MORPHISM CRYPTOGRAPHY ON CLOUD DATA FOR STRUCTURE-PRESERVING USING MRSME

D. Dinesh Babu
Assistant Professor
Alpha College of Engineering and Technology
Dept. of Computer Science and Engineering
Pondicherry, India.
dineshbabu89@pec.edu

J. Monica
Alpha College of Engineering and Technology
Dept. of Computer Science and Engineering
Pondicherry, India.
j.s.monica2010@gmail.com

P. Kanchanadevi
Alpha College of Engineering and Technology
Dept. of Computer Science and Engineering
Pondicherry, India.
kanchana.perumal.cs@gmail.com

***Abstract*—In the dawn of cloud computing, data owners are impulsion to outsource their complex data management system from local site to commercial cloud for great flexibility and economic saving. But for protecting data privacy, sensitive data has to be encrypted before outsourcing to commercial public cloud. The privacy-preserving multi-Keyword ranked search method is used in the cloud technology for improve the search result accuracy as well as enhance user searching experience by means of ranking system. It is also crucial for such ranking system for multi-Keyword search instead of using single keyword search. Encrypted cloud, search system remains a very challenging task because of inherent security and privacy obstacles, including various strict requirements like data privacy, index privacy, keyword privacy etc. Encryption often renders data useless in the sense that one loses the ability to operate on it. The data owner desires to stores structured data on an untrusted server and only retain certain information. To guarantee confidentiality the owner could encrypt the data before sending it to the server but this approach is unsatisfactory because the data loses its structure and, in turn, the owner loses the ability to query it efficiently. To address this we are designing cryptosystems that support a variety of computing on encrypted data, ranging from general-purpose computations. To overcome the problem of privacy preserving multi-keyword ranked search over encrypted cloud data, the homomorphic cryptography method is used which enhance the security in the cloud data.**

Keywords—Cloud data; Homomorphic Cryptography; Homomorphic Encryption; MRSE.

I. INTRODUCTION

The term “cloud” was coined from the computer network diagrams which use it to hide the complexity of infrastructure involved [1]. Cloud computing relies on sharing of resources to achieve coherence and economic of sales, similar to utility over a network. Cloud users can remotely store their data into the cloud so as to enjoy the features including resource pooling, Rapid elasticity, measured service, on-demand self service and broad network access. Cloud computing consumers use cloud templates to move applications between clouds through a self-service portal. The predefined blueprints define all that an application requires to run in different environments. For greater flexibility and economic saving the cloud consumers are encouraging to outsource their local complex data management system in to cloud, especially when the data produced by them that need to be stored and utilized is rapidly increased. The improved use Google docs have the issue of privacy utmost importance. To protect data privacy and unwanted accesses in cloud on sensitive data, e.g., email, financial transaction and tax document etc., might have be encrypted by the data owners before outsourcing to the public cloud [2]. Decrypting huge amount of data leads to increase in bandwidth cost in cloud scale system Reducing local storage management the data can be stored in the cloud unless they can be searched and utilized easy. For this reason the privacy-preserving and efficient search over encrypted data is most important. Considering huge amount of data may be outsourced into cloud will leads to the problem of the scalability and system usability.

Here the cloud helps the information to hold on in remote cloud servers that permits the cloud customers to remotely store their information into the cloud therefore on relish the on-demand top quality applications and services from a shared pool of configurable computing resources. With the prevalence of cloud services, additional and additional sensitive data are being centralized into the cloud servers, like emails, personal health records, personal videos and photos, company finance information, government documents. to shield information privacy and combat uninvited accesses, sensitive information needs to be encrypted before outsourcing, therefore on give end-to-end information confidentiality assurance within the cloud and on the far side. In this model we tend to build use of each the information mining and cloud computing for the information ranking and retrieval. The most effective information is retrieved from the cloud and this technique proves to be additional economical than the conventional search engines.

The results viewed via search engines are graded either by their range of clicks and hits and it'd not be the relevant information. Document clustering, that involves grouping untagged text documents into significant clusters .One assumption, taken by ancient document cluster approaches the amount of clusters K is understood before the method of document cluster. K is thought to be a predefined parameter determined by users. However, in reality, decisive the suitable worth of K could be a troublesome downside.

First, given a group of documents, users need to browse the complete document assortment so as to estimate K. this can be not solely time overwhelming however additionally false particularly once addressing giant document information sets. Moreover, Associate in nursing improper estimation of K may simply mislead the cluster method. Cluster accuracy degrades drastically if an even bigger or a smaller range of clusters are used. Therefore, it's terribly helpful if a document cluster approach can be designed restful the idea of the predefined K. We apply the Top K query algorithm to retrieve the 'n' number of best matched results for the given query. While entering the query the user will also specify the number best matched results to be display in the result page so that the cloud server will display the same in the result page itself. Security and privacy protections are also engineered into Encrypted cloud computing system protect sensitive information. This enables a secured keyword search where the contents of the documents are encrypted using the AES and then the frequency of the Cloud server Files Encrypted files Keywords are calculated to label the document to find whether the data is relevant.

To solve the matter of effective nevertheless secure keyword search over encrypted cloud information, we tend to propose this technique. Within the planned system graded search greatly enhances system usability by returning the matching files during a graded order concerning to sure connection criteria (e.g. keyword frequency), therefore creating one step nearer towards sensible readying of privacy preserving information hosting services in Cloud Computing.

Conversely, to meet the effective data retrieval need, the data can be searched and retrieved by relevance ranking method. Such rank system is useful for the user to retrieve the most relevant data from the cloud server. Rank system can also eliminating unnecessary traffic and send back only relevant to the data users. For increasing search result accuracy and enhance user searching experience [3], such ranking system support multi-keyword search instead of using single keyword search. Nowadays today's search engines tend to provide multi-keyword search rather than using single keyword search to retrieve the most relevant data [5]. The Security is major impediment to broad scale implementation for cloud, regardless of the model SaaS, PaaS and IaaS. The adoption rate has been slowed by security concerns. Cloud providers recognize this is an impediment to selling cloud services controls. Encryption is one of the important techniques to provided security over cloud. Encrypted cloud data search system remains a very demanding task because of innate security and privacy obstacles including data privacy, index privacy and keyword privacy. Multiple owners can access their data and the system will allow access by only authenticated owners. This will provide a secure and privacy-preserving access control to users.

The encryption techniques will be processed for providing the security code for the data to be shared with the cloud users. The decryption concept which will be processed for providing the decrypt the security code which is encrypted and then file will be shared within the users of cloud. Cloud data will be a secured and trusted to share within the users also to share with multiple users of the cloud. It will provide the trusted sharing of data with high clock speed and with higher bandwidth and frequency of sharing the data which will be processed by the system hardware high speed sharing of multiple data are clearly based on the speed of the internet connectivity and with the system hardware connectivity. The maximum requirement of software and hardware systems are processed for sharing of multiple data latest system configuration which are processed for high data sharing rate. The real identities of data owners can be revealed by the group manager when disputes occur. It will also provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

The encryption code which can be given by user for secure data sharing only the group manager can detect the encryption code for official dispute of user data. The decryption process allows to receive the encrypted data those data can be encrypted only with the encryption code which are shared with the authorized cloud user. Cloud is maintained by the cloud service provider Data owner is the owner of the document. Authorized Data user can access document from the cloud server. Cloud services are provided to the users for pay per use. Cloud service frameworks are Software as a service, Platform as a service, and Infrastructure as a service. Cloud computing models the user to access the document from anywhere wherever network connection available characteristics of cloud computing are on demand self-service, broad network access, resource grouping, rapid elasticity and assessed service [11].

Cloud services are available as public cloud, private cloud, community cloud, hybrid cloud. Public cloud is offered over the internet to the general public in pay as you go manner. Private cloud is operated for specific organization. Community cloud is available only to groups. Hybrid cloud is the combination of public cloud and community cloud. Cloud document will be shared among the dynamic group. Dynamic group refers the changes of membership over the group. Outsourcing the document to the third party group causes the security and privacy issue. Because the members in the group are considered as dynamic. In a group each group member can read and modify the data of the file which is shared by the company.

The changes of membership make secure data sharing extremely difficult. Any member in the group can store the data and share the services by the cloud which will be called as multiple owner models. In a single owner model group manager can only store and modify the data in the cloud Security issue is the main problem of the development and widespread use of cloud computing. Cloud service provider should be trustworthy by providing trust and secure computing and data storage. In the untrusted server data owner depot the encrypted data files and disseminate the comparable decryption keys only to authorized people. So that, unauthorized people and file servers cannot able to learn the content of the document.

Encryption easily and simply provides the protection, key management, fine-grained access controls and advanced security intelligence data to protect sensitive data-at-rest within public, private or hybrid cloud environments. Still encryption leaves data useless in the sense one loss ability to operate on it. Consider if the data owner need to store the structured data in the untrusted server and preserve the constant amount of the information locally. To assure privacy, the data owner encrypted the data this approach is unacceptable because the

data loses its structure and in turn the owner loses the ability to query it efficiently.

The paper is organized as follows .Section II presents the Related work, Section III presents the Existing work, Section IV presents the System formulation, Section V presents Proposed system and Section VI present the Conclusion and section VII Future enhancement.

II. RELATED WORK

A. *Untrusted Encryption Over Cloud Data*

Consider three entity data user anne, cloud server benny and data owner. Anne has a collection of document and stored it on an untrusted server benny. For example Anne could be a mobile user to store her e-mail message on a mail server, benny is untrusted server, so Anne needs to encrypt her documents and only store her cipher text on benny. During encryption the data losses its structure and turn the owner loses the ability to query it efficiently from the server benny.

B. *Searchabe Encryption on Cloud Data*

The encryption documents along with the index are placed in the data server. The index is hidden to the server since it is highly confidential. The third party cannot able to access the document since they don't have the trapdoor. The trapdoor is provided only to the authorized user.

C. *Symmetric Encryption*

In an extensive or distributed situation, usual cryptographic structures suffer from key distribution problems (SE) or problems related to the competence of encryption function (ASE). Figure1 illustrate the essential approach how symmetric encryption (SE) can be applied to attain secure communication.

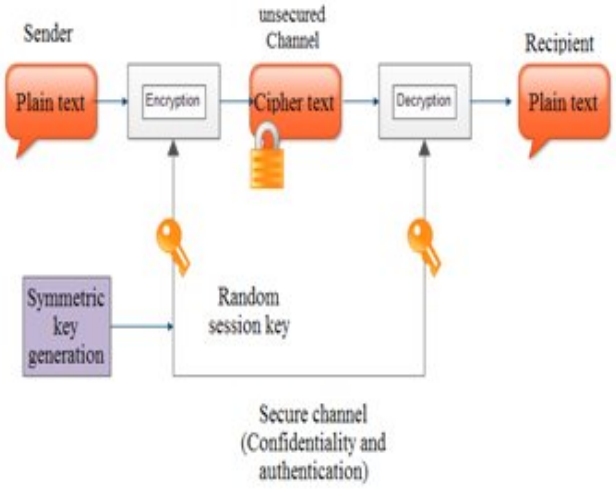

Fig. 1. Symmetric key encryption

D. *Asymmetric Encryption*

Public key encryption (figure 2) can resolve they key distribution difficulty of symmetric encryption. Now, instead of using a single symmetric key for both encryption and decryption, a couple of key is used. It consists of public key and private key, by issuing the public key of all possible receivers, a sender can send encrypted messages.

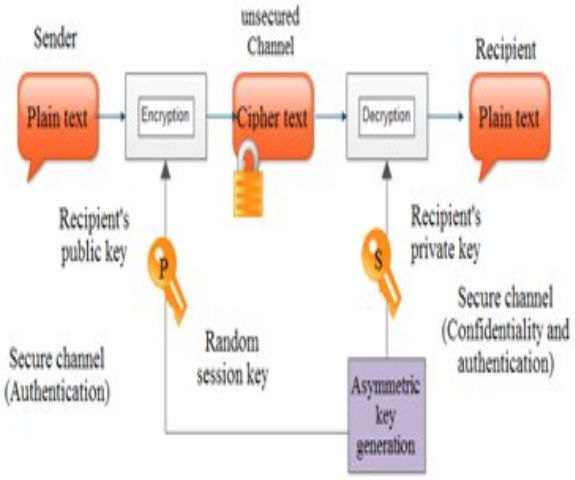

Fig. 2. Asymmetric encryption

E. *Identity-Based Encryption*

It is documentation less option to public key encryption, let's encrypting messages under textual strings, in its place of public keys [8]. Such a string at first refers to the individuality of receivers. It requires the ease of use of a complete list of all future receivers. So far, it allows understanding encryption that is partially suitable for one-to many settings, by describing a cluster by a single textual string. Dissimilarly, we search for devise an encryption scheme that is able to control more expressive policies.

F. *Single Keyword Searchable Encryption*

Traditional single keyword searchable encryption system usually builds an encrypted searchable index I such that its content is hidden to the server unless it is given suitable trapdoors created through secret key. In the symmetric key setting, and developments and advanced security definitions are given in Goh [6], Chang et al. [7]. Our early work solves secure ranked keyword search which utilizes keyword frequency to rank results instead of returning irrelevant results. It supports single keyword search. In the public key setting, Boneh et al. [9] present the first searchable encryption construction, where anyone with public key can write to the data stored on server but only authorized users with private key can search the data. Public key answers are usually very computationally high cost however. Also, the keyword privacy could not be protected in the public key setting since server could encrypt any keyword with public key and then use the received trapdoor to evaluate this cipher text.

G. *Boolean Keyword Searchable Encryption*

To enrich search functionalities, conjunctive keyword search over encrypted data have been proposed. These schemes incur large overhead caused by their fundamental

primitives, such as computation cost by bilinear map, e.g. or communication cost by secret sharing. As a more general search approach, predicate encryption schemes are recently proposed to support both conjunctive and disjunctive search. Conjunctive keyword search returns "all-or-nothing", which means it only returns those documents in which all the keywords specified by the search query appear; disjunctive keyword search returns undifferentiated results, which means it returns every document that contains a subset of the specific keywords, even only one keyword of interest. In short, none of existing Boolean keyword searchable encryption schemes support multiple keywords ranked search over encrypted cloud data while preserving privacy as we propose to explore in this paper.

The inner product queries in predicate encryption only predicates whether two vectors are orthogonal or not, i.e., the inner product value is concealed except when it equals zero. Without providing the capability to compare concealed inner products, predicate encryption is not qualified for performing ranked search. Furthermore, most of these schemes are built upon the expensive evaluation of pairing operations on elliptic curves. Such inefficiency disadvantage also limits their practical performance when deployed in cloud. On a different front, the research on top-*k* retrieval in database community is also loosely connected to our problem.

H. Vormetric Cloud System Encryption

It is easy and simpler to make the available protection, encryption key management, fine-grained access controls and advanced security intelligence data to protect susceptible data at rest within public, private or hybrid cloud environments. According to the Vormetric encryption [16] for your cloud implementations, you can:

- Support Compliance

To meet the compliance requirements for data file encryption, separation of duties and accessing the reins for protected data including PCI-DSS and Data Across Borders.

- Protect against data breach incidents

It is helping to protect from the data breach incidents with secure encryption, encryption key management and policy based access controls to protecting the data files in cloud environments included with the risks posed by exposure of the customer data to the cloud suppliers and data exposure to be shared, data storage used to support the cloud environments.

- Secure from advanced persistent threats

The Vormetric Cloud Encryption supplies the raw security intelligence about data accessing to the information protected by encryption that enables us as the Security Information and Event Management (SIEM) solution to be familiar with an advanced constant threat or malicious insider.

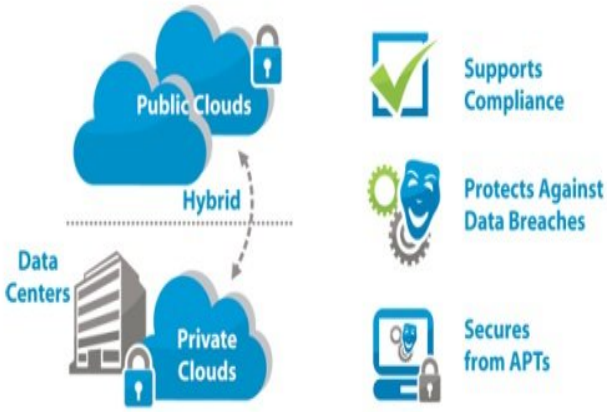

Fig. 3. Vormetric Cloud Encryption

This type of Encryption is a single, scalable solution that can easily encrypt any file, database or application, anywhere it resides on supported operating systems and file systems, without give up application performance and while avoiding key management complexity.

- Transparent

It includes many number of flawless encryption key management within the outcome and is entirely transparent to applications and users, then allowing the already existing processes and usage to prolong without any changes. Protecting any data file within cloud environments simply, easily and efficiently.

- Fine grained access controls

It will supports the detailed, policy-based separation of duties to propose a higher degree of security. To prevent the cloud administrators, root, network system administrative or unauthorized programmatic access to constrained data while allowing proper user and application usage. Lock out the cloud provider's visibility into your data, while also removing the risk that shared data file storage may result in exposure of your private information.

- Security Intelligence – It is for log data and it can be designed for easy integration with SIEM solutions, providing them with the thorough information on usage, access and access attempts that enables SIEM solutions to identify concession accounts, applications and even administrators.

III. EXISTING WORK

In the existing system we define and solve the problem for multi-keyword ranked search over encrypted cloud data (MRSE). The challenge behind is MRSE scheme secure inner product computation, which is adapt from the secure k-nearest neighbour (KNN) technique to improve the privacy in thread model. For the MRSE method the multi-keywords can be match with coordinate, MRSE framework cab change the dimension at final the inner product has computation can be

directly achieved. The same keyword has been denoted *rq* and *r'q*.

i.e., (*pi ¢rq*)=(*pi ¢r0q*) = (*pj ¢rq*)=(*pj ¢r0q*) = *r=r0*.

This relation helps to identify the similar query for multi-keyword ranked search relationship.

It's to provide a guarantee on search pattern clearly form above equation. This scheme setup after the extraction of keyword from the collections of document and data owner randomly generate the bit of vector two matrix with this 3-tuple has been generated totally. After that data owner generate the binary vector for each document, then trapdoor with the keyword as input on the binary vector to check whether it's true or false and extended the dimension vector while applying the encryption on the data. With the help of trapdoor, cloud server can compute the document with the score and return to the rank Id list.

$$I_i.T_w = \{M_1^T D_i^1, M_2^T D_i^{"}\}.\{M_1^{-1}Q^{'}, M_2^{-1} Q^{"}\}$$

$$= D_i^1.q^1 + D_i^{"}.q" = D_i.Q = r(D_i.Q)+t$$

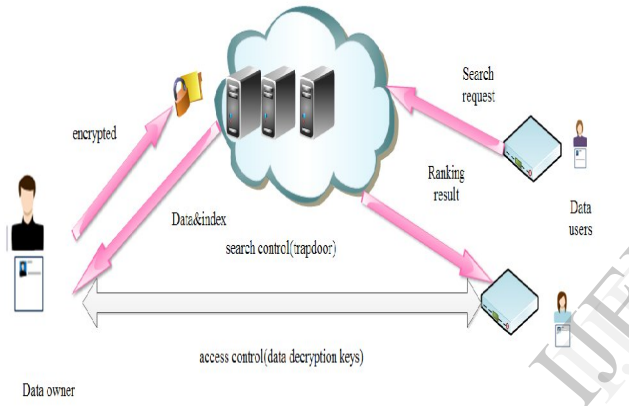

Fig. 4. Architecture of the encrypted cloud data

A. *Efficiency*

Index construction is to build a search based on index value form the dataset it can map the keyword from the document to vector for encryption on direct dimensionality of data vector in dataset.

Trapdoor affected by the number had documents in dataset that it has three schemes and becomes larger number of documents in dataset it's better when compare to the MRSE2 the MRSE3 is better for efficient outsource of the accurate data form multi-keyword ranked search technique.

Using the multiple queries the accuracy of data can be identified from the cloud server, MRSE scheme can be used for search result accuracy and enhance the user searching experience. In this searchable encryption technique is used over encrypted data. For effective data retrieval need, cloud server performs result relevant & ranking instead of returning undifferentiated result. Such ranked search system enables data use to find most relevant information quickly. To improve these search result accuracy user searching experience, it support multikeyword search for secure search, searchable encryption technique is used over encrypted data.

The main disadvantage of this existing system is a problem of encrypting structure data during encryption. In the cloud storage, searchable encryption allows the client to encrypt the data. During encryption the client lose the ability to query and retrieve it efficiently.

IV. SYSTEM FORMULATION

A. *System Model*

In view of cloud computing the search service including three entities as demonstrate figure 1 data owners, data user and cloud server. Collection of data will be stored in the cloud server by means of homomorphic encryption form. For effective searching capability the index I is build with an encrypted data and then exude both the index I and the encrypted document collection to the cloud server. When the user request the document, the data owner will placed the collection of documents to the untrusted server by means of fully homomorphic encryption for preserving data structure. We are going to apply the Ranking algorithm to rank the result as documents weights. For an example if the user enters the query as "Cloud Computing" then the server will retrieve the data and order them according to the document weights. Document will be ranks using the below mentioned formulae.

- Document weight= Total of query word query present in the document / Total number words in the document.

The ranking method is performed for the requested documents of the data user for better improvement of the results and also we can retrieve the documents using Top K query algorithm. By using this algorithm we can retrieve the Top K best matched results for the user entered query. So we retrieve most matched documents for the entered query.

B. *Security Model*

Homomorphic encryption is an another important encryption technique that encrypts the data into cipher text that can be analyzed and worked with as if it were still in its original form Figure 3. Plain text is the most portable format because it is supported by nearly every application on every machine ne and it does not contain any formatting commands. The cipher text is the result of encryption performed on plaintext using an algorithm, called a cipher. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption is the process of turning cipher text into readable plaintext, cipher text in not to be confused with code text because the latter is a result of a code, not a cipher.

C. *Design Goals*

To facilitate ranked search for effective utilization of outsourced cloud data under the abovementioned model, our design system should simultaneously achieve security and performance guarantees.

- Multi-keyword ranked search: To design search scheme which allow multi-keyword query and provide result similarity ranking for effective data retrieval, in steady of returning undifferentiated result.

- Privacy-preserving: To check cloud server from additional informational from dataset and index, to meet privacy requirement.
- Efficiency: Above goals on functionality and privacy should be achieved with low communication and computation overhead.

D. *Preliminary on coordinate Matching*

As a amalgam of conjunctive search and disjunctive search "coordinate matching [4] is an intermediate approach which uses the number of query keywords appearing in the document to quality the similarity of the document to the query. When users know to exact subset of the dataset to be retrieved, Boolean queries perform well with the precise search requirement specified by the user. In cloud computing, however this is not the practical case, given the huge amount of outsourced data. Therefore, it is more flexible for users to specify a list of keywords indicating their interest and retrieve the most relevant documents with rank order.

V. FRAMWORK AND PRIVACY REQUIRMENTS FOR MRSME

In this section, we define the framework of multi-keyword ranked search over encrypted cloud data(MRSME) and establish various strict system-wise privacy requirements for such as secure cloud data utilization system.

A. *MRSME framwork*

For easy presentation, operations on the data documents are not show in the framework since data owner could easily employ traditional symmetric key cryptography to encrypt and the outsource data. With focus on the index and query, a MRSME consists of four algorithms as follows.

- ***Setup*** *Taking a security parameter as input, data owner outputs a symmetric key as symmetric key(SK)*
- ***Build index*** *based on the dataset, data owner builds a searchable index which encrypted by the symmetric key(SK) then outsource to cloud server. After the index construction, the document collection can be independently encrypted and outsourced.*
- ***Trapdoor*** *with keywords of interest in input, this algorithm generates a corresponding trapdoor.*
- ***Query*** *when cloud server receives a query request, it performs the ranked search on the index with the help of trapdoor and finally the index the ranked id list of top-k documents sorted by their similarity with words*

Both search control and access control are nit within the scope of this paper. While the former is to regulate how the data can be encrypted with the help of multi-keyword ranked search Morphism encryption technique(MRSME) the in this paper we used to give the high performance of the data to be transfer for reducing the time performance.

B. *Privacy requiremts for MRSME*

The requirement privacy guarantee in the related literature, such as searchable encrypted is that server should search result. We deal with the set of encryption on privacy requirements specifically for the MRSME framework.

Data owner can resort to traditional symmetric key cryptography to encrypt the data before outsourcing, and successfully prevent cloud server from server into outsourced data.

Keyword privacy: As the users usually prefer to keep their search from being exposed to other like cloud server, the most important concern is to hide the searching. Although the trapdoor can be generate in the cryptographic way to protect the query keyword, cloud server do some statistical analysis over the search result to make an estimate. When cloud server knows some background information of the dataset, these keyword specific information may be utilized to reverse-engineer the keyword. This searchable encryption technique is helpful that treats encrypted data as a document and allows a user too securely of interest for developed the crypto primitives and cannot accommodate such high service-level requirement like system usablitiy,user searching experience and information can be easily discovered.

VI. PROPOSED SYSTEM

In this paper, we define and solve the problem of encryption over cloud data. Among various technique encryption, we choose the fully homomorphic encryption, because homomorphic encryption is a good basic to enhance the security measures of untrusted system or application hat stores and manipulates sensitive data. This strong protection of data results from the capability, allowed through HES, to perform arithmetic operation over encrypted bits. It allows complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets.

The term is derived from Greek words for same structure. Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations, whether they are performed on encrypted or decrypted data will yield equivalent results. It is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services. Fully homomorphic encryption is used in several applications. It allow private queries it a search engine, the user submit an encrypted query and the search engine compute concise encrypted answer without ever looking at the query in clear. It also permit searching on encrypted data, the user stores encrypted files on a remote file server and cam later have the server retrieve only files they satisfy cannot decrypted the files on its own. It improves the efficiency of secure multipart computations.

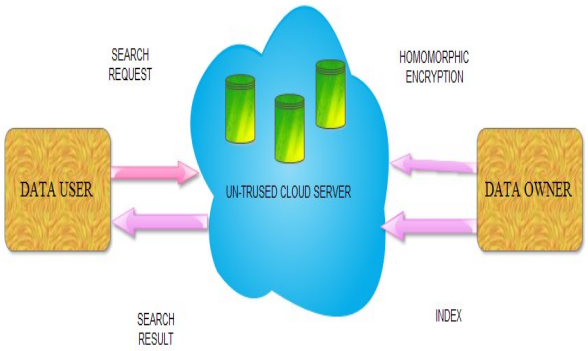

Fig. 5. Architecture of the homomorphic encryption cloud system

MRSHC scheme can be used for efficient security during encryption. In this homomorphic cryptography (structured encryption) techniques is used for encryption, data user can send request to the data owner base in the request the data owner can access the related data by the use of multi-keyword ranked search method form the cloud server and the data can be encrypted by fully homomorphic encryption method which compare to the existing the encryption is in unstructured form to overcome that vulnerability to give the security and over the cloud data we gives the more strength on encryption. In fully homomorphic techniques can give the encryption in structured form to this structure form the data can be received to data user in accuracy and relevant data. From this security over the data has been strengthen and security over each access data.

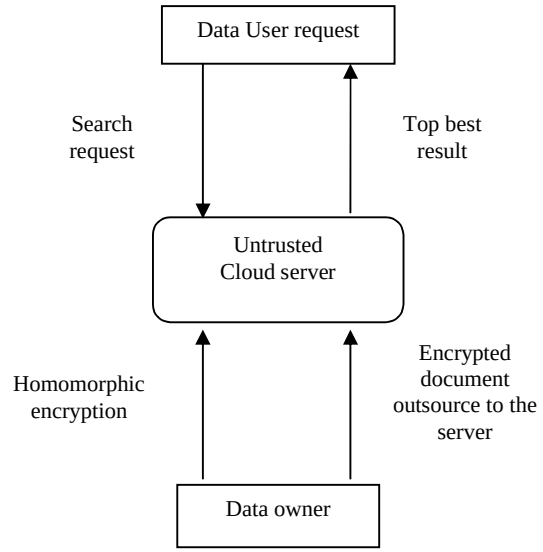

Fig. 6. System Flow Diagram

While giving the security in encryption there in less vulnerability the service of cloud can be increase because providing the security in cloud in major drawback in cloud computing**.** A structured encryption system encrypts structured data in such a way that it can be queried through the use of a query exact token that can only be created with knowledge of the secret key. In addition, the query procedure reveals no useful information about either the query or the data. An essential consideration in this perspective is the efficiency of the query operation on the server side. Actually, in the context of cloud storage, where one often works with large datasets, even linear time operations can be insufficient.

VI. Future Enhancement

In the future work us going to give more efficiency and security over the cloud data by other techniques called format preserving encryption. Format-Preserving Encryption (FPE) is a fundamentally new approach to encrypting structured data, such as credit card or Social Security numbers. FPE makes it possible to integrate data-level encryption into legacy business application frameworks that were previously difficult or impossible to address. It uses a published encryption method with an existing, proven algorithm to encrypt data in a way that does not alter the data format. The result is a strong encryption scheme that allows for encryption with minimal modifications to the way that existing applications work. This encryption method is used for more reliable access in the public cloud. For addition here we also concrete on authorization by using the biometrics of authorized user identification. Even though encryption is strong the processing time is less for that involving the high performance computing concept for speed transformation of dates.

VII. Conclusion

In this paper, we define and solved the problem of homomorphic cryptography on cloud data. Among various encryption techniques we choose the fully homomorphic encryption to avoid the leakage. The most common use of the encryption is to provide confidentiality by hiding all useful information about the plaintext. A search encryption technique has losses the data structure. So the data owner does not able to query efficiently. By using the fully homomorphic encryption can able to minimize the data losses during encryption and transferring the encryption. From this encryption can be more strong when compare to the homomorphic encryption the fully homomorphic encryption gives better result on the encryption. It reduces the data losses on the decryption of the data user from the cloud server. This encryption technique is efficient and complex for hacking so it gives the relevant data to data user and security over the cloud.

References

[1] L.M. vaquror, L.RoderoMerino, J. Caceres and M.Linder, “A breaking the cloud: towards a cloud definition,” ACMSIGOM comput comm.. Rev.Vol. 39,no.1, pp.50-55,2009.

[2] S.Kamar and K.Lauter, “Crypotographic cloud storage,” in RLCPS, LNCS, springer, Heidelberg, january 2010.

[3] D.song, D.Wangner and A.Perrig, “Practical technique for search on encryption data,” in proc.of s&p, 2000.

[4] E.J Goh, “Secure indexes Cryptology,” eprint archive, 2003.

[5] Y-C chang and M. Mitzemacher, “Privacy preserving keyword searches on remote encrypted data,” in proc of ACNS, 2005.

[6] R.Cutmola, J.A. Grarcy, S.Kamara and Rostroustrogy, “Searchable symmetric encryption: Improved definition and efficient construction,” in proc.of ACMCCS, 2006.

[7] S.G. Akl and P.D. Taylor, “Cryptographic Solution to a Multi Level Security Problem,” in Advances Cryptology CRYPTO, 1982.

[8] A. Beimel, “Secure Schemes for Secret Sharing and Key Distribution,” PhD thesis, Israel.

[9] E. Shen, E. Shi, and B. Waters, “Predicate privacy in encryption systems,” in Proc. of TCC, 2009.

[10] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proc. of ICDCS’10, 2010.

[11] Zhifeng Xiao and Yang Xiao, “Security and Privacy in cloud computing”, IEEE Communications surveys & Tutorials, 2013.

[12] Ren, K., Wang, C., & Wang, Q, “Security Challenges for the Public Cloud,” IEEE Internet Computing, 16(1), pp. 69-73, 2012.

[13] Catteddu, D.Hogben, G eds, “Cloud Computing - Benefits, risks and recommendations for information security,” European Network and Information Security Agency (ENISA), 2009.

[14] Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S.Raghu, H. Raghav Rao, “The Information Assurance Practices of Cloud Computing Vendors,” IT Pro, In IEEE Computer Society, pp. 29-37, 2010.

[15] D. Oliveira, F. Baião, and M. Mattoso, 2010, "Towards Taxonomy for Cloud Computing from an e-Science Perspective," Cloud Computing: Principles, Systems and Applications (to be published), Heidelberg: Springer-Verlag.

[16] http://www.vormetric.com/products/encryption/cloud-encryption.