A Privacy Preserving Data Search Scheme in Cloud Computing

Padamati Harika Prasanna1, CH Ramadevi[2]

[1]*M.Tech Scholar, Computer Science & Technology, Sir C.R.R College of Engineering, Andhra Pradesh, India*

[2]*Assistant Professor, Sir C.R.R College of Engineering, Andhra Pradesh, India*

Abstract—Cloud computing is a promising IT procedure that can sort out a lot of IT assets in a productive and adaptable way. Progressively various organizations intend to move their neighborhood information the board frameworks to the cloud and store and deal with their item data on cloud servers. A going with challenge is the means by which to ensure the security of the economically private information while keeping up the capacity to look through the information. In this paper, a security protecting information search conspire is suggested that can bolster both the identifier-based and include based item look. In particular, two novel list trees are developed and encoded that can be looked without knowing the plaintext information. Examination and reproduction results show the security and proficiency of our plan.

Keywords: *Cloud computing; information security.*

I. INTRODUCTION

Driven by the upheaval of data innovation as of late and with the stoppage in the monetary development, there is a critical need to change China's whole modern chain. To advance an overall mechanical redesigning, China has proposed the methodology of "Web +", and the coordination of China's web based business with its conventional economy has been essentially improved. Internet business has quickened its extension from utilization to different ventures and penetrated all parts of social and financial exercises, in this way driving the advancement of big business level web based business, both in scope and top to bottom, and encouraging the change and redesigning of endeavors. The Monitoring Report on the Data of China's Ecommerce Market [1] shows that in 2016, the volume of internet business exchanges in China arrived at around 3.5 trillion dollars, a year-on-year development pace of roughly 25.5%. The quickly rising number of digital exchanges has produced online business huge information.

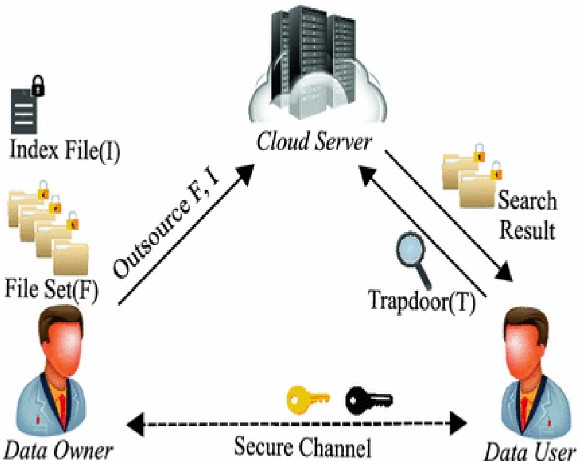


Fig.1: Multi keyword fuzzy search

As progressively various information records are being put away locally in undertakings, the weight on nearby information stockpiling frameworks incredibly increments. Neighborhood equipment disappointments lead to incredible harm or loss of information, which enormously influences the day by day tasks of the undertakings. Luckily, distributed storage procedures appeared under such conditions. Distributed computing can gather and sort out an enormous number of various kinds of capacity gadgets by methods for different capacities, for example, group applications, organize innovation and disseminated document frameworks. There have just been various normal cloud administration items at home and abroad, for example, Amazon.

II. RELATED WORK

Secure Conjunctive Keyword Search Over Encrypted Data [1]

We characterize a security model for conjunctive watchword search over scrambled information and present the primary plans for directing such quests safely. We propose initial a plan for which the correspondence cost is straight in the quantity of records, however that cost can be brought about "disconnected" before the conjunctive question is inquired. The security of this plan depends on the Decisional Diffie-Hellman (DDH) suspicion. We propose a second plan whose correspondence cost is on the request for the quantity of catchphrase fields and whose security depends on another hardness supposition.

Practical Techniques for Searches on Encrypted Data [2]

In this paper, we depict our cryptographic plans for the issue of looking on encoded information and give verifications of security to the subsequent crypto frameworks. Our strategies have various critical favorable circumstances. They are provably secure: they give provable mystery to encryption, as in the untrusted server can't get the hang of anything about the plaintext when just given the ciphertext; they give inquiry separation to look, implying that the untrusted server can't get the hang of much else about the plaintext than the query item; they give controlled looking, so that the untrusted server can't scan for a discretionary word without the client's approval; they additionally bolster shrouded inquiries, so the client may approach the untrusted server to look for a mystery word without uncovering the word to the server. The calculations we present are straightforward, quick (for an archive of length n, the encryption and search calculations just need O(n) stream figure and square figure activities), and present basically no space and correspondence overhead, and henceforth are reasonable to utilize today.

III. FRAMEWORK

In this paper, we center around the second and third sorts of information and structure a protected and productive information search conspire. For comfort, a reasonable foundation is introduced as follows. We initially expect that every item has a one of a kind identifier in the entire organization and a point by point portrayal record. The document incorporates the entirety of the point by point data of the item, for example, the structure stream, plan standard, item highlights and market position. As we as a whole know, propelling the item to the market sooner than the contender can possess the market rapidly and advantage the organization impressively. As a result, the entirety of the data ought to be kept from the contenders and people in general, taking into account that the items are time-touchy.

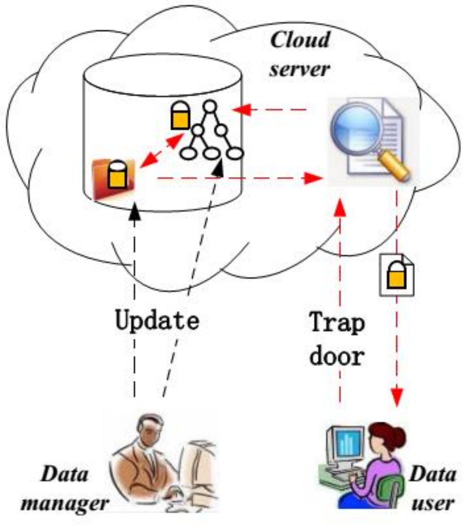


Fig.2:System Architecture

Modules:

1. Data Manager:

The data manager is responsible for managing the product and collecting the product information. In addition, the data manager needs to encrypt the product information file by a symmetric encryption technique before outsourcing the data to the cloud server.

2. Data user:

When a data user wants to search a set of chosen products, she needs to generate a trapdoor to describe her interest. Two types of the trapdoor can be provided, i.e., a set of hash values of the desired product information files or a set of feature vectors.

3.Cloud server:

The cloud server stores all the data uploaded by the data manager. When a data user needs to search the data in the cloud, she first generates a trapdoor, which is sent to the cloud server. A search engineer is employed by the cloud server to act as a bridge between the data users and the encrypted data.

KNN Algorithm:

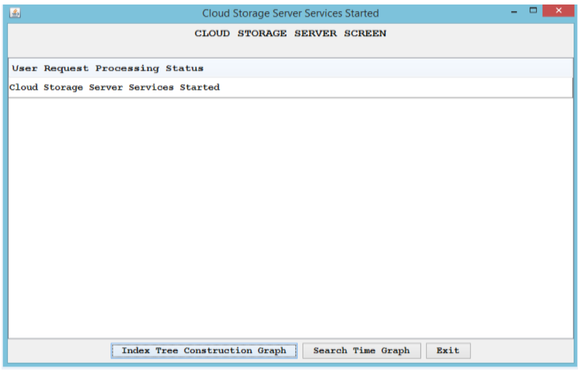
KNN otherwise called K-closest neighbor is an administered and example grouping learning calculation which causes us discover which class the new input(test esteem) has a place with when k closest neighbors are picked and separation is determined between them.

IV. EXPERIMENTAL RESULTS

To look through the ideal item data, the information client needs to initially create the trapdoor, which is sent to the cloud server. The hours of developing the trapdoors with the expanding of the size of the component word reference are introduced. The pursuit demands dependent on the identifiers are free of the component word reference, and subsequently, the hour of building the trapdoors for the IDAVL tree stays stable. Notwithstanding, the development time of the trapdoors for the MRSE and PRF trees tediously increment with the expanding of the component word reference's size. This is sensible thinking about that the size of the item highlight vector is equivalent to the size of the component word reference. Also, the time costs for the MRSE and PRF trees are like each other in light of the fact that the procedures of creating the trapdoors are comparable.

Extension:

In this project as extension we added cache temporary memory algorithm which will cache all previous search result and if user issue same query in future then cache will fetch result from memory and serve to user instead of rerunning entire algorithm. By applying this algorithm we can reduce execution time and save resources



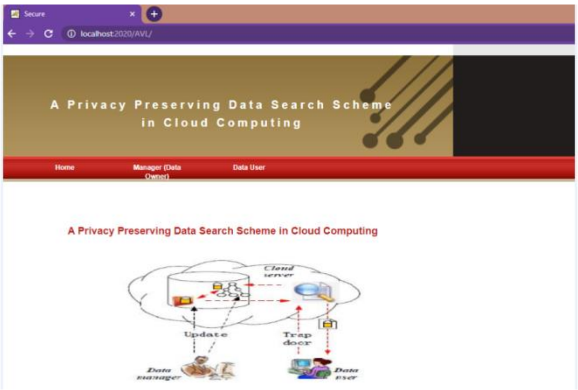
Cloud Storage Server Services Started

CLOUD STORAGE SERVER SCREEN

User Request Processing Status

Cloud Storage Server Services Started

Fig.3: Cloud storage server screen



A Privacy Preserving Data Search Scheme in Cloud Computing

A Privacy Preserving Data Search Scheme in Cloud Computing

Fig.4: Home Screen

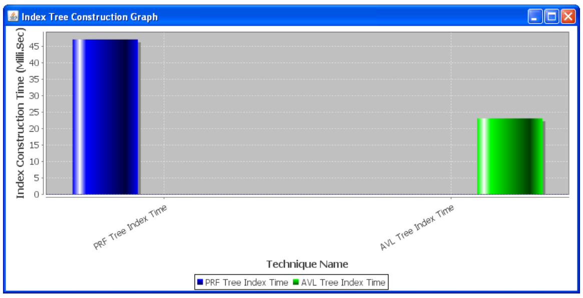


Fig.5: Index tree construction graph

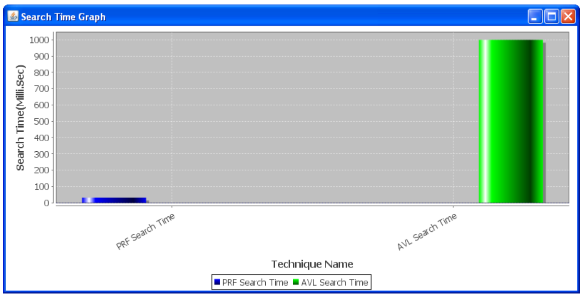


Fig.6: Search time graph

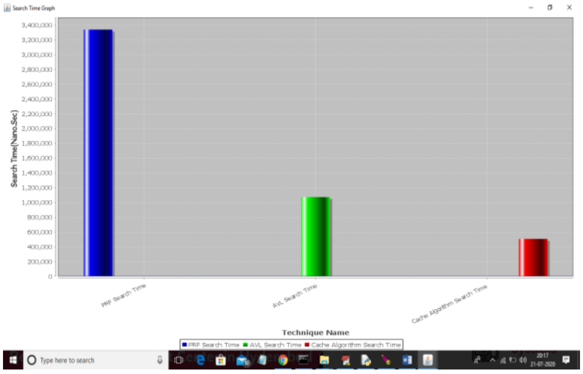


Fig.7: Extension search graph

V. CONCLUSION

In this paper, we planned a safe and proficient item data recovery plot dependent on distributed computing. In particular, two file structures, including a hash esteem AVL tree and an item vector recovery tree, are built, and they bolster an identifier-based item search and highlight vector-based item search, individually. Correspondingly, two pursuit calculations are intended to look through the two trees. To secure the item data protection, all the re-appropriated information are scrambled. The item data is evenly scrambled dependent on a lot of free mystery keys, and the item vectors are encoded dependent on the safe kNN calculation. Security investigation and reenactment results show the security and productivity of the proposed plot.

REFERENCES

[1] www.100EC.cn. 2016 Monitoring Report on the Data of China's Ecommerce Market [EB/OL]. http://www.100ec.cn/zt/16jcbg/,2017- 05-24

[2] Amazon. Amazon S3. http://aws.amazon.com/s3/

[3] Windows azure. http://www.microsoft.com/windowsazure/

[4] Apple i Cloud. http://www.icloud.com/

[5] Google App Engine. http://appengine.google.com/

[6] GolleP.StaddonJ,Waters B. Secure Conjunctive Keyword Search over Data[C]. Springer, 2004.

[7] Song D X,WangerD.Perrig A. Practical Techniques for Searched on Encrypted Data[C].IEEE,2000.

[8] Boneh D,Di Crescenzo G,Ostrovsky R. et al. Public Key Encryption with Keyword Search: EUROCRYPT[C].Springer,2004.

[9] Rhee H S.Park J K,Susilo W. et al. Trapdoor Security in A Searchable Public-Key Encryption Scheme with A Designated Tester[J].Journal of Systems and Software,2010,83(5):763-771

[10] Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." IEEE Internet Computing 16.1 (2012): 69-73.

[11] M Krishna, N Deepak and B Yamini, Alignment Establish Representative Data Uploading and Private Data Principle Test in Cloud, International Journal of Research in Electronics and Computer Engineering (IJRECE), pp: 132-135, Vol.5, Issue.4, Oct-2017.