the course of action strike, which can provoke the denied customers getting the sharing data and divulging other genuine people's insider certainties. Additionally, there is another security insufficiency in the customer selection arrange, which is the way by which to guarantee the private key while circling it in the unsecure correspondence channels. This kind of attack can in like manner incite divulging the customer's secret data [2].

C. Chu, S. Chow, W. Tzeng, et al. proposed data sharing is an essential value in dispersed stockpiling. In this article, we exhibit to securely, viably, and adaptably bestow data to others in conveyed stockpiling. We depict new open key cryptosystems which make predictable size ciphertexts with the ultimate objective that gainful task of unscrambling rights for any plan of ciphertexts are possible. The peculiarity is that one can add up to any game plan of riddle keys and make them as littler as a singular key, yet including the vitality of all the keys being gathered. Figuratively speaking, the puzzle key holder can release a steady size aggregate key for versatile choices of ciphertext set in disseminated stockpiling, yet the other mixed records outside the set remain private. This insignificant aggregate key can be favorably sent to others or be secured in a shrewd card with outstandingly compelled secure stockpiling. We give formal security examination of our arrangements in the standard model. We
furthermore portray other utilization of our arrangements. In particular, our arrangements give
the principle open key patient-controlled encryption
for versatile movement, which was yet to be known
[3].

X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang
proposed attribute based check (ABS) enables
customers to sign messages over qualities without
revealing any information other than the way that
they have affirmed the messages. Regardless,
considerable computational cost is required in the
midst of checking in existing work of ABS, which
grows straightforwardly with the traverse of the
predicate formula. Accordingly, this displays an
enormous test for resource constrained devices, (for
instance, PDAs or RFID marks) to perform such
considerable computations unreservedly. Going for
taking care of the test above, We at first propose
and formalize another perspective called
Outsourced ABS, i.e., OABS, in which the
computational overhead at customer side is
amazingly diminished through outsourcing genuine
figurings to an untrusted checking cloud authority
association (S-CSP). Besides, we apply this novel
perspective to existing ABS arrangements to
diminish the multifaceted nature. In this manner, we
show two concrete OABS arranges: i) in the main
OABS plot, the amount of exponentiations
incorporating into stamping is diminished from
O(d)to O(1) (around three), where d is the upper
bound of breaking point regard portrayed in the
predicate; ii) our second arrangement depends on
Herranz et al's. improvement with unaltering size
imprints. The amount of exponentiations in
checking is lessened from O(d^2)to O(d) and the
correspondence overhead is O(1). Security
examination demonstrates that both OABS
arrangements are secure similarly as the
unforgeability and trademark guarantor insurance
definitions decided in the proposed security
illustrate. Finally, to mull over high adequacy and
flexibility, we discuss expansions of OABS and
show to achieve duty too [4].

C. Wang, Q. Wang, K. Ren, and W. Lou proposed
appropriated registering is the since a long time
back envisioned vision of figuring as an utility,
where customers can remotely store their data into
the cloud to welcome the on-demand choice
applications and organizations from a typical pool
of configurable preparing resources. By data
outsourcing, customers can be mitigated from the
heaviness of close-by data stockpiling and upkeep.
Regardless, the way that customers no longer have
physical responsibility for possibly sweeping size of
outsourced data makes the data uprightness
confirmation in Cloud Computing an amazingly
troublesome and perhaps extensive task, especially
for customers with obliged figuring resources and
capacities. Thusly, enabling open auditability for
cloud data stockpiling security is of essential
criticalness so customers can fall back on an
external survey social event to check the
uprightness of outsourced data when required. To
securely exhibit a capable untouchable evaluator
(TPA), the going with two focal necessities must be
met: 1) TPA should have the ability to gainfully
audit the cloud data stockpiling without asking for
the adjacent copy of data, and present no additional
on-line weight to the cloud customer; 2) The pariah
reviewing system should get no new vulnerabilities
towards customer data security. In this paper, we
utilize and astoundingly join the all inclusive
community key based homomorphic authenticator
with sporadic veiling to finish the security sparing
open cloud data looking at system, which meets
each above need. To support powerful treatment of
different assessing endeavors, I moreover examine
the arrangement of bilinear aggregate check to open
up our rule result into a multi-customer setting,
where TPA can play out various investigating
assignments in the meantime. Wide security and
execution examination shows the proposed
arrangements are provably secure and especially
viable [5].

III. PROPOSE SYSTEM APPROACH
In this paper, we address this test by proposing the
novel idea of key-total searchable encryption
(KASE), and instantiating the idea through a solid
KASE plot. The propose KASE plot apply to any
distributed storage that backings the searchable
gathering information sharing helpfulness, which
implies any client may specially impart a gathering
of chose documents to a gathering of chose clients,
while enabling the last to perform catchphrase look
over the previous. To bolster searchable collecting
information sharing the basicerequirements for
proficient key administration are twofold. Initial, an
information proprietor just needs to convey a
solitary total key (rather than a gathering of keys) to
a client for sharing any number of documents. Second, the client just needs to present a solitary total trapdoor (rather than a gathering of trapdoors) to the cloud for performing catchphrase look over any number of shared records. To the best of our insight, the KASE plot propose in this paper is the main known plan that can fulfill both prerequisites (the key-total cryptosystem [4], which has motivated our work, can fulfill the principal necessity yet not the second). Contributions. All the more particularly, our principle commitments are as per the following.

1) We propose a general framework of KASEseven algorithms for security purpose parameter setup, key generational algorithm, encryption algorithm, key extraction algorithm, trapdoor generation algorithm, trapdoor adjustment scenarios algorithm, and trapdoor testing algorithm. We then describe both functional and security requirements for designing a valid KASE technique.

2) We then instantiate the KASE framework by designing a KASE scheme. After providing detailed constructions for the seven algorithms, we evaluate the efficiency of the schemes, and establish its security in the course of detailed analysis.

3) We discuss different issues in building an actual group data sharing system based on the propose scheme, and evaluate its performance. The evaluation confirms our system can meet the performance requirements of practical applications in this architecture.

IV. SYSTEM ARCHITECTURE

![System Architecture Diagram]

A. Module Description

1) Key Generation

In this module admin going to generate two keys for encryption and decryption process. By using Asymmetric algorithm, admin going to generate master secret key and public key.

2) Access Control

In which admin going to give access control for the files he will going to upload files, while uploading admin going to encrypt the file which he has to upload with the help of master secret key for the security purpose to the cloud.

3) Keyword Indexing

Remove unnecessary words from the file and find the keywords. Calculate the Content Weight age of keywords Convert the Keywords into hash code by using MD5 algorithm; place the hash code in Index Array.

4) Send Aggregate Key

Based on the categories selected by admin, system has to fetch the corresponding hash keys + fetch the Public Key. Generate the User Aggregate Key and finally send it to users.

5) Search With Keyword

User has to select the aggregate Key then after that input the search keyword. Convert the keyword into hash code. Decrypt the aggregate Key, Separate and get hash keys and separate and get public Key. Using Hash Key and keyword generate hash codes (Trapdoor). Send the Hash codes to server, based on the Hash codes received server has to check the keyword index and if any matching files are available, list all the file names to the user. (Adjust & Test) View the shortlisted files from server, download the files and finally decrypt the file with owner public key.

V. MATHEMATICAL MODEL DESIGN

Generate A Public Key And Private Key
First we need our keys: A private key that the server will keep and a public key that can be given away.

We need 2 prime numbers:

\[ p \] \& \[ q, \quad p = 29, \quad q = 31 \]

Calculate \[ n = p \times q = 29 \times 31 = 899 \]

Calculate \[ t = (p - 1) \times (q - 1) = (29 - 1) \times (31 - 1) = 840 \]

Choose a prime number \( e \), \( e \) needs to be relatively
prime to \( t \). (\( t \) cannot be divisible by \( e \)) Lets pick 11 we now need to find \( d \). we will use the formula: \( d \ast e \equiv 1 \mod t \)

This means \((d \ast 11) / t\) will give us a remainder of one. You have to find the inverse of \( e \mod t \). Since we are dealing with such small numbers we can sort of guess our \( d \) until we find one that works. \((611 \ast 11) = 6721, 6721 / 840 = 8 \) with remainder 1. So 611 works! We now have everything we need for a private and public key to encrypt our data.

\[
\begin{align*}
p & = 29 \\
q & = 31 \\
n & = 899 \\
t & = 840 \\
e & = 11 \\
d & = 611
\end{align*}
\]

Our public key becomes \( n \) and \( e \).

Our private key becomes \( n \) and \( d \).

File Encryption

\[
\text{Encrypt}(pk, i)
\]

This algorithm is run by the data owner to encrypt the \( i^{th} \) document and generate its keywords’ ciphertexts. For each document, this algorithm will create a delta \( \Delta i \) for its searchable encryption key \( k_i \). On input of the owner’s public key \( pk \) and the file index \( i \), this algorithm outputs data ciphertext and keyword ciphertexts \( Ci \).

Trapdoor Generation

\[
\text{Trapdoor}(k, w)
\]

This algorithm is run by the user who has the aggregate key to perform a search. It takes as input the aggregate searchable encryption key \( k_a \) and a keyword \( w \), then outputs only one trapdoor \( Tr \).

VI. EXPERIMENTAL SET UP

A. Graph

AES:

1) Uploading Time: -

<table>
<thead>
<tr>
<th>File Length</th>
<th>Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>173</td>
</tr>
<tr>
<td>351</td>
<td>253</td>
</tr>
<tr>
<td>15</td>
<td>265</td>
</tr>
</tbody>
</table>

2) Downloading Time

<table>
<thead>
<tr>
<th>File Length</th>
<th>Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1323994</td>
<td>67</td>
</tr>
<tr>
<td>1824603</td>
<td>114</td>
</tr>
</tbody>
</table>

CONCLUSION

Think about the practical problem of privacy of the data sharing scheme based on cloud technique which needs a data owner to give large number of keys to data users to permit them to access his/her
documents, we for the first time propose the concept of key-aggregate searchable encryption (KASE) and construct a solid KASE scheme. Both analysis and evaluation results prove that my work can give an effective solution to constructing practical sharing scheme based on public cloud storage. In a KASE scheme, the owner only needs to give single key to a user when sharing large amount of documents with the user, and the user only needs to submit a solitary trapdoor when he queries overall documents shared by the same owner. Multi cloud is to reduce storage overhead of the customer by compressing the data and reduce computational overhead of the cloud server.

REFERENCES


