International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

2017 IJIEMR.Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 19th Sept2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-8

Title: **MULTI KEYWORD RANKED SEARCH FOR MULTIPLE DATA OWNERS IN THE CLOUD COMPUTING**

Volume 06, Issue 08, Pages: 206– 209.
Paper Authors

S.VINISHA, G.SWAMY
Vivekananda Institute of Technology & Science, Karimnagar, Telangana, India.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

MULTI KEYWORD RANKED SEARCH FOR MULTIPLE DATA OWNERS IN THE CLOUD COMPUTING

[1]S.VINISHA [2]G.SWAMY
[1]M.Tech Student, Department of CSE, Vivekananda institute of Technology & science, Telangana, India.
[2]Assistant Professor, Department of CSE, Vivekananda Institute of Technology & science,Telangana, India.

ABSTRACT: Observing the perspective of distributed computing, it has moved toward becoming increasing prominent for information proprietors to outside provider their data to open cloud servers while enabling information clients to recapture this information. To identify with withdrawal, safe hunts over scrambled cloud information have incite more research works under the sole proprietor demonstrate. Be that as it may, most cloud servers practically speaking don't simply Serve interesting proprietor; rather, they bolster different proprietors to share the benefits brought by distributed computing. In this paper, we propose - To be careful the mystery and a few proprietor demonstrate look through a few keywords and Ranked. To make conceivable cloud servers to execute safe to look exclusion knowing the genuine data of the two KEYWORDS and trapdoors, To keep alive the security of related scores amongst catchphrases and records furthermore, rank the query output, we propose a novel Additive Order and Privacy Preserving Function family and dynamic shrouded key creation lead and another information client to build up as authentic run the show.

Keywords: Cloud computing, ranked keyword search, several owners, privacy preserving, dynamic hidden key

I. INTRODUCTION

Distributed storage framework, is set of capacity servers, and gives long haul stockpiling administrations over the Internet. Putting away information in an outsider's cloud framework makes grave interface with over information mystery. Typical shrouded plans shield information mystery however has some restriction to usefulness of the capacity framework in light of the fact that a couple of operations are bolstered over shrouded data. Building a grave stockpiling framework that good a few capacities is perseverance when framework is dispersed.

Administration suppliers of cloud would vow to proprietors information security utilizing marvel like virtualization and firewalls. These wonder's don't shield proprietors information security from the CSP itself, since the CSP control entire of cloud equipment, programming, and proprietors' information. Concealing the touchy information before send outside can put away information privacy against CSP. Information shrouded influences the customary information usage to benefit in light of plaintext watchword look through an

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

exceptionally difficult issue. An answer for this issue is to download all the concealed information and make the first information utilizing the shrouded key, be that as it may, this is not functional reason it make additional overhead In this paper, we propose when look through numerous proprietor various KEYWORDS that time give the security and demonstrate the bring about positioning structure to make simple cloud servers to perform safe look barring knowing the genuine estimation of the two catchphrases and trapdoors, we appropriately manufacture a novel safe hunt run the show. With the goal that different information proprietors utilize unmistakable keys to conceal their documents and KEYWORDS. Honest to goodness information clients can get a question barring knowing private keys of these different information proprietors. To rank the list items and save the security of importance scores amongst catchphrases and records, we propose a family which jelly protection, which helps the cloud server restore the most pertinent query items to information clients without uncovering any delicate data. To shield from uncovering the outcome we propose a novel dynamic mystery key era convention and another information client verification rule [1]. The primary commitments of this paper are recorded as takes after: • we characterize seek information on educated that information is shrouded organize and furthermore giving the security when look through the numerous. We propose a fit information client verification control, which stop assailants to reveal concealed key and just veritable information client can do seek. We propose an approach that plays out numerous watchword pursuits and rank them appropriately.

II. RELATED WORK

We have again visit the issue of easy to search symmetric encryption, which give permeation a client to store its data on a external server in such a way that it can search without disclosing the data . We generate more affords to add new security and new work. Motivated by subtle problems in all previous security definition for SSE, we propose new definitions and point out that the existing notions have significant practical disadvantages contrary to the natural use of easy to find encryption.[1]

Disadvantages:

They only give the assurance to security for users that fulfill all their searches at once. We notice this limitation by introducing stronger definition that guarantee security even when users perform more realistic searches. Analysis give guidance to the choice the size of cipher text space . At the end suggest a unique and efficient transformation that can be applied to any OPE scheme. Our deep study shows that the transformation yields a scheme with more result safety in that the scheme oppose the one-wayness and window one-wayness attacks[2]. We opened the new way on how to get this notion, but the more efficient variant is certainly required. Second, how to construct SCF-PEKS scheme secure against keyword guessing attacks without requiring

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

bilinear pairing operations would be very interesting [3].

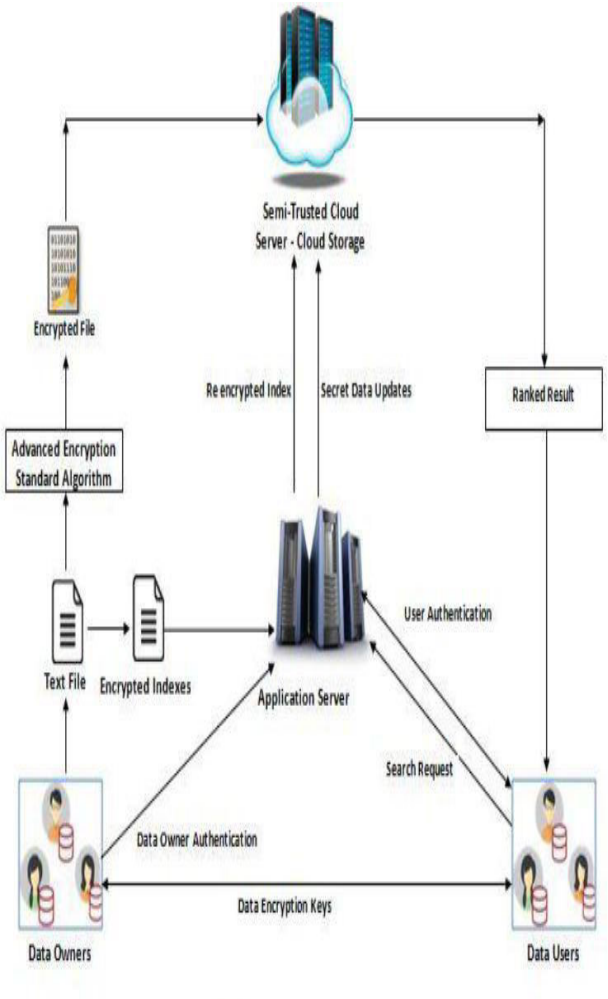

Fig1: System Architecture

System Implementation consist of various parts described as follows:

We are implementing our project by using Java Technology and My SQL database.

Various components of our system are:

1. Data Owner

2. Data user

3. Application server

4. Cloud server

1. Data Owner

Data owner have the set of files, they create the index file ad send that file to the application server. Finally Data owner encrypt that file and send encrypted file to the cloud server .as a\well as send the encryption key to the data user.

2. **Application server:**

Application server re-encrypt the index file of authenticated user and send that re-encrypted file to the cloud server

3. Data user

Data user send keywords to search to words the application server, application server send that request to the cloud server if the data user is the authenticated user by creating the trapdoor

4. Cloud server

Upon receiving the trapdoor, the cloud server searches the encrypted index *of* each data owner and returns the corresponding set of encrypted files.

III. CONCLUSION AND FUTURE WORK

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the

privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Moreover, we show that our approach computationally efficient, even for large data and keyword sets.

REFERENCES

1. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. ACM CCS'06*, VA, USA, pp. 79–88, Oct. 2006.
2. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. ACM SIGMOD'04*, Paris, France, pp. 563–574, Jun. 2004.
3. D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *EUROCRYPT*, vol. 43, pp. 506–522, 2004.

S.Vinisha Currently doing M.Tech in Computer Science & Engineering at Vivekananda Institute of Technological Sciences, Karimnagar, India. Research interests includes Networks, Mobile Computing, Data Mining etc.,

G.Swamy Currently working as an Assistant Professor at Vivekananda Institute Of Technological & Sciences, Karimnagar and has 15 years of experience in Academic. His research areas include Information Security, Mobile and Cloud computing, Data Mining, Network Security etc.,