Secure K-NN Query on Encrypted Cloud Data with Multiple Keys

R. Vignesh¹ D. Deepa² Suja Cherukullath Mana³ B.Keerthi Samhitha⁴
[¹,²,³,⁴] Assistant Professor³ Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology.

Vignesh.star975@gmail.com,Deepa.cse@sathyabama.ac.in,suja@gmail.com,keerthi.cse@sathyabama.ac.in,

Abstract: Cloud computing has become an undeniably famous assistance for its adaptability and versatility, which rouses numerous associations, foundations and organizations to want to reappropriate data administrations to cloud stage. Simultaneously, much consideration has been paid to adapt to the extraordinary security and protection issues in recloud cloud. The general methodology is to scramble data by the data owner (DO) before re-appropriating; the approved query user play out an unpredictable arrangement of encryption and decoding tasks during question execution. In any case, the above plans have accepted that the question clients are completely trusted and have the entrance to the key for scrambling and unscrambling recloud data. It will achieve a few issues in reality. So we propose a novel plan for secure KNN inquiry on encoded cloud data with various keys, in which the data owner and each question client all hold their own various keys, and don't impart them to one another; in the interim, the data owner scrambles and decodes re-appropriated data utilizing the key of his own. Our plan is built by set of conventions to jelly the data classification and question over scrambled cloud data without key-sharing.

1. Introduction

Cloud framework and adaptability persuade establishments and people to re-appropriate their data to cloud servers. Data owners re-appropriate the data to cloud server, these data can be gotten to by data owner or verified clients by questioning on cloud data. Notwithstanding, the protection and privacy worries of data regularly make them hesitant. To protect the data security and classification, re-appropriated data is scrambled by data owner before redistributing them to the cloud. In this way the data in cloud server stockpiling accessible will be protected. Be that as it may, since data has been encoded in the cloud, it deters the current strategy on using data dependent on plain content watchword looking through system. Along these lines, it is important to propose a productive plan to acquire encoded data from the cloud server is significant for re-appropriating capacity applications. Existing systems believes the clients to be real, be that as it may, it is hard to accept such in many situations. In this way secure and a productive plan to be proposed for data recovery. Essentially, existing procedures managed single watchword question over scrambled data the work in [15] improves the ASPE conspire in [8] to take care of the issue without imparting key to inquiry clients. Rather, question clients connect with the data owner to determine an inquiry encryption.
That is, these plans require data owner to be continually on the web. Zhu et al. [16] of late propose an improvement of the plan in [15], which can bolster the disconnected data owner. Nonetheless, these plans unveil pretty much data about data owner's critical.

All the more critically, the bit of the works [15], [16] is the ASPE technique, however the ASPE strategy can't be demonstrated to oppose the picked plaintext assault (CPA) [9]. The work in [17] likewise gives a protected NN (k = 1) inquiry conspire which can oppose the conspiracy between cloud server and question clients. In any case, the work isn't commonsensical on account of the solid suspicion. Right now, the above issues, we center around the safe k-NN question over encoded cloud data without key-sharing. Right off the bat, in view of the conveyed two trapdoors open key cryptosystem (DT-PKC) [18], we develop a lot of conventions of secure two-party calculation that will be utilized as sub-schedules of our proposed conspire. Moreover, we propose a novel secure k-NN plot with different keys to address the above issues. In particular, in our plan, each question client holds his own disconnected key and the data owner can encode and decode re-appropriated data utilizing the key of his own, without offering the way in to the inquiry clients. Note that, our plan is anything but a straightforward use of the safe two-party calculation strategies. Indeed, these unique conventions that we proposed are one of the remarkable commitments. To our best data, this is the principal work that reviews secure k-NN inquiry on encoded data with different keys.

Our plan not just jelly the data classification and question protection yet in addition bolsters the disconnected data owner. In view of the property of numerous keys, we can altogether tackle the issues initiated by key-offering to question clients. 2) We present a lot of novel conventions of secure twoparty calculation dependent on dispersed two trapdoors open key cryptosystem, which become a foundation of our protected k-NN plot. In our framework, each inquiry client holds his own inconsequential key and the data owner can scramble and decode recloud data utilizing the key of his own, without offering the way in to the question clients. Right now give data classification and furthermore support the disconnected data owner. In view of the property of various keys, we can completely take care of the issues actuated by key-imparting to inquiry clients. In our framework by and large inquiry clients have restricted calculation and correspondence assets, our strategy ought to be intended for lessening the clients overhand and countless question clients are engaged with the framework, along these lines supporting disconnected data owner is very vital as far as the framework's adaptability.

2.Related Work

Wong et al.[1], they characterize their work for knearest neighbor (kNN) inquiry calculation on an encoded database. Existing procedures don't bolster database inquiries on the scrambled data. Right now, considered SCONEDB, to execute security and protection on cloud storage administrations. Their intention is to change private data and inquiries in to an encoded database. It likewise manages the unscrambling of the scrambled inquiries without uncovering the data by the specialist organization's end. They proposed a protected plan called topsy-turvy scalar-item safeguarding encryption (ASPE), which bolsters kNN calculation on encoded data. The accompanying section expresses a way to deal with study different assaults types. "One way to deal with safely support kNN is to utilize separation safeguarding change (DPT) to scramble data focuses [27] so the separation between any two encoded focuses in E(DB) is equivalent to that between the comparing unique focuses in DB." J. Oberheide, Veeraraghavan et al [2] proposed the capacity level security of versatile cloud stockpiles. A model is proposed, in which portable antivirus usefulness is
moved to an off-gadget arrange administration utilizing numerous virtualized malware discovery motors. In his work, they moved discovery capacities to a system administration.

Along these lines each document is investigated by different recognition motors. Anjanadevi et al [3] proposed, which examines the ordering and meta data the board which assists with getting to the dispersed data with diminished inertness. The metadata the executives can be refreshed for huge scope document framework applications. Capacity area of the metadata and traits is dealt with viably for productive data recovery. Records are utilized to rapidly find data without looking over each area away, consequently data can be handily recovered from huge document framework and the pursuit time (inquiry inertness) was decreased. Right now, utilized record parting calculation to partition documents into pieces and meta list creation calculation to make file for put away lumps.

3. Existing System

In a current key sharing framework we expect that the inquiry clients are completely trusted and know the key of the data owner. The data owner redistributes his data and inquiry usefulness to the cloud where just believed clients are permitted to question the host data. So as to conquer the imperfections of key-sharing plan, another safe plan with key classification. This work utilized a symmetric plan with a mystery lattice change as a key, and question clients don't share this key. Rather, they interface with the data owner to determine an inquiry encryption without uncovering the question. This implies the data owners need to stay online for all the clients.

4. Problem Statement

Cloud stage can absolutely break the re-appropriated database once the key is gotten from any undermined inquiry client. Once question clients get the key, their inquiry handling won't be constrained by data owner any more, and it is hard to disavow the entrance even they are considered to be deceitful.

5. Proposed System

Fig 1. Overview of the Proposed System
In our proposed framework we propose a novel secure KNN inquiry over encoded cloud data without key-sharing. In our framework, each question client holds his own inconsequential key and the data owner can scramble and unscramble re-appropriated data utilizing the key of his own, without offering the way in to the inquiry clients. Right now give data classification and furthermore support the disconnected data owner. In view of the property of numerous keys, we can completely take care of the issues prompted by key-imparting to inquiry clients. In our framework for the most part question clients have constrained calculation and correspondence assets, our strategy ought to be intended for lessening the clients overhand and an enormous number of inquiry clients are engaged with the framework, in this manner supporting disconnected data owner is very fundamental regarding the framework's versatility.

6. Modules Description

6.1 Domain Creation

Right now can make various areas and produce the watchwords for the specific space and store the total area subtleties into server, presently client can make a record and become a part. When they made record data owner can transfer the document in server.

6.2 File Upload And Key Generation

The data owner can pick the sort of class before transfer the document into our application. We have diverse sort of watchwords dependent on the class so data owner guarantee the couple of explicit catchphrase while he transfer the document. It would contrast for different classifications the key will be created dependent on the particular catchphrases, at that point the transferred document is encoded by utilizing the key. The encoded document will be put away in the cloud dependent on the gathering into HDFS (Hadoop Data File System).

6.3 File Search And Providing Public Parameter

Right now will get to the record which is transferred in server by utilizing watchwords. In the server document will be in encoded position, so client needs to give the particular catchphrases at whatever point they need to get to the record. Our cloud administration document framework will keep track the whole record dependent on the gathering just as explicit watchwords, if client given catchphrase is coordinated with document server will give open parameter to the client then they can get to record.

6.4 File Download

Right now client will download the record utilizing catchphrase based looking through procedure. In view of watchword open parameters will be given by the server and now client will change the key by utilizing open parameters given by the server, here open parameter will be vary dependent on client catchphrases. When the client change the key utilizing open parameters appropriately then the record will be unscrambled utilizing the improved key, at that point client can download the whole document from HDFS (Hadoop Data File System).
7. Conclusion

Right now, centered around the issue of supporting k-NN question over encoded cloud data while the data owner can't impart his key to inquiry clients. For this we proposed another arrangement with multiple keys to take care of the key sharing issues thoroughly. Hence we proposed and created secure watchword based inquiry over encoded data without key sharing between data owner and client. The majority of the current techniques on data recovery slacks under security issue as these works considered cloud client to be constantly authentic. While in our proposed model, Secure K-NN recovery over encoded data is considered.

References

[1] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, “Secure knn computation on encrypted databases,” in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. ACM, 2009, pp. 139–152.

[2] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized in-cloud security services for mobile devices,” in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[3] S. Anjanadevi, D. Vijayakumar, Dr. K. G. Srinivasagan, "An Efficient Dynamic Indexing and Metadata Based Storage in Cloud Environment", 2014 International Conference on Recent Trends in Data Technology.

[4] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” Parallel and Cloud Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[5] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Cloud Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 253–262.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” Parallel and Cloud Systems, IEEE Transactions on, vol. 23, no. 1, pp. 222–233, 2014.

[7] B. Yao, F. Li, and X. Xiao, “Secure nearest neighbor revisited,” in Data Engineering (ICDE), 2013 IEEE 29th International Conference on. IEEE, 2013, pp. 733–744.

[8] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in 2014 IEEE 30th International Conference on Data Engineering. IEEE, 2014, pp. 664–675.

[9] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, “Twinclouds: An architecture for secure cloud computing,” in Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.

[10] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 223–238.

[11] H. L’ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium. ACM, 2010, pp. 220–229.
[12] J. Zhou, Z. Cao, X. Dong, and X. Lin, “Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multilevel privacy-preserving e-healthcare cloud computing systems,” in 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015, pp. 2398–2406.

[13] Y. Zhu, Z. Huang, and T. Takagi, “Secure and controllable k-nn query over encrypted cloud data with key confidentiality,” Journal of Parallel and Cloud Computing, vol. 89, pp. 1–12, 2016.

[14] Y. Zhu, Z. Wang, and Y. Zhang, “Secure k-nn query on encrypted cloud data with limited keydisclosure and offline data owner,” in Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, 2016, pp. 401–414.

[15] K. Cheng, L. Wang, and H. Zhong, “Secure nearest neighbor query on crowd-sensing data,” Sensors, vol. 16, no. 10, p. 1545, 2016.

[16] X. Liu, R. H. Deng, K. K. R. Choo, and J. Weng, “An efficient privacy-preserving outsourced calculation toolkit with multiple keys,” IEEE Transactions on Data Forensics and Security, vol. 11, no. 11, pp. 2401–2414, 2016.

[17] O. Goldreich, “The foundations of cryptography, vol. 2, chapter general cryptographic protocols,”

[18] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in INFOCOM, 2014 Proceedings IEEE.

[19] J. Zobel and A. Moffat, “Inverted files for text search engines,” ACM Computing Surveys (CSUR), vol. 38, no. 2, p. 6, 2006.

[20] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[21] R. Vignesh, D. Deepa, P. Anitha, S. Divya and S. Roobini, “Dynamic Enforcement of Causal Consistency for a Geo-replicated Cloud Storage System”, International Journal of Electrical Engineering and Technology, 11(3), 2020, pp. 181-

[22] R. Vignesh, K. Mohana Prasad, “Cloud-Implementation of E-Healthcare Framework”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019.

[23] Divya.S., R. Vignesh., Revathy, R.”A Distinctive Model to Classify Tumor Using Random Forest Classifier” , Proceedings of the 3rd International Conference on Inventive Systems and Control, ICISC 2019.
[24] Vignesh Ramamoorthy, S. Divya, Suja Cherukullapurath Mana and B. Keerthi Samhitha, “Examining and Sensing of Artificial Knee with Multi Sensors Networks”, Journal of Advanced Research in Dynamical and Control Systems (JARDCS), 10(4), 115-120.

[25] Deepa D, R. Vignesh, Sivasangari A, Suja Cherukullapurath Mana, B. Keerthi Samhitha and Jithina Jose, Visualizing Road Damage by Monitoring System in Cloud. International Journal of Electrical Engineering and Technology, 11(4), 2020, pp. 191-203

[26] Jithina Jose, Suja Cherukullapurath Mana, B. Keerthi Samhitha, “An Efficient System to Predict and Analyze Stock Data using Hadoop Techniques”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019

[27] Ishwarya, M.V., Deepa, D., Hemalatha, S., Nynesh, A.V.S., Tej, A.P.,” Gridlock surveillance and management system” 16(8):3281-3284, Journal of Computational and Theoretical Nanoscience, August 2019.

[28] Samhitha, B.K., Mana, S.C., Jose, J., Mohith, M., Siva Chandrahasa Reddy, L. (2019)” An efficient implementation of a method to detect sybil attacks in vehicular adhoc networks using received signal strength indicator”, International Journal of Innovative Technology and Exploring Engineering, (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November

[29] Mana, S.C., Samhitha, B.K., Jose, J., Swaroop, M.V., Reddy, P.C.K. (2019) “Traffic violation detection using principal component analysis and viola jones algorithms "International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September

[30] Mana, S.C., Sasipraba, T. (2019) “Highly parallel map reduce process and efficient job scheduling methodologies of big data systems” International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-9 Issue-1, November