Improving Data Storage Security Based On Key-Base Algorithm in Cloud Computing

Nikita V. Pathrabe, Prof. D. M. Khatwar

***Abstract*— Cloud computing has a big problem as security and outsource about the data like edit, delete or update the data. Consumption of highly sensitive data or information on cloud having privacy problem. The data encryption may increase the security thread in some extends but it fall in the problem about data access fastly. The processes that we introduce is Searchable Symmetric Encryption (SSE) which allows retrieval of encrypted data over cloud. So in this paper we fully focus on data privacy issues with the help of Searchable Symmetric Encryption (SSE).**

Now this is the first time we are going to use similarity relevance and scheme robustness to solve the privacy issues. We found in some system or server that the data privacy is leaks with the use of Order-Preserving Encryption (OPE). To eliminate this leakage, we propose a Two-Round Searchable Encryption (TRSE) scheme that supports Top-k-multi-keyword retrieval. In TRSE we introduce a vector space model and homomorphic encryption methods. In that the vector space model will helps to provide sufficient search accuracy, which enables users to involve in the ranking. As a result, information leakage can be eliminated and data security is ensured. So through security and performance analysis show that the propose scheme in this paper guarantees about high security and fully efficient data management.

***Index Terms*— Top-k-multi-keyword retrieval, Distributed scheme, Data redundancy, Cloud**

I. INTRODUCTION

Cloud computing is an internet based development and use of computer technology. It is possible that users can subscribe high quality services from data and software that reside solely on remote data centers with increasing network bandwidth and reliable, flexible network connections [1]. The main threat on cloud computing is about data privacy which roots in the cloud itself. When user wants to access their private data on to the cloud for performing the changes functionality on data. That all things are managed by cloud service provider. The CSP also manages the communication between the user and the cloud.

The Example of cloud service provider is Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2). These all online services which provide huge amount of storage space and customizable computing resources.

Manuscript received July 20, 2015

Nikita V. Pathrabe, Computer Science & engineering, Agnihotri College of Engineering, Wardha

Prof. D. M. Khatwar, Computer Science & engineering, Agnihotri College of Engineering, Wardha

At first the traditional cryptography is used for the purpose of data security protection but by using this user loss the control over the data. Each and every user stored his or her various kinds of data in the cloud and demands their data safety for long time assurance. The problems occur by verifying the correctness of data in the cloud becomes lots of challenging. Next Secondly, Cloud Computing is not a third party data warehouse. The stored data in the cloud frequently updated by the users i.e. insertion, deletion, modification, appending, recording, etc. to ensure storage correctness under dynamic data update.

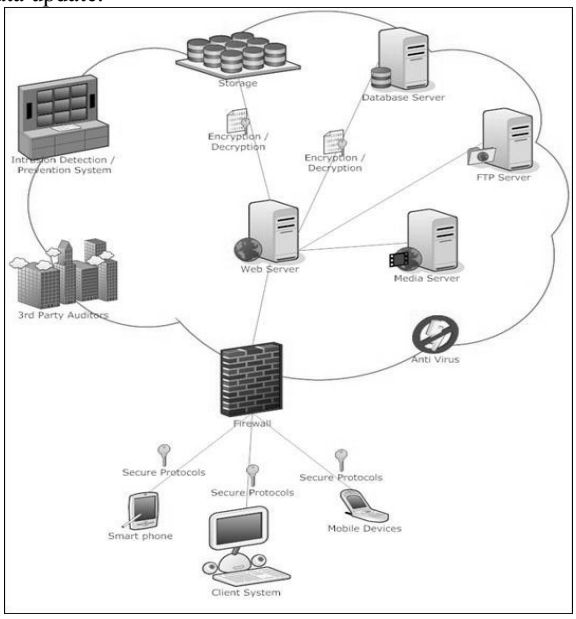

Fig. 1: Cloud data storage architecture

II. DESIGN METHODOLOGIES

The data design transforms the information domain model created during analysis into the data structures that will be required to implement the software. The data objects with the relationships defined in the entity relationship diagram with the detailed data content depicted in the data dictionary provide the basis for the data design activity. The part of the data design also may occur in conjunction with the design of software architecture. The detailed data design will occurs in each software component. Now architectural design define us the relationship between major structural elements of the software, and the design patterns that can be used to achieve the requirements the system architecture. During each design activity, we apply basic concepts and principles that lead to high quality.

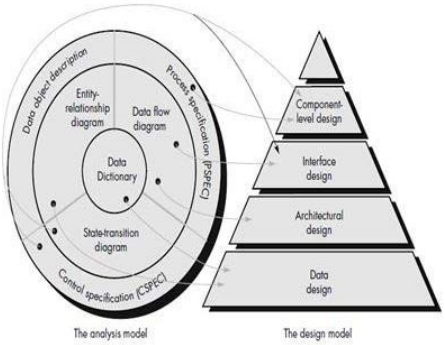

Fig.2 Translating Analysis model into Design model

The interface design describes how the software communicates itself. An interface implies a flow of information (e.g., data and/or control) and a specific type of behavior. That's why, data and control flow diagrams provide us lot of information required for interface design. The component-level design transforms structural elements of the software architecture into a procedural description of software components.

III. Flow Activity Model

As you can see in the fig. Activity diagram it actually show flow of the design model of the practically implementation of the paper. In that first the server must to in running state, and should me waiting on ports to accept the user request for connection. Once server is in running state the user can able to access the data.

Now in second step use have to login first and then access the file or resources. Once she done with the editing or updating resources he must to logout.

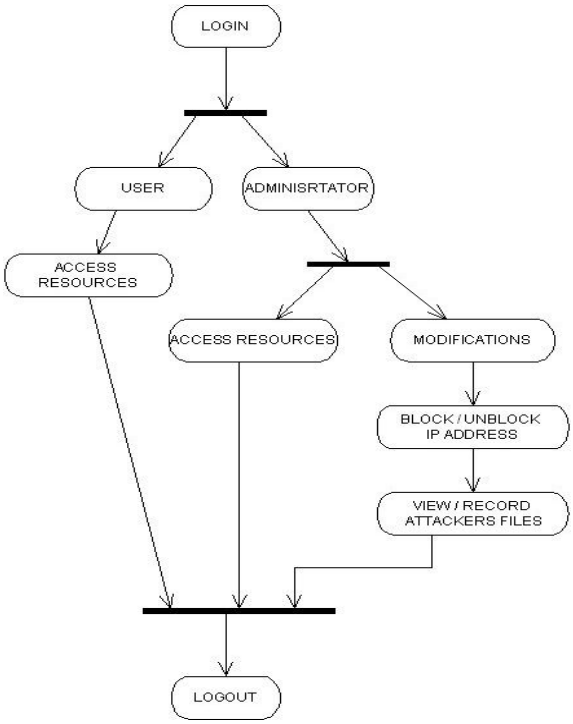

Fig.3 Activity Diagram

At admin side the admin have authority to add or remove resources do the modifications and also can block specific ip address if they found any issue.

IV. Basic Snapshot of Working Module:

A. Server login

Fig a) Server login model

B. Server model

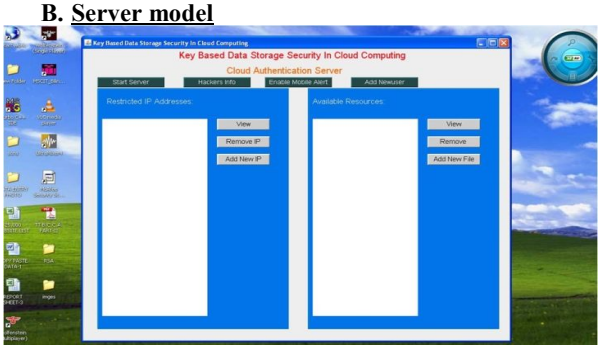

Fig b) Server working model

C. Client Login

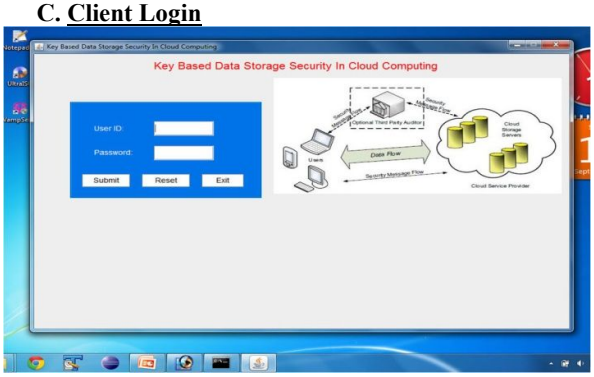

Fig c) Client Login model

D. Client model

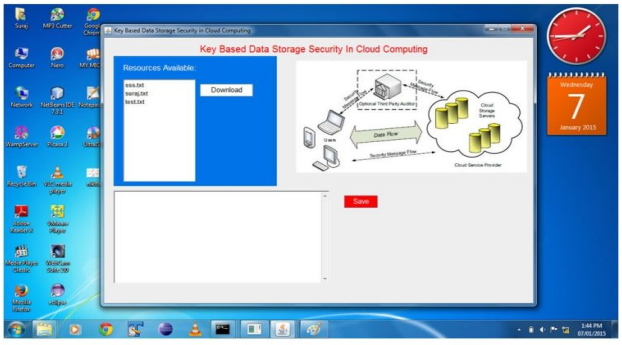

Fig d) Client Working model

E. Client confirmation key model

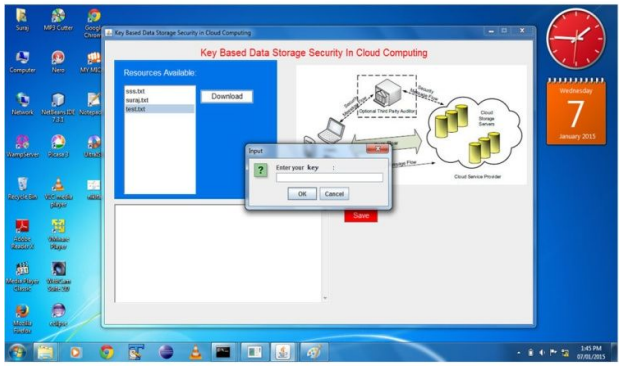

Fig e) Client Confirmation Key model

CONCLUSION AND FUTURE SCOPE

In this paper we are research and studied to working on the key based data storage security in cloud computing successfully which provide the security to the user important data in all the way. Also It grunted about the data dependency on editing, updating or deleting the data successfully.

In future we can implement the same scheme for mobile phone as well so it make so easy to handle the account via mobile rather than requirement of system or laptop so it also provide the same security thread in mobile computing in future.

REFERENCES

[1] "Key Base Data Storage Security In Cloud Computing", Nikita V. Pathrabe, Prof. D. M. Khatwar, Jan-Feb 2015,IORD Journal of Science & technology, E-ISSN:2348-0831 Vol. 2, Issue 2.

[2] "Toward Secure Multi-Keyword Top-k Retrieval Over Encrypted Cloud Data", Jaidi Yu, Peng Lu, Yanmin Zhu,Gaungtao Xue, Minglu Li, JULY/AUGUST 2013, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4.

[3] "Secure Ranked Keyword Search Over Encrypted Cloud Data", C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, 2010, Proc. IEEE 30th INT'1 Conf. Distributed Computing Systems (ICDCS).

[4] "Privacy-Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data", N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, 2011, Proc. IEEE INFOCOM.

[5] "Processing Private Queries Over Untrusted Data Cloud through Privacy Homomorphism", H. Hu, J. Xu, C. Ren, and B.choi, 2011, Proc. IEEE 27th INT'l Conf. Data Eng. (ICDE).

[6] "Searchable Symmetric Encryption: Improved Definitions And Efficient Constructions", R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, 2006, Proc. ACM 13th Conf. Computer and Comm. Security (CCS).

[7] "Fully Homomorphic Encryption over the Integers," M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, 2010, Proc. 29th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques, H. Gilbert, pp. 24-43.

[8] "Fully Homomorphic Encryption Using Ideal Lattices," C. Gentry, 2009, Proc. 41st Ann. ACM Symp. Theory of computing (STOC).

[9] "Secure And Dependable storage services in cloud computing", Cong Wang, Kui Ren, Qian Wang and Wenjing Lou, 2011, IEEE transactions on Services Computing, vol 5, no. 3, pp 220-232.

[10] "Zerber+r: Top-k Retrieval from a Confidential Index," S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, 2009, Proc. 12th Int'l Conf. Extending Database Technology: Advances in Database Technology (EDBT).

[11] "Fully Homomorphic Encryption over the Integers," M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, 2010, Proc. 29th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques.

[12] "New Lattice-Based Cryptographic Constructions," O. Regev, 2004,J. ACM, vol. 51, no. 6, pp. 899-942.

[13] "Approximate Integer Common Divisors," N. Howgrave-Graham, 2001,Proc. Revised Papers from Int'l Conf. Cryptography and Lattices (CaLC' 01), pp. 51-66.

[14] "Practical Techniques for Searches on Encrypted Data," D. Song, D. Wagner, and A. Perrig, 2000,Proc. IEEE Symp. Security and Privacy.

[15] "Public- Key Encryption with Keyword Search," D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, 2004,Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt).

[16] "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes," N. Smart and F. Vercauteren, 2010,Proc. 13th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC).