Grenze International Journal of Engineering and Technology, Special issue

Scalable Multiparty Searchable Encryption Scheme for Searching and Encrypting Data in Cloud Environment

Arun Kumar S[1], Arun Pandi T[2], Murali C[3] and K.Karthick[4]
[1]Kongunadu College of Engineering and Technology/ CSE, Trichy, Tamilnadu, India
Email: click2jak@gmail.com [1]
[2-3] Kongunadu College of Engineering and Technology/ CSE, Trichy, Tamilnadu, India
Email: 816arun@gmail.com, muralianbu33@gmail.com
4 Kongunadu College of Engineering and Technology/ AP -CSE, Trichy, Tamilnadu, India
Email: radhamayil@gmail.com

***Abstract*—The existing symmetric searchable encryption plans go for permitting a client to outsource the original information to a cloud server and agent the last to inquiry on benefit. These plans don't qualify as an issue and adaptable answer for the multiparty setting, where clients outsource their encoded information to a cloud server and specifically approve each other to hack. Because of the likelihood that the cloud server might intrigue with a malicious user, it is a test to have a secure and versatile Advanced Multiparty Searchable Encryption (AMSE) plan. In order to avoid this situation a new security model MPSE has been taken. In this symmetric searchable encryption scheme is used the user may share their key to other user for accessing the data. If other users have the key then can access the data. If other users have the key then can access the data, to avoid this problem we are using MPSE (Multiparty Searchable Encryption) scheme. In this scheme the other user cannot access the file, if they have key also.**

***Index Terms*— Advanced Multiparty Searchable Encryption (AMSE), Data encryption.**

I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. In this paper, here utilize and uniquely combine the public key based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements.

A. Ensuring Data Storage Security in Cloud Computing

Cloud security is an evolving sub-domain of computer security, network security, and, more broadly,

Grenze ID: 01.GIJET.5.1.28

information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, and Hybrid). There is number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. The responsibility goes both ways, however the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must ensure that the provider has taken the proper security measures to protect their information, and the user must take measures to use strong passwords and authentication measures.

II. Existing Systems

In the existing system the user has a single key to view the multiple indexes of the data or document. Each document has a single trapdoor. If the user leaks the trapdoor to the unauthorized user, he/she can view the particular document with that trapdoor. It is not secure for an untrusted server. Cloud improves due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. The third party auditing process should bring in no new vulnerabilities towards user data privacy.
While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. CSP might reclaim storage for monetary reasons by discarding data that have not been or are rarely accessed, or even hide data loss incidents to maintain a reputation. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.

III. Proposed Work

To avoid the single trapdoor, the multiple trapdoors has been generated for every user by AMSE schemes. AMSE 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. Due to the private nature of personal data, there is an inherent need for a user to selectively share her data with different recipients. In practice, what a user can do is to set some access control policy and then rely on the cloud server to enforce them. Unfortunately, this approach is not realistic due to two reasons. One is that the users have no means to prevent the server from accessing their data. The other is that, even if the server is benign, it may also be forced to share users' data with other parties. The concept of searchable encryption provides a promising direction in solving the above problem. Such schemes allow users to store their data in encrypted form at an untrusted server, and then delegate the server to search on their behalf by issuing a trapdoor (i.e.encrypted keyword).

IV. Modules Description

A. Cloud User login

In this module, only authorized cloud user has been allowed to access the cloud. To access the cloud the user has to register himself. The user can upload multi file in the cloud. The user can view their own files. A cloud

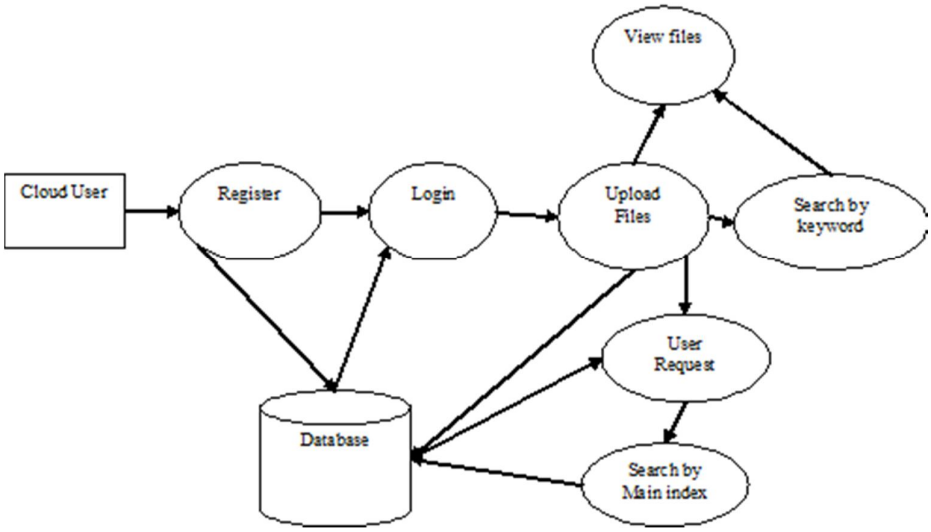

Fig 1. System Architecture

consumer that owns a cloud service hosted by a third-party cloud does not necessarily need to be the user (or consumer) of the cloud service.

Portal Direct Entry skips the Gateway and Login pages when users access the URL for Blackboard Learn. Instead, users are shown the first portal tab. When users access the system through Portal Direct Entry, they are considered guests until they log in. The Login Module is a portal module that allows users to type a user name and password to log in. This module can be placed on any module tab to allow users to log in to the system

The Login Module appears to users when Portal Direct Entry is on. Text for the module may be added from the Module Contents Login Module page. The text appears in the module along with the boxes for entering a user name and password.

B. Indexing API

In this module the user can upload any data and stored in the cloud. Before storing a file directly the user has to encrypt the data with specific key. The encrypted data is stored in the cloud. For example: A person wants to store the file in the cloud. Before uploading the file, the user has to encrypt the file with the encrypt key. After encryption the data has been uploaded and stored in the cloud

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 advanced multiparty searchable encryption (AMSE) 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 AMSE 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.

V. CONCLUSIONS

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. 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.

REFERENCES

[1] Ballard, L., Kamara, S., Monrose, F. 2005: Achieving efficient conjunctive keyword searches over encrypted data. In: Qing, S., Mao, W., López, J., Wang, G. (eds.) ICICS.

[2] Boldyreva, N. and A . O'Neill. 2009 Order preserving symmetric encryption. In A. Joux, editor, *Advancesin Cryptology — EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 224–241.Springer.

[3] Byun, J.W., Lee, D.-H., Lim, J.-I. (2006): Efficient conjunctive keyword search on encrypted data storage system. In: Atzeni, A.S., Lioy, A. (eds.) EuroPKI 2006. LNCS, vol. 4043, pp. 184–196. Springer, Heidelberg

[4] Cash, D., Jagger, J., Jarecki, S., Jutla, C., Krawczyk, H., Rosu, M.C., Steiner, M. 2013: Dynamic searchable encryption in very-large databases: Data structures and implementation (manuscript)

[5] Cash, D., Jarecki, S., Jutla, C., Krawczyk, H., Rosu, M., Steiner, M. 2013: Highlyscalable searchable symmetric encryption with support for boolean queries. Report 2013/169, Cryptology ePrint Archive

[6] Chang, Y.-C., Mitzenmacher, M. 2005: Privacy preserving keyword searches on remote encrypted data. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 442–455. Springer, Heidelberg

[7] Chase, M., Kamara, S. 2010: Structured encryption and controlled disclosure. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 577–594. Springer, Heidelberg

[8] Curtmola, R., Garay, J.A., Kamara, S., Ostrovsky, R. 2006: Searchable symmetric encryption: improved definitions and efficient constructions. In: Juels, A., Wright, R.N., Vimercati, S. (eds.) ACM CCS 2006, pp. 79–88. ACM Press

[9] Gentry, C. 2009: Fully homomorphic encryption using ideal lattices. In: Mitzenmacher, M. (ed.) 41st ACM STOC, pp. 169–178. ACM Press

[10] Golle, P., Staddon, J., Waters, B. 2005: Secure conjunctive keyword search over encrypted data. In: Jakobsson, M., Yung, M., Zhou, J. (eds.) ACNS 2004. LNCS, vol. 3089, pp. 31–45. Springer, Heidelberg (2004)G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros.Practical group signatures without random oracles.http://eprint.iacr.org/2005/385.

[11] Islam, M., Kuzu, M., Kantarcioglu, M. 2012: Access pattern disclosure on searchable encryption: Ramification, attack and mitigation. In: Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2012), San Diego, CA. Internet Society

[12] Yogapriya, J., Saravanabhavan, C., Asokan, R., Vennila, I., Preethi, P., Nithya, B. 2018. A Study of Image Retrieval System Based on Feature Extraction, Selection, Classification and Similarity Measurements. Journal of Medical Imaging and Health Informatics, 8(3), 479-484.

[13] 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.

[14] Thillaiarasu N., Chenthur Pandian S., Naveen Balaji G., Benitha Shierly R.M., Divya A., Divya Prabha G. (2019) Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems. In: Hemanth J., Fernando X., Lafata P., Baig Z. (eds) International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018. ICICI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 26. Springer, Cham.

[15] Thillaiarasu, N. and ChenthurPandian, S., 2017. A novel scheme fo safeguading confidentiality in public clouds fo sevice uses of cloud computing. Cluster Computing, pp.1-10.
[16] Saravanan Kumarasamy and Dr.R.Asokan An Efficient Detection Mechanism for Distributed Denial of Service (DDoS) Attack. International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.5, December 2011.
[17] 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.
[18] 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.
[19] 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).
[20] 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).
[21] 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.