Identity-Based Encryption Using Multi-Authority in Cloud Computing

Yadamakanti Vinay Kumar[1], M.Omprakash[2]
[1]*M.Tech, Computer Science &Engineering*
[2]*Associate Professor & HOD, Department of CSE*
JJ Institute of Information Technology

Abstract- **Identity-Based Encryption (IBE) which makes simple to the public key and credential management at Public Key Infrastructure (PKI) is a significant option to public key encryption. The computation capacity of resource-confined devices with that of computer systems can not be in comparison when a betteruseful resource disturbing functions is to be carried out. Withfine to computer computers, mobile devices for instance,are less powerful in computations like video streaming,teleconferencing and even decrypting data. In this paper we are proposedusually three concepts i.e. Multi authority of users,key generation, encryption and decryption of cloudstorage data. By way of enforcing multi authority ofclients in cloud method we are using identification baseddigital signature schema. An extra concept fornew release of key utilizing random code key generationsystem.In this paper data encryption anddecryption method we're utilizing multiplied tinyencryption algorithm. In this paper we're alsoenforcing mailing principles for sending secondlevel. By means of making use of second degree we can get first stage forthe intent of data encryption and decryption.**

Index Terms- **multi authority, key generation, security, cloud computing, signature**

I. INTRODUCTION

Identity based encryption system allow any user to generate a public key from a known identity value such as anASCII string. There is trusted third party, called the Private Key Generator (PKG), who generates the correspondingprivate keys. For encryption and decryption operations, PKG first publishes a master public key, and then generate thecorresponding master private key (referred as master key). Using this master public key, any user can generate a publickey corresponding to the identity by combining the master public key with the identity value. To get a correspondingprivate key, authorized user can use identity ID contacts PKG, which uses the master private key to generate privatekey for identity ID. As a result, user can encrypt messages with no prior distribution of keys between participants. Thisis very useful in cases where predistribution of keys is inconvenient because of technical restraints. However, fordecryption of message, the authorized user must obtain an appropriate private key from PKG. In this approach theproblem is that PKG must be highly trusted, as it has ability to generate any users private key and decryption ofmessage without authorization. Because any user's private key can be generated using third party's secret, this systemhas inherent key assurance.

A different systems have been proposed which remove this including certificate-based encryption and secure keyissuing cryptography. In PKI setting, revocation is done by appending validity periods to certificates or usingcombinations of techniques. But, this require management of certificates which is precisely the burden that IBE strivesto alleviate. Boneh and Franklin suggested that their private keys can renewed by user periodically and senders usereceivers identity with current time period.But this mechanism would results in an overhead at PKG. In another word,all the users even though their keys have been revoked or not, have to contact with private key generator(PKG)periodically to prove their identities and update new private keys. It is needed that PKG must be online and the securechannel has to be maintained for all the transactions, which will become a bottleneck for IBE system as the number ofgstage users grows. Many businesses large and small use cloud computing today either directly or indirectly instead oftraditional onsite alternatives.

There are a number of reasons like Reduction of costs,Universal access and many more because of which cloudcomputing is so widely used among businesses today. Thus it require a new working paradigm for introducing cloudservices into IBE revocation to fix the issue of efficiency and storage overhead. A naive approach is hand over theprivate key generators (PKG) master key to the Cloud Service Providers (CSPs). The CSPs then simply update allprivate keys by using the traditional key update technique and transfer the private keys to unrevoked users. However,this approach is based on an unrealistic assumption that CSPs are fully trusted and are allowed to access the master keyfor IBE system. But, in practice the public clouds are likely outside of the same trusted domain of users and are curiousabout users individual privacy. For this reason, a challenge is how to design a secure revocable IBE scheme so that wecan reduce the overhead computation at PKG with an untrusted CSP is raised.

In this paper, we design an efficient multi-authority identity based signature schema without using a global authority and propose a multi-authority access control scheme for cloud storage systems. With no global authority, existing techniques for key randomization in multi-authority schemes are no longer applicable, because there is no such a global authority to tie all the pieces together. In our method, we introduce a certificate authority to assign a global user identifier to each user as in [4] and an authority identifier to each authority. The user identifier can uniquely identify a user in the system and it is used together with the secret keys issued by different authorities for data decryption, such that it is impossible for two users to collude together to gain illegal access of data. We also propose a new technique to solve the attribute revocation problem in multi-authority systems. To improve the efficiency of attribute revocation, we move the work of re-encrypting the cipher text to the server by using proxy encryption method, such that there is no need for the server to decrypt the cipher text before re-encryption (i.e., the server cannot get the content key). The main contributions of this work can be summarized as follows.

1. We design an access control framework for multiauthority systems and propose an efficient and secure multi-authority access control scheme for cloud storage.

2) We design an efficient multi-authority identity based signature schema that does not require a global authority and can support any LSSS access structure.

3) We propose an efficient attribute revocation method for multi-authority while still keeping the system secure against the collusion attack.

II. RELATED WORKS

The accessibility of speedy and responsible Digital Identitiesis a key element for the fruitful execution of the finalpopulace key base of the web. All computerizedidentity plans ought to comprise a system for denyinganyone's advanced character for the problem that thischaracter is stolen (or wiped out) before its termination date(just like the cancelation of a master playing cards for the obstacle thatthey are stolen). In 1995, S. Micali proposed a rich approachfor personality denial which requires close to nocorrespondence in the middle of clients and varies within theframework.

In this paper, we develop his plan by means of loweringthe overall CA to directory correspondence, at the same time as yetpreserving up the identical minor customer to vendor correspondence.We differentiate our plan to different recommendations additionally. In this paper the creator demonstrated that endorse atotally useful character based encryption plan(IBE). The plan has picked cipher text protection in thearbitrary prophet mannequin accepting a variation of thecomputational Diffie-Hellman quandary. Our frameworkdepends on bilinear maps between gatherings. The Weilblending on elliptic bends is an illustration of this sort of guide.We supply designated definitions for secure character establishedencryption plans and provides just a few functions for suchframeworks.

In this paper [3] the author studied that the a further type ofidentification-based Encryption (IBE) plan that we name Fuzzypersonality established Encryption. In Fuzzy IBE we see a way oflife as set of illustrative traits. A Fluffy IBE plan takesinto consideration a personal key for a character, !, to unscramblea cipher text scrambled with a character, !0, if and just ifthe characters ! What‟s more, 0 are near one an extra asmeasured via the "set duvet" separation metric. A Fuzzy IBEplan can also be linked to empower encryption making use ofbiometric inputs as personalities; the blunder resistanceproperty of a Fuzzy IBE plan is correctly what takes intoaccount the utilization of biometric personalities, whichinalienably will have some commotion every time they areinspected. Moreover, we demonstrate that Fuzzy-IBE can beutilized for a sort of application that we term "quality basedencryption".

III. SYSTEM AND METHODOLOGY

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to the data access control. Because the cloud server may give data access to the users who do not have the access permission for profit gain, the data owners can no longer trust the cloud servers and rely on them to do data access control. Before retrieve data from cloud storage system each user will identify the given users are authenticated users or not. After performing authentication process the cloud service will generate key for encryption and decryption process stored data. If any user want to retrieve data from the cloud they are verify the status and also retrieve key from the data base. After retrieving key we can decrypt the data and get original plain format data. The implementation procedure of proposed system is as follows.

Identity based digital signature schema: In this module each user will registered into cloud storage system. After completion ofregistration each user will get username, password and also the verification code. The cloud service will send verification for individual users and using that code the users will generate signature. The users will send the signature to cloud service and get authentication status. The cloud service will generate signature for each user and compare both signatures. If the signatures are equal the cloud service will send authentication status to individual users. The cloud service will send verification code to users using mail.

Key Generation and File Encryption:
In the process of file encryption, the code A is randomly generated, and the string in request stream is encoded with code A to generate the first level encryption key. Subsequently, the data owner would use the first level encryption key to encrypt files using the extended tiny encryption algorithm. Finally, a new file is generated based on the original file and the first level encryption key. The new file is stored in the cloud storage system. This is the first level encryption. In the second level, the random code B is generated, and the first level encryption key are encoded with code B to generate the second level encryption key. The code B is stored in the database, and the new file of second level encryption key is generated and sent to the user by using the mail which is developed by using the smtp protocol. In case of losing the second level encryption key, the system generates the third level encryption key based on the second level encryption key and a protection code which is randomly generated by the system.

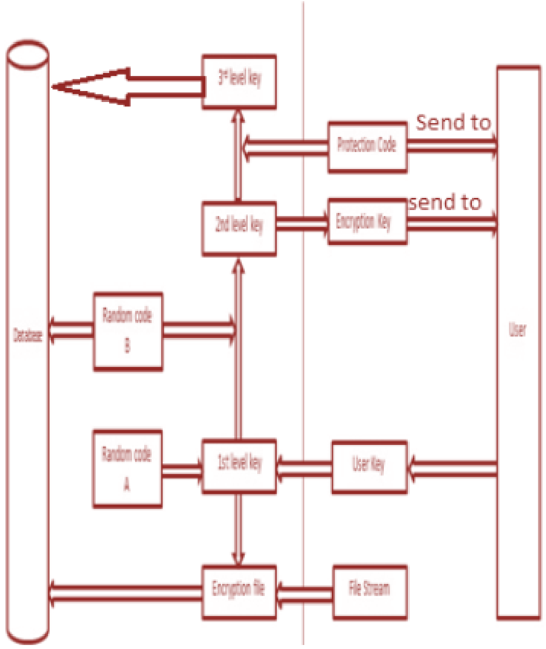

Fig.1 Model for system

The third level encryption key is stored in the database. In conclusion, the random code B and the third level key are stored in the database, and the encrypted file is stored in the cloud storage system. The user needs to save the second level encryption key, and remember the protection code. Other files or keys used in the processes need not be saved. The cloud service would send user a common encryption key (the common encryption key is also the second level encryption key, which is sent to the user). To upload a file, the data owner needs to upload file to be encrypted and stored into cloud service. The user would decrypt the general encryption key to the first level encryption key using the database stored random code B.

The pseudo code for encryption process is asfollows.

```
void encipher(unsigned int num_rounds, uint32_t
v[2], uint32_t const key[4])
{
unsigned int i;
uint32_t v0=v[0], v1=v[1], sum=0,
delta=0x9E3779B9;
for (i=0; i < num_rounds; i++)
{
v0 += (((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum +
key[sum & 3]);
sum += delta;
v1 += (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum +
key[(sum>>11) & 3]);
}
v[0]=v0; v[1]=v1;
}
```

File decryption process:

If the user wants to download the files, thesecond level encryption key must be provided. Usingthe second level encryption key and the databasestored random code B, the system can decrypt thefirst level encryption key and decrypt the files, thensend the files in the form of stream to the client. Thedecrypted files would be generated in the client side.

The decryption process of extended tiny encryption algorithm is as follows.

```
void decipher(unsigned intnum_rounds, uint32_t
v[2], uint32_t constkey[4])
{
unsigned int i;
uint32_t v0=v[0], v1=v[1], delta=0x9E3779B9,
sum=delta*num_rounds;
for (i=0; i <num_rounds; i++)
{
v1 -= (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum +
key[(sum>>11) & 3]);
sum -= delta;
v0 -= (((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum +
key[sum & 3]);
}
v[0]=v0; v[1]=v1;
}
```

After encrypt the file each user will get original file with a secure manner. By implementing those concepts we can provide authentication of each user in cloud and also provide more efficient data access control policy. Because in this paper we are using mailing concepts for sending second level key and also send verification code of individual users or clients

IV. CONCLUSION

In this paper, we defined a brand new access control framework for multi-authority approaches in cloudstorage and proposed an effective and secure multiauthority access control scheme. We first designedan efficient multi-authority scheme that doesn'trequire a global authority and can help any lessaccess constitution. Then, we proved that our multiauthority utilising identity based signature scheme isprovably at ease within the random oracle model. We are able toalso endorse other ideas for iteration of sharedkey for encryption and decryption file. After encryptthe file we will saved into cloud storage approach. Inthis paper the generation of encryption key can also beaccomplished by cloud provider and send that key to dataowner. Earlier than sending key to data proprietor the cloudprovider additionally send second degree key to all clients incloud. By way of using the second level key each and every user willget first degree encryption key. Utilising that key each and everyuser will participate in the decryption method and getlong-established plain structure data. In this we're utilizing accelerated tiny encryption algorithm for encryptionand decryption cloud stored data.

REFERENCES

[1]. P. Mell and T. Grance, “The NIST definition ofcloud computing,” National Institute of Standardsand Technology, Tech. Rep., 2009.

[2]. M. Chase, "Multi-authority attribute basedencryption," Theory of Cryptography, vol. 4392, pp.515–534, 2007.

[3] M. Chase and S. Chow, "Improving privacy andsecurity in multiauthority attribute-basedencryption," in Proceedings of the 16th ACMconference on Computer and communicationssecurity. ACM, 2009, pp. 121–130.

[4] A. Lewko and B. Waters, "Decentralizingattribute-based encryption," Advances inCryptology–EUROCRYPT 2011, pp. 568–588, 2011.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attributebased data sharing with attribute revocation," inProceedings of the 5th ACM Symposium onInformation, Computer and CommunicationsSecurity. ACM, 2010, pp. 261–270.

[6] J. Hur and D. Noh, "Attribute-based accesscontrol with efficient revocation in data outsourcingsystems," IEEE Transactions on Parallel andDistributed Systems, 2010.

[7] S. Jahid, P. Mittal, and N. Borisov, "Easier:encryption-based access control in social networkswith efficient revocation," in Proceedings of the 6thACM Symposium on Information, Computer andCommunications Security. ACM, 2011, pp. 411–415.

[8]. M. Kallahalla, E. Riedel, R. Swaminathan, Q.Wang, and K. Fu, "Plutus: Scalable secure filesharing on untrusted storage," in Proceedings of the2nd USENIX Conference on File and StorageTechnologies. Berkeley, CA, USA: USENIXAssociation, 2003, pp. 29–42.

[9]. D. Naor, M. Naor, and J. Lotspiech,"Revocation and tracing schemes for statelessreceivers," in Advances in Cryptology–CRYPTO2001. Springer, 2001, pp. 41–62.

[10] D. Li, X. Du, X. Hu, L. Ruan, and X. Jia,"Minimizing number of wavelengths in multicastorg/.

BIODATA

YADAMAKANTI VINAY KUMAR pursing M.Tech in Computer Science Engineering from **JJ INSTITUTE OF INFORMATION TECHNOLOGY**

M.OMPRAKASH working as Associate Professor & HOD, Department of CSE in **JJ INSTITUTE OF INFORMATION TECHNOLOGY**