ANONYMOUS KEY BASED SECURE FILE ENCRYPTION IN CLOUD

S.Rajesh kumar[1], Sanjith Mohan [2], G.Raja Durai[3], K.J Dilip Raj [4]

[1]Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of technology, Chennai.
[2,3,4.] UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai

---

Abstract-*Cloud storage is associate degree application of cloud that liberates organizations from establishing in-house knowledge storage systems. However, cloud storage provides rise to security considerations. Just in case of group-shared knowledge, the info faced are cloud specific and traditional business executive threats. Secure knowledge sharing among a gaggle that counters business executive threats of legitimate nevertheless malicious users is a vital analysis issue. We have a tendency to propose a replacement system within which the information are shared to the individual user a lot of firmly through secret writing. The one info is maintained for the individual user for a lot of security. We have a tendency to produce a neighborhood server during this system that contains user key for secret writing purpose. The documents to be shared are kept as an encrypted format and keep within the cloud info. We have a tendency to produce native server for maintaining the users key a lot of firmly. Therefore, we have a tendency to stopping the key to be shared globally.*

Keywords used: Anonymous keys, Cloud computing, triple DES

1.INTRODUCTION

Governments and corporations today treat data sharing as a vital tool for enhanced productivity. Cloud computing has revolutionized education, healthcare and social networking. Perhaps the most exciting use case for cloud computing is its ability to allow multiple users across the globe share and exchange data, while saving the pangs of manual data exchanges, and avoiding the creation of redundant or out-of-date documents. Social networking sites have used the cloud to create a more connected world where people can share a variety of data including text and multimedia. Collaborative tools commonly supported by cloud platforms and are extremely popular since they lead to improved productivity and synchronization of effort. The impact of cloud computing has also pervaded the sphere of healthcare, with smartphone applications that allow remote monitoring and even diagnosis of patients. In short, cloud computing is changing various aspects of our lives in unprecedented ways.

Despite all its advantages, the cloud is susceptible to privacy and security attacks, that are a major hindrance to its wholesome acceptance as the primary means of data sharing in today's world. According to [2], Cloud users regarded security as the top challenge with 75% of surveyed users worried about their critical business and IT systems being vulnerable to attack. While security threats from external agents are widespread, malicious service providers must also be taken into consideration. Since online data almost always resides in shared environments (for instance, multiple virtual machines running on the same physical device), ensuring security and privacy on the cloud is a non trivial task. When talking about security and privacy of data in the cloud, it is important to lay down the requirements that a data sharing service must provide in order to be considered secure.

The most common primary requirements in a cloud based data sharing service are:

- *Data Confidentiality*: Unauthorized users (including the cloud service provider), should not be able to access the data at any given time. Data should remain confidential in transit, at rest and on backup media.
- *User revocation*: The data owner must be able to revoke any user's access rights to data the without affecting other authorized users in the group.
- *Scalability and Efficiency*: Perhaps the biggest challenge faced by data management on the cloud is maintaining scalability and efficiency in the face of immensely large user bases and dynamically changing data usage patterns.
- *Collusion between entities*: Any data sharing service in the cloud must ensure that even when certain malicious entities collude, they should still not be able to access any of the data in an unauthorized fashion.

A traditional way of ensuring data privacy is to depend on the server to enforce access control mechanisms [3]. This methodology is prone to privilege escalation attacks in shared data environments such as the cloud, where data corresponding to multiple users could reside on the same server. Current technology for secure online data sharing comes in two major flavors - trusting a third party auditor [4], or using the user's own key to encrypt her data while preserving anonymity [5]. In either case, a user would want a reliable and efficient cryptographic scheme in place, with formal guarantees of security, high scalability and ease of use. The main challenge in designing such a cryptosystem lies in effective sharing of encrypted data. A data sharing scheme on the cloud is only successful if data owners can delegate the access rights to their data efficiently to multiple users, who can then access the data directly from the cloud servers. Assume that a data owner A is using an online data sharing service such as Microsoft OneDrive [6] to store certain classes of data (here *class* may refer to any data structure such as a file, folder or any collection of these). A wishes to add an additional layer of security for her data by storing them in an encrypted fashion. Now, A intends to share a specific subset S of these documents with a set $\hat{S}$ of data users. For that, A needs to provide each of these users with decryption rights to specific classes of the data that they are authorized to access. The challenge therefore is to design a secure and efficient online *partial* data sharing scheme that allows Alice to perform this task in an efficient and secure manner.

A naive (and extremely inefficient) solution is to have a¨ different decryption key for each message class, and share them accordingly with the designated users via secured channels. This scheme is not practically deployable for two major reasons. Firstly, the number of secret keys would grow with the number of data classes. Secondly, any user revocation event would require Alice to entirely re-encrypt the corresponding subset of data, and distribute the new set of keys to the other existing valid users. This makes the scheme inefficient and difficult to scale. Since the decryption key in public key cryptosystems is usually sent via a secure channel, smaller key sizes are desirable. Moreover, resource constrained devices such as wireless sensor nodes and smart phones cannot afford large expensive storage for the decryption keys either. An ideal scenario of A can construct a single constant size decryption key K_S that combines the decryption rights to each of the data classes in S, and then use a public key framework to broadcast this key to the target set of users $\hat{S}$ in the form of a low overhead broadcast aggregate key $K_{(S,\hat{S})}$. This scheme is efficient, avoids the use of secret channels which are costly and difficult to realize in practice, and is scalable to any arbitrary number of data classes and data users.

In the proposed system which addresses the limitation of the data sharing in social media. We improve the security by restricting the user to share the data in the group. We create separate databases for the individual user for improving the security. We introduce local server for maintaining the user keys. The user keys are responsible for the decryption of the file. The keys are created whenever the new user creates an account in the social media. We use cloud database for storing the file in the encrypted format so that no one can access the document without the key. The user can share the document to another member by providing the key through the local server .We introduce another temporary server that is responsible to decrypt shared user file and re-encrypt to respected user using that user key. Temp Server which is interconnected with the local server. In this paper, we attempt to build precisely such a data sharing framework that is provably secure and at the same time, efficiently implementable.

2. RELATED WORKS

Khan.S.U worked on Cloud computing which is emerging as a new computing paradigm in the healthcare sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Nonetheless, storing the patient health data in the third-party servers also entails serious threats to data privacy. Because of probable disclosure of medical records stored and exchanged in the cloud, the patients' privacy concerns should essentially be considered when designing the security and privacy mechanisms. Various approaches have been used to preserve the privacy of the health information in the cloud environment. This survey aims to encompass the state-of-the-art privacy-preserving approaches employed in the e-Health clouds. Moreover, the privacy-preserving approaches are classified into cryptographic and noncryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted

Xiaoli Li, Lizhe Wang and Khan.S.U experimented on the Analysis of neural data with multiple modes and high density has recently become a trend with the advances in neuroscience research and practices. There exists a pressing need for an approach to accurately and uniquely capture the features without loss or destruction of the interactions amongst the modes (typically) of space, time, and frequency. Moreover, the approach must be able to quickly analyze the neural data of exponentially growing scales and sizes, in tens or even hundreds of channels, so that timely conclusions and decisions may be made. A salient approach to multi-way data analysis is the parallel factor analysis (PARAFAC) that manifests its effectiveness in the decomposition of the electroencephalography (EEG). However, the conventional PARAFAC is only suited for offline data analysis due to the high complexity, which computes to be O(n2) with the increasing data size. In this study, a large-scale PARAFAC method has been developed, which is supported by general-purpose computing on the graphics processing unit (GPGPU). Comparing to the PARAFAC running on conventional CPU-based platform, the new approach dramatically excels by >360 times in run-time performance, and effectively scales by >400 times in all dimensions. Moreover, the proposed approach forms the basis of a model for the analysis of electrocochleography (ECoG) recordings obtained from epilepsy patients, which proves to be effective in the epilepsy state detection. The time evolutions of the proposed model are well correlated with the clinical observations. Moreover, the frequency signature is stable and high in the ictal phase. Furthermore, the spatial signature explicitly identifies the propagation of neural activities among various brain regions. The model supports real-time analysis of ECoG in > 1;000 channels on an inexpensive and available cyber-infrastructure.

Seung Hyun Seo, Mohamed Nabeel, Xiaoyu Ding and Elisa Bertino found that a mediated certificateless encryption (mCL-PKE) scheme solves the key escrow problem and certificate revocation problem. However, existing mCL-PKE schemes are either inefficient because of the expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. In this system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The users subsequently fully decrypt the partially decrypted data using their private keys. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information. The proposed system is an extension to the above approach to improve the efficiency of encryption at the data owner. The implementation of mCL-PKE scheme and the overall cloud based system, and evaluate its security and performance. The results show that the proposed system schemes are efficient and practical

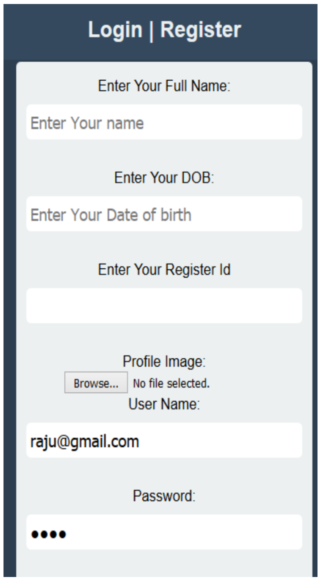
Yi-Ruei Chen and Wen-Guey Tzeng worked on the group key management is for a group manager to maintain a consistent group key for a dynamic group of members through a broadcast channel. It proposed a group key management scheme based on a meta proxy re-encryption (PRE) scheme. In particular, we propose an RSA-based PRE scheme with special properties. It is the first RSA-based PRE scheme for group key management and has the desired properties of uni-directionality and multi-hop. In our group key management scheme, each group member holds just one secret auxiliary key and logN public auxiliary keys. The size of rekey messages for each group key update remains O(logN). Additionally, our scheme has some distinct features. Firstly, the size of the key update history is a constant O(N) no matter how many times of group key updates occur. Secondly, the computation time of computing the newest group key from the key update history is always O(logN) no matter how many group key updates are missed. This feature provides a practical solution for group key update when members go offline from time to time. Finally, the proposed scheme is immune to the collusion attack of other members

3. PROPOSED SYSTEM

We propose a new system which addresses the limitation of the data sharing in social media. We improve the security by restricting the user to share the data in the group. We create separate databases for the individual user for improving the security. We introduce local server for maintaining the user keys. The user keys are responsible for the decryption of the file. The keys are created whenever the new user creates an account in the social media. We use cloud database for storing the file in the encrypted format so that no one can access the document without the key. The user can share the document to another member by providing the key through the local server .We introduce another temporary server that is responsible to decrypt shared user file and re-encrypt to respected user using that user key. Temp Server which is interconnected with the local server

3.1. User Interface

In this module ,First we Create and Establish Connection between client and server for user Actively inter face with server. Get All user Information from Registration page and encrypt that information finally stored in cloud database. Once registration process completed ,Server provide Unique username and password for every user, from this key securely maintain our profile and Sharing data’s



Login | Register

Enter Your Full Name:

Enter Your name

Enter Your DOB:

Enter Your Date of birth

Enter Your Register Id

Profile Image:

Browse... No file selected.

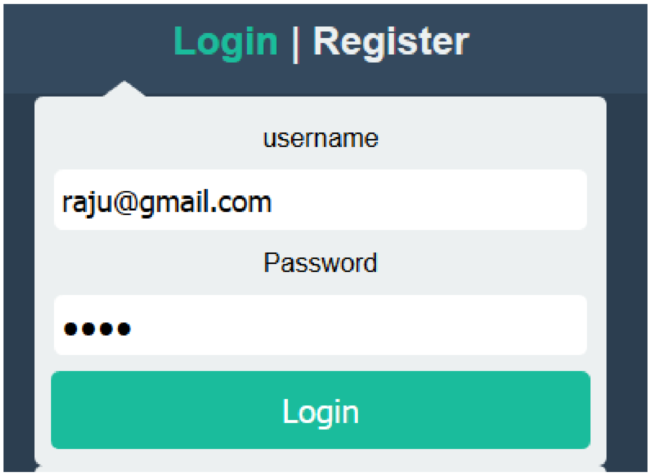
User Name:

raju@gmail.com

Password:

••••

Fig1-Register page



username: raju@gmail.com

Password: ●●●●

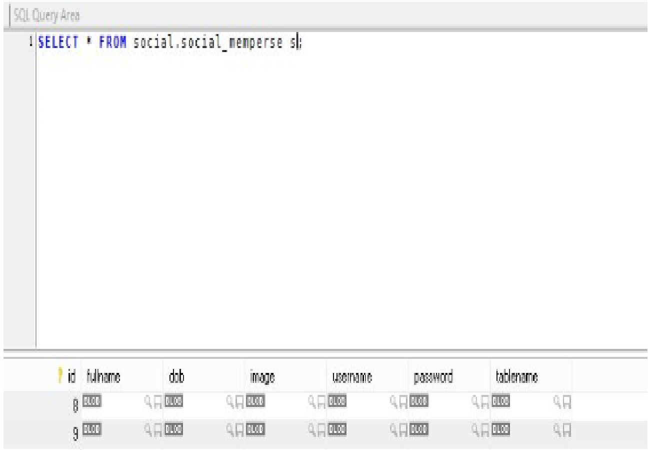
Fig2- Login Page

3.2 Upload data's

We design another user profile page for user upload our personal data's, once you upload a data the data must be encrypted using **triple DES** algorithm then stored in cloud database. Inn this project we maintain two servers. One for store all encryption data that is cloud server, maintained by cloud provider. Another one is data owner server maintained by local networks that contain encryption key for every user. So, Cloud provider not known encryption key information.

3.3 Key generation

In local server we are going to create a key which is not visible to anyone. The key is based on the Triple DES algorithm's generated key is been protected in the cloud server



```
SELECT * FROM social.social_memperse s;
```

id	fullname	dob	image	username	password	tablename
8	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB
9	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB

Fig3-Creation of table using sql

3.4 Securely Sharing Data's

In this module we explain secure data sharing information .

If user want to share our data to other user , first encrypted data read from cloud database ,then perform Under re-encryption by shared user encryption key, because data owner server maintain unique encryption key for each and every user.

Then that re-encrypted data Stored in cloud database server . From this way we can share and store our data securely.

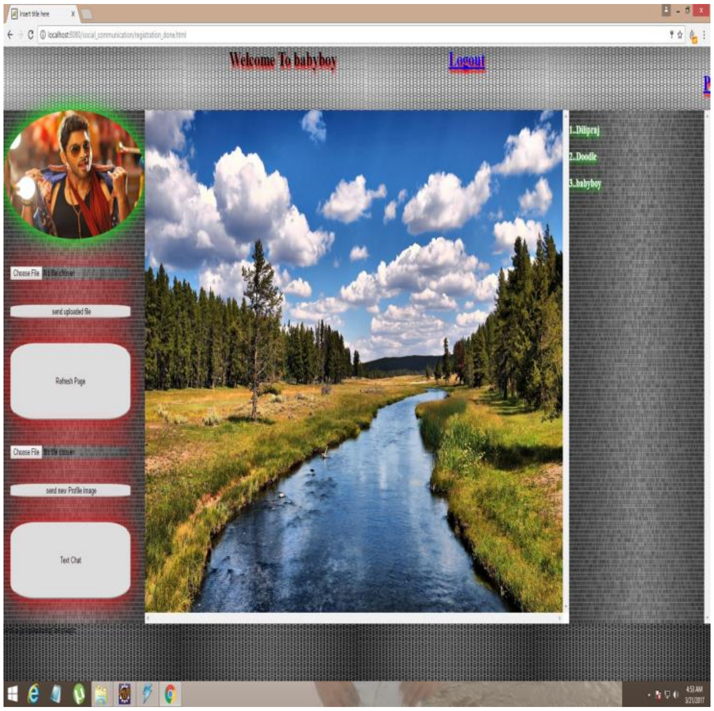


Fig4-Sharing of data

4.CONCLUSION AND FUTURE ENHANCEMENT

We separate network admin and cloud service provider, that means all security system (Encryption Keys) under controlled by admin, so we can prevent third party user can access.

- In future we enhance more security in cloud for example make two level encryption instead of single level encryption.
- Improve packet level security in network

REFERENCES

[1] Sikhar Patranabis, Yash Shrivastava and Debdeep Mukhopadhyay, "Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud", , IEEE Transactions on Computers, may 2016

[2] IDC Enterprise Panel. It cloud services user survey, pt. 3: What users want from cloud services providers, august 2008.

[3] Sherman SM Chow, Yi-Jun He, Lucas CK Hui, and Siu Ming Yiu. Spice–simple privacy-preserving identity-management for cloud environment. In Applied Cryptography and Network Security, pages 526–543. Springer, 2012.

[4] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for secure cloud storage. Cryptology ePrint Archive, Report 2009/579, 2009.

[5] Sherman SM Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou, and Robert H Deng. Dynamic secure cloud storage with provenance. In Cryptography and Security: From Theory to Applica- tions, pages 442–464. Springer, 2012.

[6] Erik C Shallman. Up in the air: Clarifying cloud storage protec- tions. Intell. Prop. L. Bull., 19:49, 2014.

[7] Chitchanok Chuengsatiansup, Michael Naehrig, Pance Ribarski, and Peter Schwabe. Panda: Pairings and arithmetic. In Pairing- Based Cryptography - Pairing 2013 - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers, pages 229–250, 2013.

[8] EricZavattoni,LuisJ.DominguezPerez,ShigeoMitsunari,AnaH. S´anchez-Ram´ırez, Tadanori Teruya, and Francisco Rodr´ıguez- Henr´ıquez. Software implementation of an attribute-based en- cryption scheme. IEEE Trans. Computers, 64(5):1429–1441, 2015

[9] Michel Abdalla, C´eline Chevalier, and David Pointcheval. Smooth projective hashing for conditionally extractable commitments. In Advances in Cryptology-CRYPTO 2009, pages 671–689. Springer, 2009.

[10] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. Parallel and Dis- tributed Systems, IEEE Transactions on, 24(1):131–143, 2013.