Grenze International Journal of Engineering and Technology, Special issue

A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

K.Baskar[1] , Dr.G.K.D.Prasanna Venkatesan[2] , R.Jagatheswar[3] , S.Mohamed ashif[4] and S.Parthiban[5]
[1]Kongunadu College of Engineering and Technology, Trichy, Tamilnadu, India
Email: dishabaskar@gmail.com
[2]Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India
Email: prasphd@gmail.com
[3-5]Kongunadu College of Engineering and Technology, Trichy, Tamilnadu, India

***Abstract*—With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. Proposing the novel concept of key aggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme. A data owner only needs to distribute a single key to a user for sharing a large number of documents. The user only needs to submit a single trapdoor to the cloud for querying the shared documents. The experimental results show that this method can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.**

I. INTRODUCTION

With the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data. Nowadays, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also provide data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners. The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient. They cannot meet all the requirements of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted

Grenze ID: 01.GIJET.5.1.32

data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data. However, this approach requires fine-grained access control. In both cases, password management is a big issue. Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. However, the data encryption brings new problems. How to provide efficient access control mechanism on ciphertext decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owners effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data access control over ciphertext. In these researches, they have the following common assumptions. First, the CSP is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple ciphertext access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE). All these proposals are designed for non-mobile cloud environment. They consume large amount of storage and computation resources, which are not available for mobile devices. According to the experimental results in [26], the basic ABE operations take much longer time on mobile devices than laptop or desktop computers. It is at least 27 times longer to execute on a smart phone than a personal computer (PC). This means that an encryption operation which takes one minute on a PC will take about half an hour to finish on a mobile device. Furthermore, current solutions don't solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud. As the mobile cloud becomes more and more popular, providing an efficient secure data sharing mechanism in mobile cloud is in urgent need.

A. Existing System

With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. The data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud.However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications.Securely distributing to users a large number of keys for both encryption and search, and those users will have to securely store the received keys, and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data.

B. Proposed System

Propose a lightweight data sharing scheme for mobile cloud computing. Proposing the novel concept of key aggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme A data owner only needs to distribute a single key to a user for sharing a large number of documents.
The user only needs to submit a single trapdoor to the cloud for querying the shared documents. The experimental results show that this method can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

II. HELPFUL HINTS

A. Owner Module

This Module have the encryption algorithm, Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. In this module the data owner give request to TPA (Domain) and get the username and password from TPA through mail. Data owner login with that user name and password, finally data owner upload the text file with encryption algorithm and also generate secret key.

B. User Module

In this module the data user give request to TPA(Domain) and get the username and password from TPA through mail. Data user login with that user name and password, Data user request to data owner and get the

secret key from data owner, Finally data user to give the secret key and get the decrypt text file. If user enter wrong key for 3 times means account is blocked and send alert message to user.

C. Remote Data Upload

Every data has a unique index, the index is just a keyword that are assigned to the data. The keyword makes the cloud user to access the data very fast by entering the specific keyword to select the particular data.

D. Encode Interface

Exploiting data encryption before outsourcing is one way to mitigate this privacy concern, but it is only complementary to the privacy preserving public auditing scheme to be proposed. Without a properly designed auditing protocol, encryption itself cannot prevent data from"flowing away" towards external parties during the auditing process. Thus, it does not completely solve the problem of protecting data privacy but just reduces it to the key management. Unauthorized data leakage still remains a problem due to the potential exposure of decryption keys.

E. Access Privilege

The user can share their data. The shared data can be viewed only by the accessed user if properly get permission. The accessed user views the file only with the key that gets from the file owner. The key is generating using multiparty searchable encryption (MPSE) scheme. If honest user may leak all her search patterns even if she shares only one of her documents with another malicious user. Based on our analysis, we present a new security model for MPSE by considering the worst case and average-case scenarios, which capture different server-user collusion possibilities.

F. Browsing

Keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop two advanced techniques on constructing keyword sets, which achieve optimized storage and representation overheads. To search a keyword the user need a valid key.

III. DATA FLOW DIAGRAM

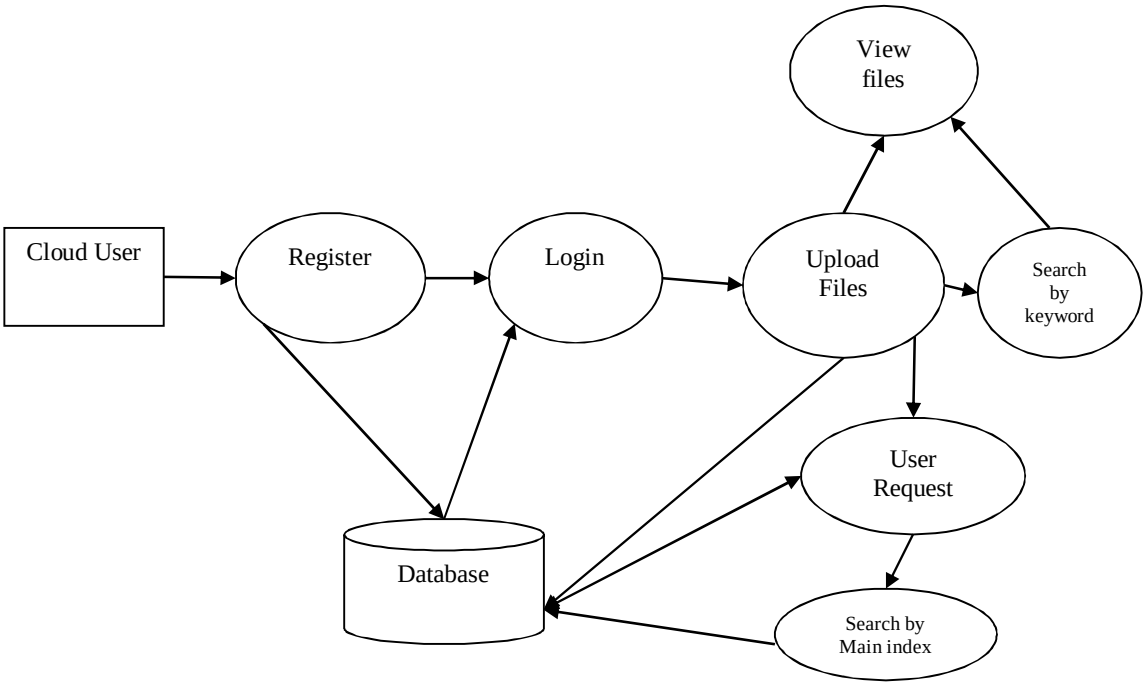

Fig 1. System Architecture

III. CONCLUSION

Cloud Computing is gaining popularity and advancement day-by-day. But still the security threat hinders the success of Cloud Computing. In this paper, some of the privacy threats are addressed and the techniques to overcome them are surveyed. While some approaches utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy. Also, approaches to preserve privacy at the time of public auditing are also discussed. Thus, to conclude it is necessary that every cloud user must be guaranteed that his data is stored, processed, accessed and audited in a secured manner at any time. Data freshness is essential to protect against misconfiguration errors or rollbacks caused intentionally. We can develop an authenticated file system that supports the migration of an enterprise-class distributed file system into the cloud efficiently, transparently and in a scalable manner. It's authenticated in the sense that enables an enterprise tenant to verify the freshness of retrieved data while performing the file system operations. The user must be given complete access control over the published data. Also, powerful security mechanisms must always supplement every cloud application. Attaining all these would end up in achieving the long dreamt vision of Cloud Computing in the nearest future. In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

FUTURE ENHANCEMENT

To avoid the single trapdoor, the multiple trapdoor has been generated for every user by MPSE schemes. MPSE can be regarded as a multi-party version of the symmetric searchable encryption. The data can be prevented by the unauthorized user. The concept of searchable encryption provides a promising direction in solving the privacy problem when outsourcing data to the cloud. Cloud systems [1, 2] can be used to enable data sharing capabilities and this can providean abundant of benefits to the user. There is currently a push for IT organizations to increase their data sharing efforts. According to a survey by InformationWeek [3], nearly all organisations shared their data somehow with 74 % sharing their data with customers and 64 % sharing with suppliers. A fourth of the surveyed organizations consider data sharing a top priority. The benefits organizations can gain from data sharing is higher productivity. With multiple users from different organizations contributing to data in the Cloud, the time and cost will be much less compared to having to manually exchange data and hence creating a clutter of redundant and possibly out-of-date documents. With social networking services such as Face book, the benefits of sharing data are numerous such as the ability to share photos, videos, information and events, creates a sense of enhanced enjoyment in one's life and can enrich the lives of some people as they are amazed at how many people are interested in their life and well-being. For students and group-related projects, there has been a major importance for group collaborative tools. Google Docs provides data sharing capabilities as groups of students or teams working on a project can share documents and can collaborate with each other effectively. This allows higher productivity compared to previous methods of continually sending updated versions of a document to members of the group via email attachments. Also in modern healthcare environments, healthcare providers are willing to store and share electronic medical records via the Cloud and hence remove the geographical dependence between healthcare provider and patient.

REFERENCES

[1] M. Abdalla, E. Bresson, O. Chevassut, and D. Pointcheval.Password-based group key exchange in a constant number ofrounds. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors,Public Key Cryptography — PKC 2006, volume 3958 of LNCS, pages427–442. Springer, 2006.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu.Order preservingencryption for numeric data.In Proceedings of the 2004 ACMSIGMOD international conference on Management of data, pages 563–574.ACM, 2004.

[3] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros.Practical group signatures without random oracles.http://eprint.iacr.org/2005/385, 2005.

[4] F. Bao, R. H. Deng, X. Ding, and Y. Yang.Private query onencrypted data in multi-user settings. In L. Chen, Y. Mu, andW. Susilo, editors, Proceedings of the 4th international conference onInformation security practice and experience, volume 4991 of LNCS,pages 71–85. Springer, 2008.

[5] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill.Orderpreservingsymmetric encryption. In A. Joux, editor, Advancesin Cryptology — EUROCRYPT 2009, volume 5479 of LNCS, pages 224–241.Springer, 2009.

[6] D. Padmini Bai and P. Preethi , “Security Enhancement of Health Information Exchange Based on Cloud Computing System”, International Journal of Scientific Engineering and Research, pp. 79-82, Volume 4 Issue 10, October 2016.
[7] S.Sangeetha P.Dhivya Bharathy, P.Preethi, K.Karthick, Hand Gesture Recognition for Physical Impairment Peoples, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), pp. 6-10, Volume 4 Issue 10, October 2017.
[8] Christo Paul.E Preethi.P, Baskaran.G, An Eyes-Free Model Implementation: Voice Based Optical Character Recognition for Mobile Devices, International Journal of Advanced Research in Computer Science & Technology, Volume 2, Issue 1, March 2014.
[9] Shyamambika, N. and Thillaiarasu, N., 2016. Attaining integrity, secured data sharing and removal of misbehaving client in the public cloud using an external agent and secure encryption technique. Advances in Natural and Applied Sciences, 10(9 SE), pp.421-432.
[10] Yogapriya, J., Ila.Vennila,2013, Feature Dimension Reduction For Efficient Medical Image Retrieval System Using Unified Framework, Journal of Computer Science, Vol.9, No.11, pp.1472-1486, ISSN No. 1549-3636.
[11] Dr.Raghavendran P.S., Dr.Asokan R., Vishnupriya M., Enhancing the security against Flooding Attack in MANET for Medical Application, Asian Journal of Research in Social Sciences and Humanities, Vol. 6, Issue 6, 2016.
[12] R.Pavithra, Dr.R.Asokan, K.Baskar,Improving Privacy And Dynamic Updation Using Ranked Search Over Outsourced Cloud Data, International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 10, Oct-2016.
[13] Saravanan, K; Asokan, R; Venkatachalam, K., Neuro- Fuzzy Based Clustering of Distributed Denial of Service (DDoS) Attack Detection Mechanism, International Information Institute (Tokyo). Information; Koganei Vol. 16, Iss. 11, (Nov 2013).
[14] Vellingiri, J.; Balambigai, S.; Saravanan, K.; Asokan, R., Secure Real Time Web Based Electrocardiogram Monitoring System for Improved Healthcare, Journal of Medical Imaging and Health Informatics, Volume 6, Number 3, June 2016, pp. 774-778(5).
[15] M. Bhuvaneshwari, Dr. J. Yogapriya, Decentralized, Energy-Efficient, Low Latency and Less Homogeneous Settings based Workload Management in Enterprise Clouds, International Journal of Scientific Engineering and Research (IJSER), Volume 4 Issue 10, October 2016.