An Efficient Data Sharing in Public Cloud using two way Authentication & Encryption

Roshni Sharma
Truba Institute of Engg. & Information Technology
Bhopal, India

Prof. Amit Saxena
Truba Institute of Engg. & Information Technology
Bhopal, India

Dr. Manish Manoria
Truba Institute of Engg. & Information Technology
Bhopal, India

***Abstract*— Cloud computing enables various users to share their data over secure channel. Although various security algorithms are implemented for the security of shared data over public clouds. Here in this paper a new and efficient technique for the data sharing over public clouds is proposed using two password based authentication and public auditing. The planned method implemented here provides competent communication cost as well as provides high detection of valid and revoked users. The methodology is based on the idea of provided that one instance private key and then sharing of data and encryption using Session keys using image.**

I. Introduction

Cloud computing is a replica for enabling suitable, on-demand system right of entry to a joint puddle of configurable compute capital that can be quickly provisioned and at large with negligible organization try. The causal notion of cloud computing is the departure of applications from the operating systems and the hardware on which they run. Cloud computing convey applications via the internet, which are accessible from trap browsers and desktop and itinerant apps, while the software and data are stored on servers at a remote location [1].

Today, our data is migrating beyond the boundaries of our personal computers and all our data would still safely reside on the web, accessible from any Internet-connected computer, anywhere in the world because of cloud computing.

Before a extended occasion we were as long as verification with the bodily look of being and by their name physically, but at the present a day's dissimilar technique were implemented. One of them is contracts signing. Contract signing is very significant procedure by which we can conversation our documents by operational. So through the assistance of this system we can stop different attack So the solution is implemented a new scheme or new protocol which is more efficient and more secure and preventing from different attacks which can be used in a variety of applications especially in E-commerce. Cloud Computing is the emerging technology where we can get platform as a service, software as a service and infrastructure as a service. While it comes to storage as a overhaul, information privacy and information operation are the most important issues to be dealt with. For lever the business of documents to and on or after the darken wine waiter, the documents are encrypted prior to being outsourced to the commercial public cloud. Cloud computing is an budding paradigm offering outsourced services to enterprises for storing and processing a huge amount of data at very competitive costs. However, they do not hold admission be in charge of policies to adjust right to use to a scrupulous division of the stored information. State-of-the-art policy based mechanisms can effort only once they are positioned and operated within a trusted domain [2].

Proper security is achieved if exchange protocol having no los-preventing property. Loss preventing property means any party incurred no loss at all with other party. We can say that this protocol provide true fairness whenever parties exchange their data or information to each other or not.

The procedure itself is comparatively easy find computationally well-organized calculation. Though, maintaining a TTP that needs to be on-line continually can be luxurious. In this brand of a etiquette, the TTP is drawn in in the etiquette only if one of the parties behaves unlawfully or aborts the set of rules ahead of time; or else the TTP is by no means concerned in the procedure. Hence, these rules are also known as "hopeful" fair-exchange protocols [2]. These procedures are unfeasible since extensive amounts of communication are needed.

The cloud computing environment refers to the hardware and systems software in the datacenters that provide computing resources as services [3]. Delivering the computing resources such as operating system, hardware, software as a service rather than a product is called a cloud computing service.

Cloud Computing is a promising next-generation IT architecture which provides elastic and unlimited resources, including storage, as services to cloud users. In Cloud Calculating cloud operators and cloud facility earners are nearly sure to be from different trust areas. It turns out that on one hand sensitive data should be encrypted before uploading to cloud waitpersons; on the additional cane, a safe user- compulsory statistics admission switch device must be as long as before cloud operators have the freedom to subcontract delicate data to the cloud for stowage, Comparable to previous work [4].

Proxy waitrons will apprise top-secret keys for all employers but the one to be annulled. In this way our construction places minimal load on the authority upon each revocation event. Existing schemes 5] suggest associating expiration time attributes to user secret keys.

However, the expiration method just enables user revocation at a prearranged time, but is not able to efficiently revoke user attributes on the fly.

One Time Private Key

In daily life there are various electronic transaction techniques by which we can perform quick transactions from one party to other. There are various security techniques implemented by which we can perform a secure communication of data from one party to other. So to overcome this problem a newly implemented security technique is used for authentication that is known as One Time Private Key (OTPK). One period private important is main which is used for actual small time by the despatcher and headset ,when the correspondent and headset gets authenticate or performing encryption or decryption the key is destroyed and we can never be use this key for further communication.

II. Literature Survey

Lei et al. [6] additionally evaluated to symmetric key based methods, here author find a new approach can proficiently deal with keys and user revocations. In symmetric key methods, clients are necessitated to deal with a number of keys equivalent to as a minimum the logarithm of the numeral of clients, while in their come within reach of each client only requires to sustain its public/private key pair. Additional, revocation of clients in a characteristic symmetric key method involves informing the private keys known to all the clients in the group, while in their method private keys of the clients are not need to be transformed.

In this paper, author has concentrate on the limitations of such they differentiate and appreciate the concerns of make safe investigate over encrypted cloud [7] data at the same time as discount firm scheme intelligent security in the distributed computing perfect representation. Among different multi-keyword semantics, they make a choice the productive correspondence determine of "direction matching," i.e., the identical amount of matches as feasible, to grab the significance of information documents to the search query. In exacting, they make use of "inner product similarity", i.e., the amount of query keywords demonstrating up in a document, to quantitatively evaluate such similarity calculate of that document to the search query.

In this paper author complete practice of CP-ABE in the background of innovativeness claims and also industrialized a cancelation instrument that instantaneously permits high flexibility, fine-grained access control and revocation. The department assigns users a set of attributes within their secret key and distributes the secret key to the respective users. Any user that satisfies the access control policy defined from the data collaborator can access the data. When a user is revoked access rights, the data is re-encrypted in the Cloud rendering the revoked user’s key useless. The scheme is proven to be semantically securing against chosen cipher text attacks against the CP-ABE model. However, the scheme is not elegant in the case of user revocation since the updating of cipher texts after user revocation places heavy computation overhead even if the burden is transferred to the Cloud [8].

In this paper author has propose a novel mediated Certificateless Public Key Encryption (mCL-PKE) [9] method that does not use pairing process. In view of the fact that most CL-PKC methods are in illumination of bilinear pairings, they are computationally expensive. In such case of bilinear pairings, the data owner has to encrypt the identical data encryption key multiple instants, once for each customer, using the client’s public keys. To concentrate on this deficiency, they commence an expansion of the essential mCL-PKE system. Their widen mCL-PKE method necessitate the data owner to encrypt the data encryption key only once upon a time and to make available some extra information to the cloud so that authorized customers can decrypt the substance using their private keys their method abbreviates the computational in the clouds by exploiting a pairing-free move toward.

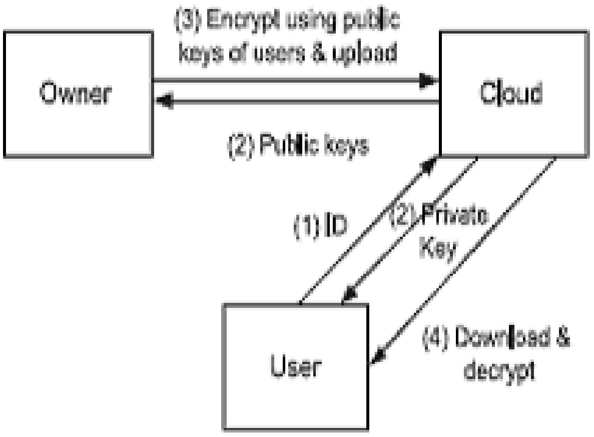

Fig .1 CL-PKE based fine-grained encryption [9]

Additional, the handing out expenditures for straightening out at the clients are reduced as a semi-trusted security go between to some extent decrypts the encrypted data before the clients decrypts. The safety measure goes about as a collection accomplishment position also and facilitates immediate revocation of cooperation or malicious users. The cloud is working as a secure storage space in addition to a key generation center. The secrecy of the substance and the keys is protected with value to the cloud, because the cloud cannot entirely decrypt the information. Figure 1 shows CL-PKE based fine grained encryption. They put into operation mCL-PKE method and the overall cloud based system, and evaluates its security and performance [9]. Results show that schemes are efficient and practical. Further, for multiple users satisfying the same access control policies, the get better move toward completes only a single encryption of each data item and decreases the on the whole transparency at the data owner.

A. Sahai and B. Waters proposed Fuzzy Identity-Based Encryption. They present two constructions of Fuzzy IBE schemes. This building can be imply as an Identity-Based Encryption of a communication beneath more than a few attribute that create a (fuzzy) individuality. They primary introduce quality base encryption (ABE) for encrypted right of entry manage [10].

V. Goyal et al. [11] first introduced the concept of CP-ABE based on ABE. The main idea is to develop a much richer and secure type of attribute-based encryption cryptosystem.A user is able to decrypt a ciphertext if the attributes associated with a ciphertext satisfy the key's access structure. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [11].

Bethencourt et al [12] suggested Ciphertext-Policy Attribute Based Encryption. They created a system for Ciphertext-Policy Attribute Based Encryption.

III. Proposed Methodology

Stage 1: Registration

In the registration process TTP (trusted third party) generate a registration form for the user, user filled all the required information and send to the TTP. TTP verify all the beneficial information and store in his database. User generate password as per the instruction given by the trusted third party and send to the TTP, after that TTP store this password in his database for further verification of the user at the time of signing.

Here example of some important information which is needed to registration form to registered like:

1. user name
2. mobile number
3. email address
4. Address etc.

Stage 2: Signing

User enter the password and signing to the trusted third party. Here in this stage each of the user's needs to generate digital signatures for the authentication. First of all generate a key pair of public/private key and for the authentication of the user, each user needs to provide the OTP token to the CA (certified authority) so that it will verifies the authenticity of the user and as soon as authentication gets success the key pair gets destroys.

In our proposed protocol we have work on OTPK (one time private key) in the context of password authentication key exchange (PAKE) protocol. Our protocol works on three steps which are deliberated under. In step 1 we show the message amid party P_1 and right-hand third party, in step 2 shows the announcement between trusted third party and party P_2 and step 3 shows the statement between party P_1 and party P_2.***Step 1***. Communication between party P_1 and trusted third party (TTP) or Server.

Party P_1 TTP ↔

In figure 2 we have show working module between the party P_1 and trusted third party.

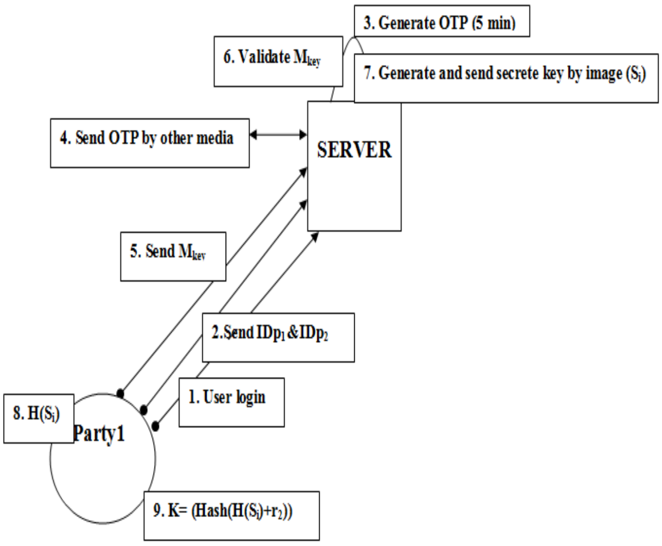

Figure 2: Communication between party P_1 and server

a) User login

Party P_1 login with Pw_1 and required information to the trusted third party, TTP verify the password and if password is valid then print the message user successfully login otherwise print the invalid password message.

b) Send identities

Party P_1 send the identities (IDp_1 & IDp_2) to the trusted third party, and TTP recognized the identities for further communications.

Generate random number r (one time password)

When the above two steps is successfully done the TTP generate random number 'r_1' for the party P_1 with the timestamp (5 minute). That random number r_1 sends to the party via other media (email).

Note: timestamp (5 minute) means r automatically destroys in 5 minute.

Party P_1 perform function

In this stage party P_1 perform some functions like:

i. Generate master key (M_{key})
M_{key}= H(r_1+Pw_1)
ii. Keep this random number in memory.
iii. Send M_{key} to the TTP.

c) Verification

TTP matched the M_{key} with own calculated M_{key}, if that is valid then server generated imaged based key (this method describe above in section image based key generation) S_i and calculated hash H(S_i) of this key and send to the party P_1.

Session key(K) generation:

$$K=Hash(H(S_i) + r_1)$$

The party P_1 generated his common session key (K) by the concatenate of H(S_i) and random number r_1.

Step 2. Communication between party P_2 and trusted third party (TTP) or Server.

Party P_2 TTP ↔

In figure 3 we have show working module between server and party P_2.

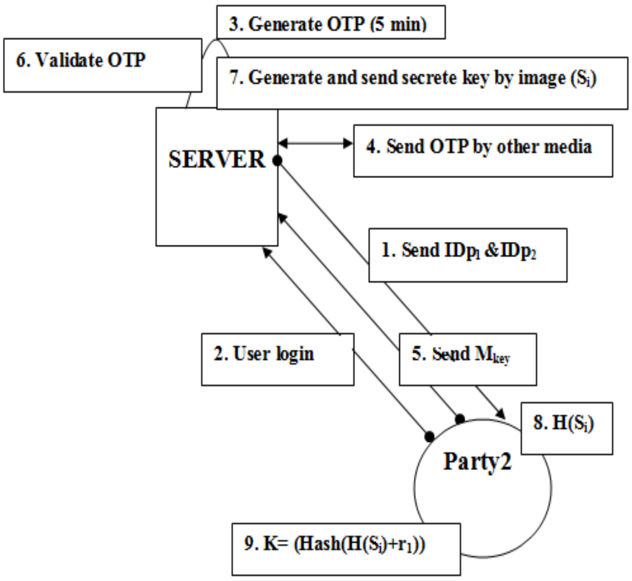

Figure 3: working module between party P_2 and server

a) Send identities

TTP send the identities (IDp_1 & IDp_2) to the party P_2 via other media(mobile or email), party P_2 recognized the identities for further communications and go to process of login.

b) User login

Party P_2 login with Pw_2 and required information to the trusted third party, TTP verify the password and if password is valid then print the message user successfully login otherwise print the invalid password message.

c) Generate random number r (one time password)

When the above login process is successfully done the TTP send previously generated random number 'r_2' for the party P_2 with the timestamp (5 minute). That random number r_2 sends to the party via other media (email).

Where $r_1 = r_2$;

Note: timestamp (5 minute) means r automatically destroys in 5 minute.

d) Party P_2 perform function

In this stage party P_2 perform some functions like:

a. Generate master key (M_{key})

$M_{key} = H(r_2+Pw_2)$

b. Keep this random number in memory.

c. Send M_{key} to the TTP.

e) Verification

TTP matched the M_{key} with own calculated M_{key}, if that is valid then server generated imaged based key (this method describe above in section image based key generation) S_i and calculated hash $H(S_i)$ of this key and send to the party P_2.

f) Session key(K) generation

$$K=Hash(H(S_i) + r_2)$$

Party P_2 generated his common session key (K) by the concatenate of $H(S_i)$ and random number r_2.

Here we know $r_1 = r_2$;

So $K= (Hash(H(S_i) + r_1)) = (Hash(H(S_i) + r_2))$

Step 3. Communication between party P_1 and party P_2.

Party P_1 ↔ party P_2

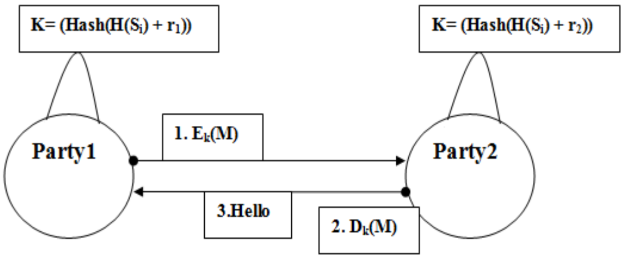

Figure 4: working module between party P_1 and party P_2

IV. Result Analysis

The table shown below is the analysis and comparison of data sharing techniques using ciphertext attribute based encryption and proposed work. The comparison is based on the time for the data to be shared and the communication cost required in bits.

Here the communication cost can be computed and analyzed on the basis of various times such as 1,2, 3….10 hrs and hence the existing and the proposed technique is analyzed. The planned procedure executed here offers efficient communication cost as compared to the existing CP-ABE based technique.

	Communication Cost in bits	
Time in hours	**CP-ABE**	**Proposed Work**
1	10	5
2	12	7
3	13	9
4	15	10
5	17	13
6	18	15
7	25	18
8	28	19
9	31	20
10	35	22

Table 1. Comparison of Communication Cost in bits

The table shown below is the comparison of total user revocations time required for the data to be shared. The proposed methodology generates and requires less user revocations as compared to CP-ABE.

Here the User revocation can be computed and analyzed on the basis of various times such as 1, 2, 3….10 hrs and hence the existing and the proposed technique is analyzed. The planned procedure realized here provides efficient detection of user revocation as compared to the existing CP-ABE based technique.

	CP-ABE		**Proposed Work**	
Time in hours	**Valid User**	**Revoked User**	**Valid User**	**Revoked User**
1	2	1	4	0
2	3	1	4	1
3	5	2	6	1
4	5	3	7	2
5	5	3	7	2
6	5	3	8	2
7	6	4	8	2
8	6	4	9	3
9	7	5	9	3
10	7	5	10	4

Table 2. Comparison of Computation Time

The graph shown below is the analysis and comparison of data sharing techniques using ciphertext attribute based encryption and proposed work. The comparison is based on the time for the data to be shared and the communication cost required in bits.

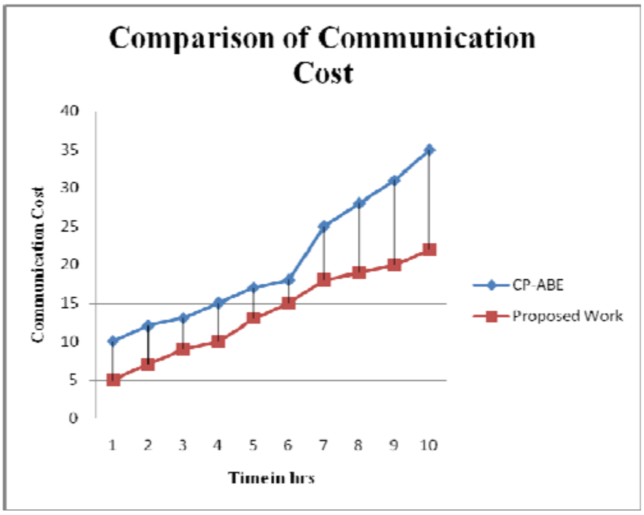

Figure 5. Communication Cost in bits

V. Conclusion

Statistics Distribution using Crucial based encryption system is not a feasible technique when compared with the existing cryptogram transcript strategy Attribute based encryption, but the projected procedure executed here grounded key policy based encryption using Two feature using OTPK and Image based authentication provides efficient security from various attacks and also escrow problem and user revocation is prevented.

The result analysis shows the performance of the proposed methodology. The technique implemented for the data sharing takes less computational cost and needs less user revocations as compared to the cipher text attribute based encryption technique. The methodology implemented here for the data sharing using one time private key and true random number generator is an efficient technique which prevents from various attacks in the network as well as minimizing the computational cost and increases the detection of valid users and revoked users.

References

[1] Seung-Hyun, Xiaoyu Ding,” An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”, IEEE Transactions on Knowledge & Data Engineering, IEEE 2014.

[2] Alfin Abraham, Vinodh Ewards, Harlay Maria Mathew ,“A Survey on Optimistic Fair Digital Signature Exchange Protocols”, *International Journal on Computer Science and Engineering (IJCSE)*, ISSN: 0975-3397, Vol. 3, No. 2, pp. 821 – 825, Feb 2011.

[3] Michael Armbrust, Armando Fox, Rean Grith, Anthony D. Joseph, Randy H.Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[4] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In Proc. of VLDB’07, Vienna, Austria, 2007.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP’07, Washington, DC, USA, 2007.

[6] X. W. Lei Xu and X. Zhang, “CL-PKE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud,” in ACM Symp. Inform. Comput. Commun. Security, 2012.

[7] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014.

[8] Tu S, Niu S, Li H, Xiao-ming Y, Li M, “Fine-grained access control and revocation for sharing data on clouds,” IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.

[9] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding and Elisa Bertino "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.

[10] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption”, *Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt ’05)*, pp. 457-473, 2005.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data”, *Proceedings of ACM Conference on Computer and Communication Security*, pp. 89-98, 2006.

[12] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-PolicyAttribute Based Encryption”, *Proceedings IEEE Symposium Security and Privacy*, pp. 321-334, 2007.