ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Protection of Outsourced Data using remotely verifying integrity of regeneration codes approach in Cloud Computing.

Chinta Srinu
M.Tech (Software Engineering),
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Management.

Behara Vineela
Assistant Professor,
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Management.

Abstract:

A cloud refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources. The term originated as a metaphor for the Internet which is, in essence, a network of networks providing remote access to a set of decentralized IT resources. The moving of business data to the cloud means that the responsibility over data security becomes shared with the cloud provider. The remote usage of IT resources requires an expansion of trust boundaries by the cloud consumer to include the external cloud.

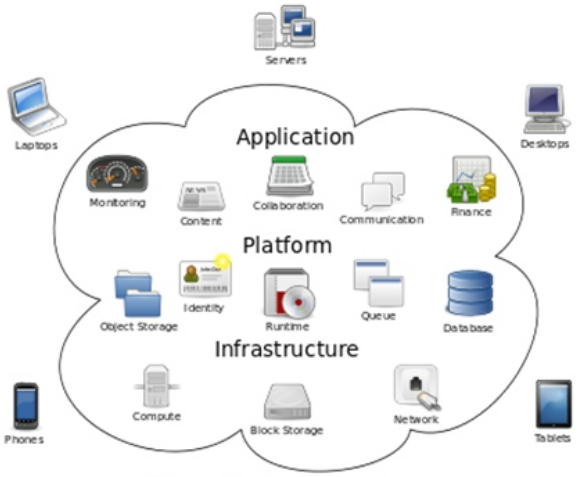
It can be difficult to establish a security architecture that spans such a trust boundary without introducing vulnerabilities, unless cloud consumers and cloud providers happen to support the same or compatible security frameworks - which is unlikely with public clouds. There are many searching operations that search the multiple keywords in the documents. In many traditional approaches searching on data server is professional. In this the data is very sensitive. So there is a use in sensitive data and protecting techniques. It supports only single or prediction keywords search. So we introduced a novel technique which searches multiple keywords search and those are to be converted using cryptographic algorithm. In our architecture is search performed based on the key words only. We group the keywords in the search by using clustering.

Keywords:

Cloud computing, Communications, Nodes, security, Data Integrity, searchable encryption, Ranked search.

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



Cloud Computing

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

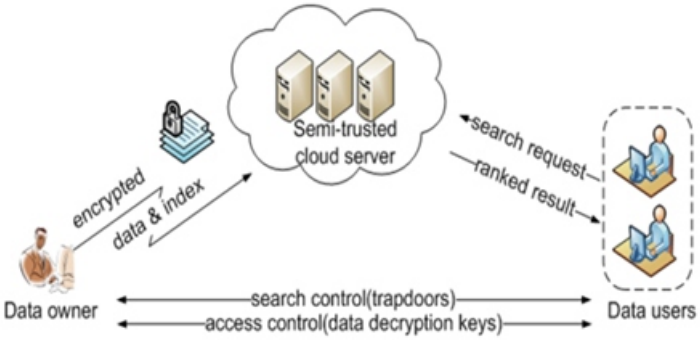
Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

To protect data privacy, confidential data has to be encrypted before outsourcing, so as to provide end-to-end data confidentiality assurance in the cloud. Data encryption makes effective data utilization a verychallenging task given that there could be a large amount of outsourced data files. Besides, in Cloud Computing, data owners may share their outsourced data with a large number of users, who might want to only retrieve certainspecific data files they are interested in during a given session. One of the most popular ways to do so is through keyword-based search.

This keyword search technique allows users to selectively retrieve files of interest and hasbeen widely applied in plaintext search scenarios. Unfortunately, data encryption, which restricts user's ability to perform keyword search and further demands the protection of keyword privacy, makes the traditionalplaintext search methods fail for encrypted cloud data. Ranked search greatly improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency).

Architecture:



Exiting System:

To protectdata privacy and combat unsolicited accesses in the cloudand beyond, sensitive data, for example, e-mails, personalhealth records, photo albums, tax documents, financialtransactions, and so on, may have to be encrypted by dataowners before outsourcing to the commercial public cloud; this, however, obsoletes the traditional data utilizationservice based on plaintext keyword search. The trivialsolution of downloading all the data and decrypting locallyis clearly impractical, due to the huge amount ofbandwidth cost in cloud scale systems.

Moreover, asidefrom eliminating the local storage management, storingdata into the cloud serves no purpose unless they can beeasily searched and utilized. Thus, exploring privacypreserving and effective search service over encryptedcloud data is of paramount importance.

Considering thepotentially large number of on-demand data users andhuge amount of outsourced data documents in the cloud,this problem is particularly challenging as it is extremelydifficult to meet also the requirements of performance,system usability, and scalability.

Disadvantages:

»Single-keyword search without ranking.

»Boolean- keyword search without ranking.

»Single-keyword search with ranking.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proposed System:

In our proposed work we generate strong cipher based on the crypto system of data after Genetic algorithm. Information security has become a very critical aspect of modern computing systems. With the global acceptance of the Internet, virtually every computer in the today is connected to every other.

So at this point of time maintaining of secrecy and security of information has become necessity. For these reasons different types of research works on encryption and decryption is going on so that various algorithm are developed in this field.

Advantage:

1. Multi-keyword ranked search over encrypted cloud data (MRSE)
2."Coordinate matching" by inner product similarity.

Encryption is a method that converts the plain text into non-readable one and Decryption is the method that converts the non-readable cipher text into readable plain text. Encryption is inversely proportional to Decryption. This algorithm combines the features of Genetic Functions and Cryptography. Here we generate random numbers with the help of genetic functions

"CROSSOVER" and "MUTATION". The algorithm contains a key of four parameters, for security.
KEY= {Seed Value (Xn), Modulus (m), Multiplier (a), Incrementer(c)}
Where, Xn, a, c, m is the parameters of the linear method, which are known to only sender and receiver. The proposed algorithm consists of two steps i.e. random number generator and encryption.

Linear Genetic algorithm adopts linear recursive method as shown below:

After generation 1, the numbers of the next generation is obtained by CROSSOVER followed by MUTATION. The pairing up of numbers is done first, with the concept that for odd type generation pairing is done in one way and for even type generation in the opposite way. For example, after the first generation we got the following numbers: -

333, 6578, 8614, 5959, 7922, 8837, 4440, 903, 3693, 2686.

2nd Generation: -

Pairing up: - (333, 6578), (8614, 5959), (7922, 8837), (4440, 903), (3693, 2686)
For this generation crossover and mutation will take place
let at 6th locus of the gene of chromosome.

CROSSOVER: -

Binary Representation of the first pair:
333 = 0000101001101
6578 = 1100110110010

Crossover:

0000100110010 1100111001101

MUTATION: -
Mutation:

0000110110010 1100101001101
= 434 =6577

Similarly, the other pairs can also be generated in the following way. Now after generating all the numbers by applying crossover and mutation on each pair we get; 434, 6577, 263,5798,8069,9202,4478,816,3646,2605 After the second generation we continue with the 3rd, 4thand 5th generation to generate 50 numbers (Eachgeneration 10 populations) and get the final set of numbers.

STEP-2 ENCRYPTION :

1. Once all the numbers are generated then let this array of numbers be called SUB_ARRAY and select the first digit of each number from SUB_ARRAY and a new collection of numbers is generated and let this collection is called

COLLECTION_ARRAY:

2. Use this numbers from COLLECTION_ARRAY sequentially for substituting on a one-to-one basis for the characters of the plain text.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

3. Use ASCII values of the plain text characters and subtract the numbers of COLLECTION_ARRAY from the ASCII values.

For example the message "SOUMYA" the CIPHER TEXT will be calculated according to following method.
LET SUB_ARRAY = {4167, 10117, 5602, 4867, 4307, 2452}

ENCRYPTION:-

Character ASCIIValue
Collection_Array
Number
Taken sequentially Subtract Result
S-> 83 4 83 - 4 79
O ->79 1 79 - 1 78
U ->85 5 85 - 5 80
M ->77 4 77 - 4 73
Y ->89 4 89 - 4 85
A ->65 2 65 - 2 63
The enciphered message is "RESULT"
The Cipher text is: {79, 78, 80, 73, 85, 63}

STEP-3 DECRYPTION :

3. Results and analysis
In this section the implementation of different types of files are presented. The text, executable and dynamic link libraries files are taken for experiments. This implementation has been done using high-level language.
79 83 -S
78 79 -O
80 85- U
73 77 -M
85 89 -Y
63 65 –A

MODULES:

1.Encrypt Module.

2.Client Module.

3.Multi-keyword Module.

4.Admin Module.

Encrypt Module:

This module is used to help the server to encrypt the document using RSA Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download.

Client Module:

This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail from the "customerservice404" email before enter the activation code. After user can download the Zip file and extract that file.

Multi-keyword Module:

This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list.

Admin Module:

This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart. The admin can upload the file after the conversion of the Zip file format.

CONCLUSION:

In this paper, surprisingly we characterize and tackle the issue of multi-magic word positioned inquiry over scrambled cloud information, and build an assortment of protection necessities. Among different multi-magic word semantics, we pick the productive comparability measure of "direction matching,"

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

i.e., as numerous matches as could reasonably be expected, to viably catch the significance of outsourced reports to the inquiry essential words, furthermore utilize "inward item comparability" to quantitatively assess such similitude measure. For gathering the test of supporting multi-decisive word semantic without security ruptures, we propose a fundamental thought of MRSE utilizing secure inward item reckoning.

References:

[1] Ning Cao, Member, IEEE, Cong Wang, Member, IEEE, Ming Li, Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014.

[2] Weifeng Su, Jiying Wang, and Frederick H. Lochovsky, Member, IEEE Computer Society Record Matching over Query Results from Multiple Web Databases.

[3] Y.Srikanth,M.VeereshBabu, P.Narasimhulu Combined Keyword Search over Encrypted Cloud Data Providing Security and Confidentiality .

[4] Cong Wang†, Ning Cao‡, Jin Li†, KuiRen†, and Wenjing Lou‡ †Department of ECE, Illinois Institute of Technology, Chicago, IL 60616 ‡Department of ECE, Worcester Polytechnic Institute, Worcester, MA 01609 Secure Ranked Keyword Search over Encrypted Cloud Data .

[5] A. Singhal, Modern information retrieval: A brief overview, IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 3543, 2001.

[6] R. Ananthakrishna, S. Chaudhuri, and V. Ganti, Eliminating Fuzzy Duplicates in DataWarehouses, Proc. 28th Intl Conf. Very Large Data Bases, pp. 586-597, 2002.

[7] R. Baeza-Yates and B. Ribeiro-Neto, Modern Information Retrieval. ACM Press,1999.

[8] I. H. Witten, A. Moffat, and T. C. Bell, Managing gigabytes: Compressing and indexing documents and images, Morgan Kaufmann Publishing, San Francisco, May 1999.

[9] E.-J. Goh, Secure indexes, Cryptology ePrint Archive, 2003, http://eprint.iacr.org/2003/216.

[10] D. Song, D. Wagner, and A. Perrig, —Practical techniques for searches on encrypted data, in Proc. of IEEE Symposium on Security and Privacy'00, 2000.

[11] E.-J. Goh, —Secure indexes, Cryptology ePrint Archive, Report 2003/216, 2003, http://eprint.iacr.org/.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, —Public key encryption with keyword search, in Proc. of EUROCRYP'04, volume 3027 of LNCS. Springer, 2004.

[13] Y.-C. Chang and M. Mitzenmacher, —Privacy preserving keyword searches on remote encrypted data, in Proc. of ACNS'05, 2005.

[14] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, —Searchable symmetric encryption: improved definitions andefficient constructions, in Proc. of ACM CCS'06, 2006.

Author Details :

ChintaSrinu
is a Student in M.Tech(SE) in Sarada Institute of Science Technology And Management, Srikakulam. HeReceived his B.Tech(CSE) from Sarada Instituteof Science Technology And Management(SISTAM), Srikakulam. JNTU Kakinada Andhra Pradesh.His interesting areas are Network,data mining.

BeharaVineela
is working as Asst.professorin Sarada Institute of Science, TechnologyAnd Management,Srikakulam, Andhra Pradesh. He received his M.Tech (CSE)from AITAM ,Tekkali,Srikakulam, AndhraPradesh. JNTU Kakinada Andhra Pradesh.His research areas include Network Security