Privacy preserving ranked multi keyword search for Multiple Data owners in cloud computing

[1] Vadlamudi Prasanna, [2]Mr.Gopinath reddy .M

[1]M. Tech Student, Department of Computer Science , Nalanda Institute of Engineering and technology, Kantepudi Village, Sattenapalli, Guntur, Andhra Pradesh, India, 522438

[2] Assistant Professor , Department of Computer Science, Nalanda Institute of Engineering and technology, Kantepudi Village, Sattenapalli, Guntur, Andhra Pradesh, India, 522438

Abstract:-

With the appearance of cloud computing, it has turned out to be progressively prominent for data owners to outsource their information to open cloud servers while enabling information clients to recover this information. For protection concerns, secure hunts over scrambled cloud information have persuaded a few research works under the single proprietor show. In any case, most cloud servers by and by don't simply serve one proprietor; rather, they bolster various proprietors to share the advantages brought by cloud computing. In this paper, we propose plans to manage Privacy protecting Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To empower cloud servers to perform secure search without knowing the genuine information of the two watchwords and trapdoors, we efficiently develop a novel secure inquiry convention. To rank the query items and save the security of pertinence scores amongst catchphrases and documents, we propose a novel Additive Order and Privacy Preserving Function family. 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. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user

Introduction:-

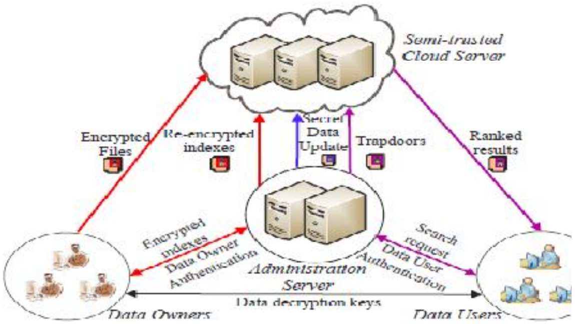
As a new model of computing, cloud computing provides abundant benefits including easy access, decreased costs, quick deployment and flexible resource management, etc. Enterprises of all sizes can leverage the cloud to increase innovation and collaboration. Despite the abundant benefits of cloud computing, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including emails, personal health records and government confidential files, to the cloud. This is because once sensitive data are outsourced to a remote cloud; the corresponding data owners lose direct control of these data. Cloud service providers (CSPs) would promise to ensure owners' data security using mechanisms like virtualization and firewalls. However, these mechanisms do not protect owners' data privacy from the CSP itself, since the CSP possesses full control of cloud hardware, software, and owners' data. Encryption on sensitive data before outsourcing can preserve data privacy against CSP. However, data encryption makes the traditional data utilization service based on plaintext keyword search a very challenging problem. A trivial solution to this problem is to download all the encrypted data and decrypt them locally. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset.

Searchable encryption is further developed. However, these schemes are concerned mostly with single or Boolean keyword search. Extending these techniques for ranked multi keyword search will incur heavy computation and storage costs. Secure search over encrypted cloud data is first defined by Wang et al. and further developed. These researches not only reduce the computation and storage cost for secure keyword search over encrypted cloud data, but also enrich the category of search function, including secure ranked multi-keyword search, fuzzy keyword search, and similarity search. we propose PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model. To enable cloud servers to perform secure search without knowing the actual value of both keywords and trapdoors, we systematically construct a novel secure search protocol. We have discussed the potential opportunities and the current state-of-the-art of high-performance scientific computing on public clouds. The adoption of Cloud computing as a technology and a paradigm for the new era of computing has definitely become popular and appealing within the enterprise and service providers. Users are not able to check his data again and again from the cloud storage it is secure or not. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. We study the setting in which a user stores encrypted documents (e.g. e-mails) on an untrusted server. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Work in this area has largely focused on search criteria consisting of a single keyword. If the user is actually interested in documents containing each of several keywords (conjunctive keyword search) the user must either give the server capabilities for each of the keywords individually and rely on an intersection calculation (by either the server or the user) to determine the correct set of documents, or alternatively, the user may store additional information on the server to facilitate such searches.

2. RELATED WORK

Scientific computing often requires the availability of a massive number of computers for performing large scale experiments. Traditionally, these needs have been addressed by using high-performance computing solutions and installed facilities such as clusters and super computers, which are difficult to setup, maintain, and operate. Cloud computing provides scientists with a completely new model of utilizing the computing infrastructure. The cloud storage has a lot of problems about the security and data Integrity. So we need to prevent the all problems. In cloud storage users can remotely store their data and enjoy the on-demand high quality applications and services from shared resources, without the burden of local data storage and maintenance. Users are not able to check his data again and again from the cloud storage it is secure or not. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. We study the setting in which a user stores encrypted documents (e.g. e-mails) on an untrusted server. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Searchable encryption is a technique that allows a client to store documents on a server in encrypted form. Stored documents can be retrieved selectively while revealing as little information as possible to the server. In the symmetric searchable encryption domain, the storage and the retrieval are performed by the same client.

3. Frame Work



Data owner scalability: Data owners to enter this system without affecting other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model.

Data user revocation: Data users can perform correct searches. Moreover, once a data user is revoked, he can no longer perform correct searches over the encrypted cloud data.

Security Goals: The proposed scheme should achieve the following security goals:

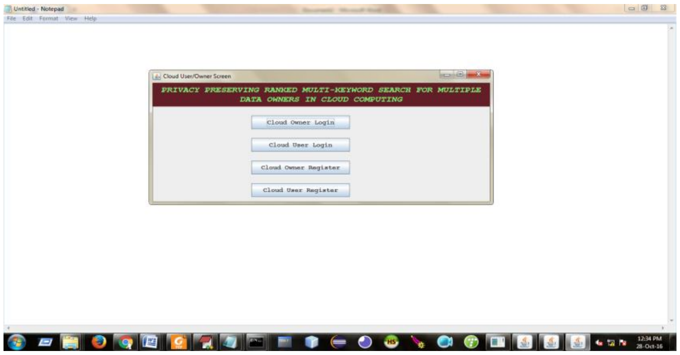
1) Keyword Semantic Security: We will prove that PRMSM achieves semantic security against the chosen keyword attack.

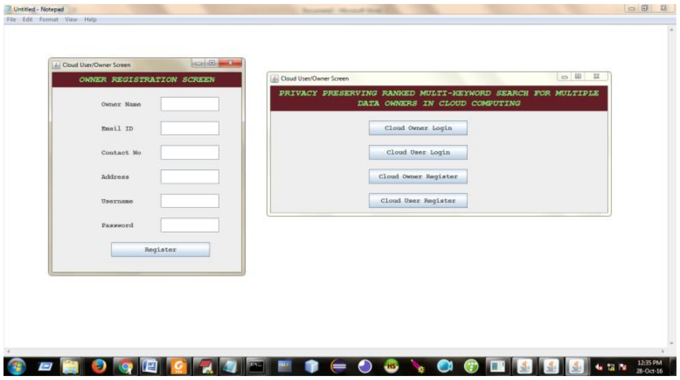
2) Keyword secrecy: Since the adversary *A* can know whether an encrypted keyword matches a trapdoor, we use the weaker security goal (i.e., secrecy), that is, we should ensure that the probability for the adversary *A* to infer the actual value of a keyword is negligibly more than randomly guessing.

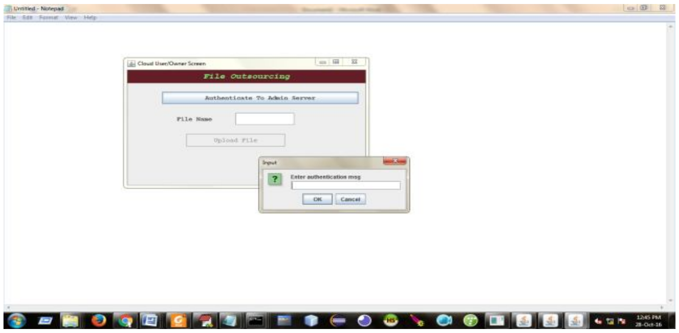
3) Relevance score secrecy: We should ensure that the cloud server cannot infer the actual value of the encoded relevance scores.

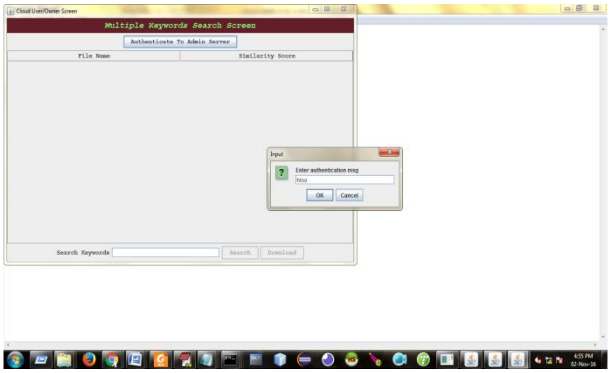
4. Experiment Results:-

Here in the cloud computing we are storing the data with the security if we are providing the security to the owner data here we have to provide the data access to the multiple data owner and multiple data user if the owner can upload the data with the security and one more verification option if the user want to access the data user need to search the data and access to the secure path owner can upload the data in to the cloud with the security when you login as the user we have the option we can upload the data and download the file and save the file and here we have the file verification process for that it have the process of verifying the data into the file and verify to that file and download the file and provide the permission to the file. If we need to access the file we need to search with the keyword if we need access the file we just search the file with the key word. Here we have revoke process admin can revoke the user.


Untitled - Notepad
File Edit Format View Help
Cloud User/Owner Screen
PRIVACY PRESERVING RANKED MULTI-KEYWORD SEARCH FOR MULTIPLE DATA OWNERS IN CLOUD COMPUTING
Cloud Owner Login
Cloud User Login
Cloud Owner Register
Cloud User Register

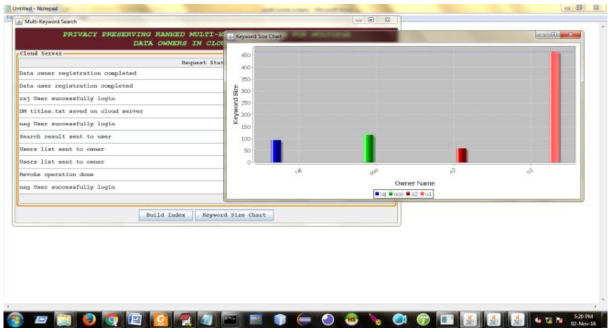






Enter authentication msg

hioo



Data owner registration completed
Data user registration completed
raj User successfully login
DM titles.txt saved on cloud server
nag User successfully login
Search result sent to user
Users list sent to owner
Users list sent to owner
Revoke operation done
nag User successfully login

Conclusion:-

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.

REFERENCES :-

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communication of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE International Symposium on Security and Privacy (S&P'00), Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003) Secure indexes. [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79–88.

[6] 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.

[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[8] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Information and Communications Security (ICICS'05), Beijing, China, Dec. 2005, pp. 414–426.

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253–262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829–837