SECURE EFFICIENT ENCRYPTED DATA SEARCH IN CLOUD

ALMAS SAFIA KAUSER[1]| AMTUL SHANAZ[2] | DR.SYED UDDIN[3]

[1](Dept of cse, Deccan College of Engineering & Tech,Hyderabad,India,almas_safia2002@yahoo.com),
[2](Dept of cse, Deccan College of Engineering & Tech, Hyderabad, India,amtulshanaz@deccancollege.ac.in)
[3](dept of cse Deccan College of Engineering & Tech, Hyderabad, India,hod_cse@deccancollege.ac.in)

Abstract**—** Storage of documents in cloud has gaining more popularity. However for security issues data has beenencrypted in cloud. Encrypted data should be effectively searchable and retrievable without any privacy leak. In this paper we are proposing a method to execute operations on encrypted data without decrypting them; this will provide the same results after calculations as if we have worked directly on the raw data. The vendor uploads the document in the mobile cloud environment. The user has to send the specific keyword related to the document that the user is searched for. Here we use Homomorphic Encryption algorithm for encryption because it reduces the search time. The vendor uses homomorphic Encryption algorithm for uploading and searching the document in the cloud. This scheme reduces search time delay and highly secure when compared to traditional schemes.

Keywords—Encrypted search;Homomorphic Encryption;Mobile Cloud.

1. INTRODUCTION

Cloud computing refers to the delivery of computing resources over the Internet .Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications.

In other words Cloud Computing is the use of computing resources that are delivered as a service over a network." So, you push your data to the cloud then tell the cloud what computation to perform. The cloud computes the result and sends the answer back to you. Hence the data can be accessed from any remote location via internet. However doing so may give rise to certain privacy implications. As Cloud is not trusted.

The cloud might acts maliciously so this is the reason the data provider encrypts the data before uploading them to cloud. When user needs to query certain documents they first send the search request.EnDAS[1] stores a pre-computed Trapdoor Mapping Table (TMT) in mobile devices, Which Maps common English words to corresponding trapdoors(encrypted keyword). Trapdoor mapping table stores the information needed for mapping and search, the heavy computation for generating trapdoors is not needed to be conducted online. However, it is inevitable that the trapdoors of some keywords have not been stored in the trapdoor mapping table in advance. In this case, the keyword is encrypted by the user. Then the newly retrieved or generated pure trapdoor is added with some noises from a noise set, to prevent the cloud from examining the same trapdoors. The Trapdoor is sent to cloud by users to get the requested document. The cloud then uses that trapdoor to search the requested document by using Ranked Serial Binary Search Algorithm. Ranked serial binary search is a different approach to finding a particular record. The idea is that you divide all the records into two, a top half and a bottom half. You then test to see which half the record you want is in. Whichever half it isn't in, you discards. So you are now left with only half of the original records. You then split that half into two and repeat the process, until you eventually find the record you want. Finally, the user receives these encrypted search results and uses the private key from the provider to decrypt documents.

This study focuses on security and search time inefficiency issues over mobile cloud. We present an Efficient Data Search in Cloud Using Homomorphic Encryption scheme to tackle this problem. Our system uses the Homomorphic Encryption to reduce the search time delay and to secure the data in cloud.

2. PROBLEM STATEMENT

In this section, we briefly introduce the existing ENDAS architecture [1] and outline their short comings.

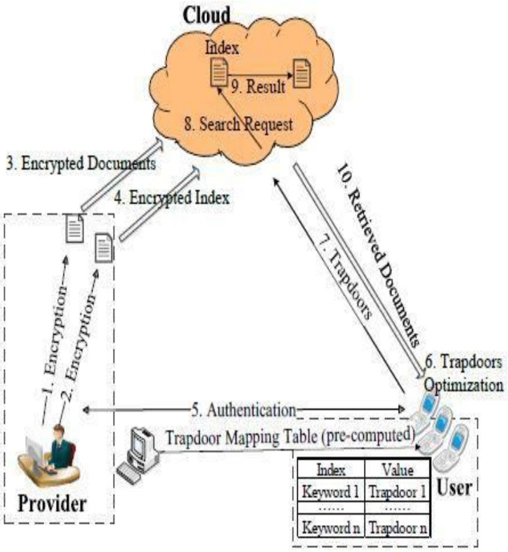

Figure 1.Efficient Encrypted Data search as a mobile cloud service

2.1 ENDAS:

As shown in (figure 1), the efficient data search in cloud using Homomorphic Encryption is composed of three different participants, Vendor, Cloud and User, which are defined below.

The Vendor possesses a set of documents. It intends to outsource these to the cloud and let users contact the cloud for the search service. The Cloud is a commercial organization that provides computation and storage resources in the form of virtual machines, commonly known as “cloud” services. The User is someone who submits keywords to search documents that contain these keywords. In our scenario, users would use mobile device such as smartphones and tablets to submit search requests.

Figure 1 details the execution flow of aENDAS, including the three main flows: Indexing the document Uploading Process (steps 1 to 4), trapdoor generation process (steps 5 to 7) and document retrieval process (steps 8 to 10).

2.2. Indexing the document Uploading Process:

The provider encrypts the document and uploads it over cloud. The encryption algorithm used to encrypt the documents is symmetric key encryption algorithm .It is the encryption method in which both the sender and receiver share the same key. In symmetric key cryptography [15], the algorithm used for decryption is the inverse of the algorithm used for encryption. This means that if the encryption algorithm uses a combination of addition and multiplication, the decryption algorithm uses a combination of division and subtraction. They are named so, since the same key is used for both encryption as well as decryption.

2.3. Trapdoor Generation Process:

To get the document from cloud the user needs authentication from cloud. When the user sends the search request, which refers to trapdoor mapping table to get the trapdoor. Trapdoor is the encrypted keyword. Trapdoor mapping table stores the information needed for mapping and search, the heavy computation for generating trapdoors is not needed to be conducted online. However, it is inevitable that the trapdoors of some keywords have not been stored in the trapdoor mapping table in advance. In this case, the keyword is encrypted by the user.

2.4. Document Retrieval Process:

In this process user sends the trapdoor to get the search result. The cloud uses Ranked Serial Binary Search Algorithm to search the requested document. Ranked serial binary search [11] is a different approach to finding a particular record. The idea is that you divide all the records into two, a top half and a bottom half. You then test to see which half the record you want is in. Whichever half it isn’t in, you discards. So you are now left with only half of the original records. You then split that half into two and repeat the process, until you eventually find the record you Want. Finally, the user receives this encrypted search results and uses the private key from the provider to decrypt documents.

3. PROPOSED SYSTEM

This section introduces the design of the Efficient Data search in cloud using Homomorphic Encryption. As compared to Endas system, this system 1) speeds up the search time, as it eliminates the reference to trapdoor mapping table to get a trapdoor for sending a search request to cloud. Instead of trapdoor ,the keyword is directly sent to the cloud 2)Usage of the Homomorphic Encryption Algorithm not only encrypts and searches the document but also provides security to the data in the cloud.

3.1 Architecture:

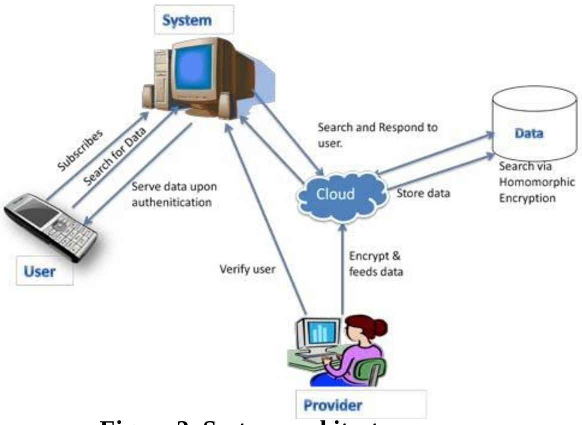

Figure 2. System architecture

Above figure shows the search flow of Efficient Data search in cloud using Homomorphic Encryption system. It contains the two main flows: Document Uploading Process and Document Retrieval Process.

3.1. Document Uploading Process:

First the provider uploads the encrypted data in the cloud. The Homomorphic Encryption algorithm is used to encrypt the document in the Cloud. Homomorphic encryption [9]is a form of encryption that Allows computations to be carried out on cipher text, thus Generating an encrypted result which, when decrypted, Matches the result of operations performed On Theplaintext. This is sometimes a desirable feature In Modern communication system Architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried Out the calculation on the raw data. The user then sends the search keyword to the cloud.

3.2 Document Retrieval Process:

The cloud uses the Homomorphic encryption algorithm to perform the computation in the encrypteddocument. The cloud then retrieves the results, the list of documents which matches the search keyword. The requested document will be downloaded only when the user provides the valid private key from the provider. The private key will be generated from the provider to the user by using Advanced Encryption Standard (AES).AES is a symmetric block cipher and is the most secure encryption algorithm available today. The authorized user will use his private key to download the requested document.

3.2 Homomorphic Encryption:

Acryptosystem that supports arbitrary Computation on cipher texts is known as fully homomorphic encryption [8] and is far more powerful. In Other words Homomorphic encryption is the conversion of data into cipher text that can be analyzed and worked with as if it were still in its original form. Such a scheme enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the result. Since such a program need never decrypt its inputs, it can be run by an untrusted party without revealing its inputs and internal state. The existence of an efficient and fully homomorphic cryptosystem [5] would have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing. Homomorphic encryption 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.

The utility of fully homomorphic encryption has been long recognized. The problem of constructing such a scheme was first proposed within a year of the development of RSA. A solution proved more elusive; for more than 30 years, it was unclear whether fully homomorphic encryption was even possible. During that period, partial results included the Boneh–Goh–Nissim cryptosystem that supports evaluation of an unlimited number of addition operations but at most one multiplication, and the Ishai-Paskin cryptosystem that supports evaluation of (polynomial-size) Branching program.Cloud computing fully safe. Therefore, Cloud computing security becomes the current research focus.

In order to solve the problem of data security in cloud computing system, by introducing fully homomorphism encryption algorithm in the cloud computing data security, a new kind of data security solution to the insecurity of the cloud computing is proposed and the scenarios of this application is hereafter constructed. This new security solution is fully fit for the processing and retrieval of the encrypted data, and security of data transmission and thestorage of the Cloud Computing.

With the rapid development of Cloud computing, more and more users deposit their data and application on the cloud. But the development of Cloud computing is hindered by many Cloud security problem. Cloud computing has many characteristics, e.g. multi- user, Virtualization, scalability and so on. Because of these new characteristics, traditional security technologies can't make.

4. PERFORMANCE EVALUATION:

The performance is tested based on different metrics.Algorithms are implemented using the following libraries.**System.Security.Cryptography :**Consist classes for implementing AES Encryption algorithm, Homomorphic Encryption **Scheme.System.Web.Security:**contains classes that are used to implement ASP.NET security in Web server applications.
System.Net.Mail : Consist classes for sending keys through mail.

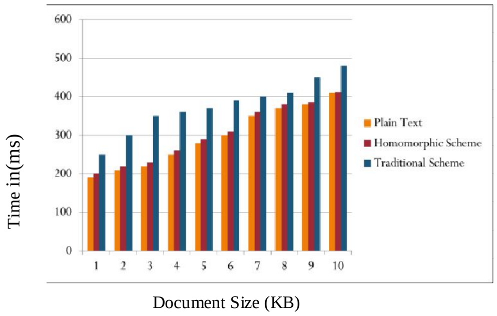

Figure 3.Analysis on Comparison of Plaintext, Homomorphic Scheme and Traditional Scheme

5. CONCLUSION:

In this paper we proposed an efficient data search in cloud using homomorphic encryption which reduces the search time delay and provides security. We analyzed the problem in Endas[1] and developed an efficient architecture of Efficient Data Search In Cloud Using Homomorphic Encryption. We have used homomorphic encryption algorithm to speed up the search and to provide security. Finally our evaluation study experimentally demonstrates the performance advantages of Efficient Data Search in Cloud Using Homomorphic Encryption.

REFERENCES

[1] Ruhui Ma, Jian Li, Haibing Guan, Mingyuan Xia and Xue Liu "**EnDA**S: Efficient Encrypted Data Search as a mobile Cloud Service," IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING,Jan.2015.

[2] J. Li, R. Ma, and H. Guan, "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Trans. Cloud Comput., Feb. 2015.

[3] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE

Trans. Parallel Distrib. Systems, vol. 23, no. 8, pp. 1467–1479, 2012

[4] C. ¨Orencik and E. Savas¸, “Efficient and secure ranked multikeyword search on encrypted cloud data,” in Proc. Joint EDBT/ICDT Workshops, Mar. 2012, pp. 186–195.

[5] C. Gentry and S. Halevi, “Implementing fully homomorphic encryption scheme,” in Advances in Cryptology– EUROCRYPT 2011, 2011, pp. 129–148.

[6] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2010, pp. 253–262.

[7] J. S. Culpepper, G. Navarro, S. J. Puglisi, and A. Turpin, “Top-k ranked document search in general text databases,” in Proc. Annu. Euro. Conf. Algorithms (ESA), Sep. 2010, pp. 194–205.

[8] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” in Advances in Cryptology-EUROCRYPT 2010, 2010, pp. 24–43.

[9] D.Stehl’e and R Steinfeld “Faster fully homomorphic encryption,”in Advances in Cryptology-ASIACRYPT 2010,pp.377-394.

[10] A.BoldyreyaN.Chenette,Y.Lee,and A.Oneill,”Order Preserving Symmetric encryption,” in Advances in Cryptology EUROCRYPT 2009, pp. 224-241.

[12] MsMayuraR.Grime,ProfG.M.Bhandari “Efficient secure Rankedkeyword search algorithm over outsourced cloud data” International Journal of Emerging Trends and Technology in Computer Science- Oct 13

[13] P.Wang,H.Wang,and J. Pieprzyk, “An efficient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data,” pp. 145–159, 2009.

[14] D.Boneh,G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology-Eurocrypt 2004, 2004, pp. 506–522.

[15] R.Agarwal,J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proc. ACM SIGMOD Int. Conf. Manag. Data (COMAD), Jun. 2004, pp. 563–574.

[16] R.Curtmola,J.Garay S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption:improved definitions and efficient con-Strucyions”in Proc. ACM Conf. Compute.Commun. Secure (CSS),Oct. 2006, pp. 79–88