International Journal of Science Engineering and Advance Technology (IJSEAT)
ISSN 2321-6905, Vol. 8, Issue 4, April -2020

A new method for secure kNN algorithm to guarantee the security of the outsourced data maintaining its searchability

[1]V.Srinivas, [2]Mrs.P.RadhikaKrupalini
[1]Final year ,M.Sc(CS), Dept. of Computer Science, Ideal College of Arts & Sciences,Kakinada,AP,India
[2]Associate Professor of Computer Science, Ideal College of Arts & Sciences, Kakinada,AP, india

ABSTRACT:
Distributed computing is a promising IT framework that can make a ton out of IT resources in a profitable and versatile manner. Continuously different associations plan to move their close by information the board systems to the cloud and store and manage their item information on cloud servers. A going with challenge is the way to guarantee the security of the monetarily mystery information while keeping up the capacity to look through the information. In this paper, a security protecting information search plan is suggested that can support both the identifier-based and include based item look. Specifically, two novel rundown trees are created and encoded that can be looked without knowing the plaintext information.

KEYWORDS: cloud computing; data security

1] INTRODUCTION:

Driven by the turmoil of information advancement starting late and with the respite in the money related turn of events, there is a basic need to change China's entire mechanical chain. To propel an all around mechanical refreshing, China has proposed the arrangement of "Web +", and the blend of China's web business with its standard economy has been on a very basic level improved. Web based business has animated its augmentation from use to various endeavors and infiltrated all pieces of social and money related activities, along these lines driving the improvement of enormous business level online business, both in degree and start to finish, and empowering the change and refreshing of attempts. The Monitoring Report on the Data of China's Ecommerce Market [1] shows that in 2016, the volume of online business trades in China showed up at around 3.5 trillion dollars, a year-on-year improvement pace of generally 25.5%. [2,8]

The rapidly rising number of advanced trades has delivered online business huge information. As continuously different information records are being taken care of locally in attempts, the weight on close by information accumulating systems altogether increases. Neighborhood hardware dissatisfactions lead to mind blowing damage or loss of information, which uncommonly impacts the regular errands of the undertakings. Fortunately, distributed storage frameworks showed up under such conditions[9,10].

2] LITERATURE SURVEY:

Wang cong et al [15] described and deal with the troublesome issue of protection saving multi-watchword positioned search over encoded information in distributed computing (MRSE). We develop a great deal of demanding insurance requirements for such a sheltered cloud information use structure. Among various multi-watchword semantics, we pick the compelling likeness extent of "encourage planning," i.e., anyway numerous matches as would be judicious, to get the hugeness of information documents to the request question. We further use "internal item resemblance" to quantitatively survey such similarity measure. We at first propose a principal thought for the MRSE subject to make sure about internal item calculation, and a short time later give two basically improved MRSE plans to achieve distinctive rigid insurance necessities in two various hazard models.

Rhee et al[9] organized a safe distributed storage administration which keeps an eye on the trustworthiness issue with close perfect all things considered execution. By allowing an untouchable to play out the open genuineness affirmation, information owners are on a very basic level released from the awkward work of once in a while checking information uprightness. To thoroughly free the information owner from the heaviness of being on the web after information re-appropriating, this paper proposes an exact fix game plan with the objective that no metadata ought to be created on the fly for fixed information.

3] PROBLEM DEFINTION:

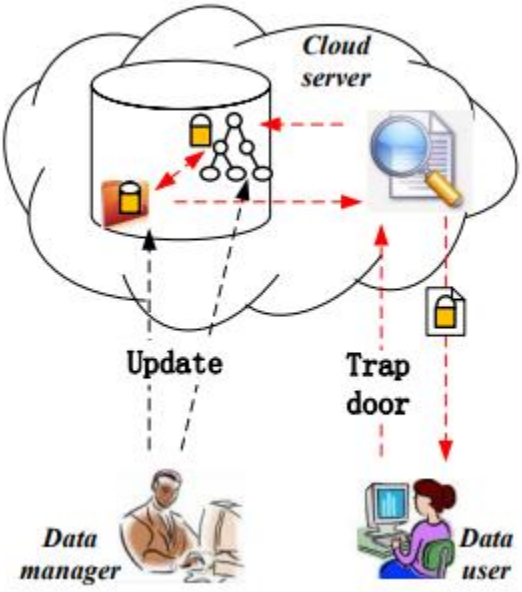
Have a couple of focal points, for instance, accommodation and cost saving, and they are commonly used in various fields. In any case, a couple of troubles are connected with them. With the extending reputation of distributed storage, security issues have become a critical factor restricting its

new development. Starting late, information spillage mishaps have more than once occurred in such associations as Microsoft, Google, Amazon, and China's Home Inn, Hanting, and Ctrip, and these scenes have exacerbated customers' concerns[11,12].

4] PROPOSED APPROACH:

The information administrator, the cloud server and the information customer. The basic obligations of these three components are presented in the going with. The information executive is at risk for managing the item and social event the item information. Additionally, the information director needs to scramble the item information record by a symmetric encryption technique before re-appropriating the information to the cloud server. To improve the security of the reports, each record is mixed by a singular secret key, and the keys of different records are independent[13].

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

6.1] Data Owner

This encourages the proprietor to enlist those subtleties and furthermore incorporate login subtleties. This module encourages the proprietor to transfer his document with encryption utilizing RSA calculation. This guarantees the records to be shielded from unapproved client.

6.2] Data User

This incorporates the client enrollment login subtleties. This module is utilized to assist the customer with searching the document utilizing the numerous catchphrases idea and get the exact outcome list dependent on the client question. The client will choose the necessary record and register the client subtleties and get initiation code in mail email before enter the enactment code. After client can download the Zip document and concentrate that file[15].

6.3] Encryption

This is utilized to assist the server with encrypting the report utilizing RSA Algorithm and to change over the scrambled record to the Zip document with initiation code and afterward actuation code send to the client for download[14].

6.4] Rank Search

These guarantee the client to look through the documents that are looked through much of the time utilizing rank pursuit. This module permits the client to download the document utilizing his mystery key to unscramble the downloaded information. This module permits the Owner to see the transferred documents and downloaded records

7] ALGORITHM:

Step 1: u=r ;

Step 2: **while** u is not a leaf node

Step 3: Calculate all the relevance scores between the child nodes of with V_Q

Step 4: u the most relevant child node;

Step 5: end while

Step 6: Select the most relevant k document vectors in u by RScore(V ,V) and construct $RList$;

Step 7: $Stack$ push(r);

Step 8: **while** $Stack$ is not empty

Step 9: u =$Stack$ pop (r);

Step 10: **if** the node u is not a leaf node

Step 11: Sort the child nodes of u in ascending order based on the relevant scores with V ;

Step 12: Push the children of u into $Stack$ in order, i.e., the most relevant child is latest inserted into $Stack$;

Step 13: else

Step 14: break;

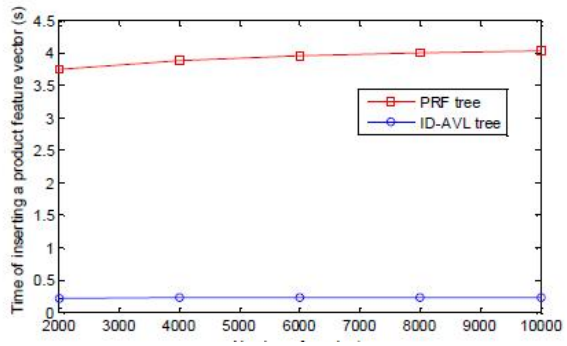
Step 15: end if

Step 16: else

Step 17: Calculate the relevance scores between the document vectors in the leaf node with V and update $RList$;

Step 18: end if

8] RESULTS:



Time consumption of inserting a node into the trees

9] CONCLUSION:

We arranged a secured and powerful item information recuperation plot dependent on distributed computing. Specifically, two record structures, including a hash regard AVL tree and an item vector recuperation tree, are created, and they support an identifier-based item search and feature vector-based item search, separately. Correspondingly, two chase calculations are expected to glance through the two trees. To make sure about the item information insurance, all the re-appropriated information are encoded. The item information is equitably encoded reliant on a great deal of free riddle keys, and the item vectors are scrambled dependent on the safe kNN calculation.

10] EXTENSION WORK:

Security analysis and efficiency of the proposed scheme will be increased.

11] 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 S
[3] 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] Golle P.Staddon J,Waters B. Secure Conjunctive Keyword Search over Data[C]. Springer, 2004.
[7] Song D X,Wanger D.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] Song, Dawn Xiaoding, David Wagner, and Adrian Perrig. "Practical techniques for searches on encrypted data." Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000.
[12] Goh, Eu-Jin. "Secure indexes." IACR Cryptology ePrint Archive 2003 (2003): 216.
[13] Curtmola, Reza, et al. "Searchable symmetric encryption: improved definitions and efficient constructions." Journal of Computer Security 19.5 (2011): 895-934
[14] Swaminathan, Ashwin, et al. "Confidentiality-preserving rankordered search." Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007.

[15] Wang, Cong, et al. "Enabling secure and efficient ranked keyword search over outsourced cloud data." IEEE Transactions on parallel and cloud systems 23.8 (2012):
1467-1479.

Mr.V.Srinivas is a student of Ideal College of Art & Science, Kakinada Presently he is pursuing his M.Sc(Computer Science) from this college and he received his BSc (Computer Science) from Ideal college of Art & Science, affiliated to AKNU University, Kakinada in the year 2017 His areas of interest includes Computer Networks and Object Oriented Programming

languages, all current trends and techniques in Computer Science.

Mrs.P.Radhikakrupalini is an Associate Professor of Computer Science Department at Ideal College of Arts & Sciences, Kakinada, AP, INDIA. She obtained her MCA from Andhra University, M.Tech (CSE) from University College of Engineering, JNTUK. She qualified AP SET in Computer Science and Applications. She has 14+ years of teaching experience at Post Graduate Level. Her areas of interest are Operating Systems, Network Security & Cryptography, Artificial Intelligence, Cloud computing, Data Mining and Software Engineering.