EFFICIENT DATA TRACKING FOR SECURE CLOUD STORAGE

Dr.P.ChittiBabu[1], C.SivaKrishnaiah[2] , K.Supraja[3]

1Professor & Principal , APGCCS , Rajampet, Kadapa

2Assistance Professor, MCA Department ,APGCCS , Rajampet , Kadapa

3Student, MCA Department , APGCCS , Rajampet , Kadapa

[1]drpcbit@gmail.com
[2]sivacmca@gmail.com
[3]suprajakaperlamca9@gmail.com

***Abstract*— Cloud computing provides convenient, on-demand services from a shared pool of configurable computing resources. So many of them prefer to use cloud computing services such as data storage, customized applications etc., it offers economical and technical advantages. And also it has unpredictable security and privacy concerns particularly for data storage in public cloud infrastructure. So encrypted remote data access is necessary to guarantee the data privacy and usability. To enable authorized data usage, efficient access control is necessary in cloud environment with multi-user system capability. However the authorized user may intentionally or unintentionally become a victim for leak the secret key. In such condition, tracing and revoking leak of secret key needs to be solved first. For this purpose this work proposes an attribute based multiple keywords subset search system with encryption decryption mechanism. The proposed mechanism could effectively prevent the Key Generation Centre from unauthorized searching and decrypting all encrypted files of users. The decryption process uses energy aware computation for energy constrained nodes. The efficient user revocation is feasible after locating the malicious user. The malicious users can be find out and they're blocked only authorized users may be allowed to go looking the files.**

***Keywords*— Cloud computing, Cloud data storage, Data tracking, Key generation, Attribute based search.**

I. INTRODUCTION

With the new technology, cloud computing becomes the most important one, which provides convenient, on-demand services from a shared pool of configurable computing resources. So many of them prefer to use cloud computing services such as data storage, customized applications etc., it offers economical and technical advantages. But on the other side it has unpredictable security and privacy concerns particularly for data storage in public cloud infrastructure. So encrypted remote data access is necessary to guarantee the data privacy and usability. Encryption is primary method to protect data privacy in remote storage. To enable authorized data usage, efficient access control is necessary in cloud environment with multi-user system capability. However the authorized user may intentionally or unintentionally become a victim for leak the secret key. In such condition, tracing and revoking the abused secret key needs to be solved immediately. For this purpose this work proposes an attribute based multiple keywords subset search system with encryption decryption mechanism. Searchable encryption mechanism provides to enable keyword search over encrypted data.

II. RELATED WORK

For the file sharing system, there are multiple-owners and multiple users exist, fine-grained search authorization is a desirable function for the data owners to share their private data with other authorized user. However, the available systems, requires the user to perform a large amount of complex bilinear pairing operations. These issues come to be a heavy burden for user's terminal, which is in particular severe for energy constrained devices. The decryption system permits user to recover the message with light-weight decryption. However, the cloud server might return wrong half-encrypted information as a result of malicious attack or system malfunction. Thus, it is an important issue to guarantee.

The proposed mechanism could effectively prevent the Key Generation Centre from unauthorized searching and decrypting all encrypted files of users. The decryption process uses energy aware computation which is desirable for energy constrained nodes. The efficient user revocation is enabled after the identification of malicious user. The proposed system is attribute based system and uses multiple keyword subsets to realize the desired outcome.

Searchable encryption permits key-word seek over encrypted data. The concept of public key encryption with keyword search is important for protecting the privacy of outsourced data. Data owners in Public Key Encryption schemes store their files in encrypted form in the remote untrusted data server. The data users query to search on the encrypted files by generating a keyword trap door, and the data server executes the search operation. In 2016, Chen ET AL. introduced the concept of “dual server” into Public Key Encryption to resist off-line keyword guessing attack. Attribute Based Encryption is an important method to realize fine-grained data sharing. In ABE schemes, descriptive attributes.

III. PROPOSED ALGORITHMS

In this we can use the Fully Homomorphic Encryption Algorithm.

The fully homomorphic encryption (FHE) scheme consist of the following algorithms.

(1) Key generation. Taken a security parameter κ as input, the algorithm outputs a public and secret key pair (pk1, sk1).

(2) Encryption. Taken a message ms and the public key pk as input, the algorithm outputs a cipher text ct = HEncpk(ms).

(3) Decryption. Taken a ciphertext c and the secret key sk1 as input, the algorithm outputs a message ms = HDecsk(ct).

(4) Homomorphic addition. Taken two cipher texts ct1 = HEncpk(m1) and ct2 = HEncpk(m2) as inputs, the algorithm outputs a cipher text ct = ct1 $\oplus$ct2 such that HDecsk(ct) = m1 + m2, where $\oplus$is the homomorphic addition.

(5) Homomorphic multiplication. Taken two cipher texts ct1 = HEncpk(m1) and ct2 = HEncpk(m2) as inputs, the algorithm

outputs a ciphertext c = ct1 $\otimes$ ct2 such that HDecsk(ct) = m1 $\cdot$ m2, where $\otimes$ is the homomorphic multiplication.

Algorithm 1 Key generation
Step 1: n = pk1sk1, the RSA modulus
Step 2: λ = lcm (pk1 − 1, sk1 − 1)
Step 3: g ϵ Z /n2 Z s.t. n|or dn2(g)
Step 4: Public-key: (n, g), secret key: u, μ

Algorithm 2 Encryption of ms
Step 1: ms ϵ {0, 1... n − 1}, a message
Step 2: h ϵR Z/n Z
Step 3: ct = gm hn mod n2, a cipher text

Algorithm 3 Decryption of ct
ms = L (cu mod n2) L(g u mod n2) − 1 mod n
The constant parameter,
L (gu mod n2)-1 mod n or L (g α mod n2)-1 mod n
where g=1+ n mod n2 can also be recomputed once for all.

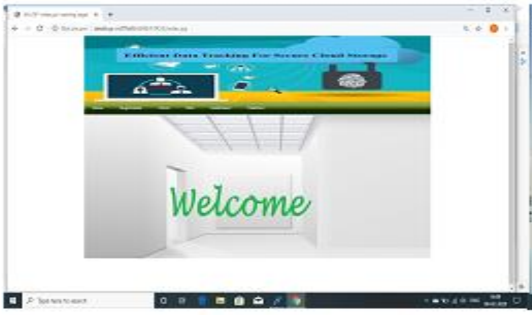
IV. COMPARITIVE RESULTS

Fig. 1: Represents the home page and displays welcome message to the screen, it contains the buttons like, Registration, Cloud, KGC, Data user, and Data owner. Those are used to login into the corresponding home pages. To login it requires the ID and Password.

Fig. 2: Represents the Registration page. It can be used for registering the new Data users and Data owners. For registration it requires to fill the details of new entry. This can be used to avoid the unauthorized users.

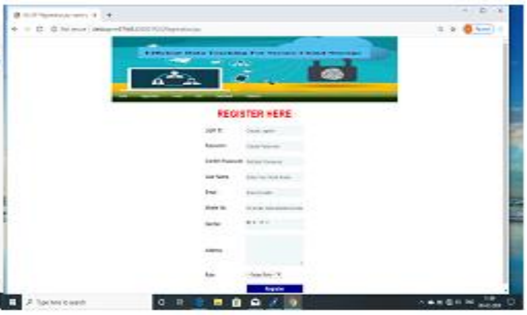
Fig. 3: Represents the Upload files page. In this all the files can be uploaded, in this page Data owners can upload the files. The files which are uploaded by the Data owners can be viewed by Cloud and KGC.

Fig. 4: Represents the view all uploaded files page. This can be used for viewing the all uploaded files, those are uploaded by the Data owner. These can be viewed by the Data owner, KGC, and Cloud.


Efficient Data Tracking For Secure Cloud Storage

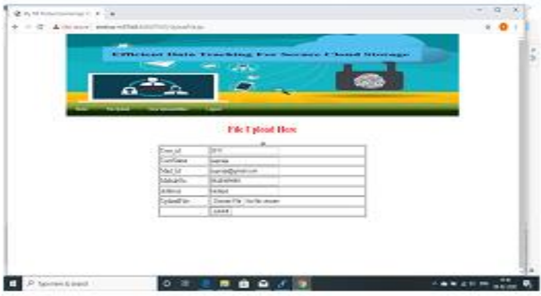
Welcome

Fig. 1 Home Page


Efficient Data Tracking For Secure Cloud Storage

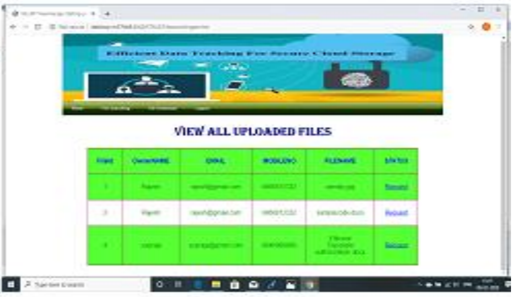
REGISTER HERE

Fig. 2 Registration Page


Efficient Data Tracking For Secure Cloud Storage

File Upload Here

Fig. 3 Upload Files


Efficient Data Tracking For Secure Cloud Storage

VIEW ALL UPLOADED FILES

[illegible]	OwnerNAME	EMAIL	MOBILENO	FILENAME	STATUS
1	[illegible]	[illegible]	[illegible]	[illegible]	Request
2	[illegible]	[illegible]	[illegible]	[illegible]	Request
3	[illegible]	[illegible]	[illegible]	[illegible]	Request

Fig. 4 View All Uploaded Files

V. CONCLUSION

The enforcement of access manipulate and the guide of key-word search are important troubles in at ease cloud storage gadget. In this, I described a brand new paradigm of searchable encryption gadget, and proposed a concrete creation. It helps flexible a couple of keywords subset search, and solves the key escrow hassle at some point of the key generation procedure. Malicious user who sells mystery key for gain may be traced. The decryption operation is in part outsourced to cloud server and the correctness of half of-decrypted result may be demonstrated by way of records consumer.

REFERENCES

[1] Li, K. Ren, W. Lou. "Secure ranked keyword search over encrypted cloud data"[C]//IEEE 30thInternational Conference on Distributed Computing Systems (ICDCS), IEEE, 2010: 253-262.

[2] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server Public Key Encryption with Keyword Search for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 789-798.

[3] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in NDSS, 2004.

[4] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language". IEEE Transactions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.

[5] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine grained Owner-enforced Search Authorization in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

[6] K.Liang, W. Susilo, "Searchable Attribute-Based Mechanism Efficient Data Sharing for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, 2015, vol.10,no.9,pp.19811992.

[7] M.Green, S.Hohenberger, and B.Waters, "Out sourcing the decryption of ABE cipher texts," in USENIX Security Symposium, ACM, 2011, pp. 34-34.

[8] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 13431354.

[9] B.Qin, R.H.Deng, S.Liu, and S.Ma, "Attribute Based Encryption with Efficient Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1384-1394.

[10] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in: EUROCRYPT, 2004, pp. 506-522.

[11] Z. Liu, Z. Cao, D.S. Wong, “White-box traceable cipher text-policy attribute-based encryption supporting any monotone access structures,” IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 1, pp. 76-88.

[12] Z. Liu, Z. Cao, D.S. Wong, “Traceable CP-ABE: how to trace decryption devices found in the wild,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.

[13] B. Zhang, F. Zhang, “An efficient public key encryption with conjunctive-subset key words search,” Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 262-267.

[14] L. Fang, W. Susilo, C. Ge, J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Information Sciences, 2013, vol. 238, 221-241

[15] S. Hohenberger, B. Waters, “Attribute-based encryption with fast decryption,” in: PKC, springer, 2013, vol. 7778, pp. 162-179.