International Journal of Science Engineering and Advance Technology

A New Mechanism to Search Cipher text Data in Cloud in Fog Computing

[1]G.Ramya Sri, [2]P.Radhika Krupalini
[1]Final year student MSc(CS), [2]Associate Professor
[1,2]Dept. of Computer Science, Ideal College of Art & Sciences, Kakinada, A.P., India.

ABSTRACT:

We first present a Lightweight Fine-Grained Ciphertext Search (LFGS) system in mist processing by expanding Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Searchable Encryption (SE) innovations, which can accomplish fine-grained access control and keyword search all the while. The LFGS can move fractional computational and capacity overhead from end clients to picked mist nodes. Besides, the fundamental LFGS system is improved to help conjunctive keyword search and attribute update to abstain from returning immaterial query items and illicit gets. The formal security examination demonstrates that the LFGS system can oppose Chosen-Keyword Attack (CKA) and Chosen-Plaintext Attack (CPA), and the recreation. Utilizing a genuine world dataset shows that the LFGS system is effective and possible, practically speaking.

KEYWORDS: Searchable Encryption, Attribute Update, Decryption

1] INTRODUCTION:

The promising distributed computing [1] worldview can provide on-request administrations with flexible assets and enable cloud customers to soothe the high stockpiling and computation costs [2] locally. In any case, the pervasiveness of Internet of Things (IoT) applications [3] represents an immense test to the brought together distributed computing worldview which incurs unbearable transmission inertness and corrupted administrations between user demands and cloud reactions. Moreover, large amounts of information created from the IoT applications are often put away in the cloud. To diminish inactivity and network congestion, a haze registering worldview [4] which is an extension of distributed computing administrations to organize edge has been a generally late research point. In haze computing, the haze nodes embedded into the center of cloud and end users (or IoT gadgets) can give different administrations (i.e., data computation, information stockpiling, and so on.) for asset restricted end users (i.e., sensor nodes, portable terminals, and so forth.), note that fog nodes are a lot nearer to end clients than cloud, which is shown in Fig. 1. At the point when touchy information(i.e. content, picture, video, and so on.) [5], [6], [7] are redistributed to legit however inquisitive fog nodes which are like open cloud stage, the data security and security concerns [8] still obstruct the adoption of haze registering as information proprietors lose the physical control over their information in haze nodes or cloud.

2] LITERATURE SURVEY:

[1] Y. Yangwe present a novel cryptographic crude named as Conjunctive Keyword Seek with Assigned Analyzer and Timing Empowered Intermediary Reencryption work (Re-dtPECK), which is a sort of a period subordinate SE scheme. It could empower patients to designate fractional access rights to others to work seek works over their documents in a constrained time span. The length of the time span for the delegatee to search and decode the delegator's encrypted documents can be controlled. Also, the delegatee could be naturally denied of the entrance and search expert after a predetermined time of successful time. It can likewise bolster the conjunctive watchwords hunt and oppose the keyword speculating assaults. By the arrangement, just the assigned analyzer can test the presence of specific watchwords. We figure a system demonstrate and a security display for the proposed Re-dtPECK plan to demonstrate that it is a productive plan demonstrated secure in the standard model. The examination and broad reproductions show that it has a low algorithm and capacity overhead.

[2]H. Li,we build up the accessible encryption for multi-keyword positioned search over the capacity information. In particular, by thinking about the extensive number of redistributed documents (information) in the cloud, we use the pertinence

score and k-closest neighbor procedures to build up a productive multi-watchword search scheme that can restore the positioned query items dependent on the exactness. Inside this structure, we influence a productive list to additionally improve the search proficiency, and receive the visually impaired capacity system to disguise get to example of the pursuit client. Security examination exhibits that our plan can accomplish secrecy of documents and list, trapdoor protection, trapdoor unlink ability, and hiding access example of the pursuit client.

3] PROBLEM DEFINTION:

In distributed computing condition, SE gives a key answer for issue seek inquiries over encrypted information as indicated by determined watchwords. Tune et al. [13] gave the principal SE scheme which required litter correspondence; however the computational overhead was direct in the measure of pursuit search. To handle this issue, Boneh et al. [14] exhibited a Public key Encryption with Keyword Search (PEKS) scheme. From that point onward, numerous SE plans enhanced with various highlights had been proposed, for example, single watchword seek, different keywords search, fluffy key word search, obvious keyword seek, positioned watchword seek.

Contrasted and single keyword search [23], [24], different watchword seek [25], [26] can rapidly find the aftereffects of intrigue and incredibly decline the misuse of algorithm and transfer speed assets. As there is no resilience of minor kinds and configuration irregularities in definite watchword search questions, fluffy keyword seek [27] improves the system ease of use by utilizing Wildcard, Locality-Sensitive Hashing (LSH) or Bloom Filter (BL) methods. As the cloud is a semi confided in outsider which will execute a small amount of hunt activities and return a small amount of query items to spare algorithm assets or shroud information debasement mishaps, irrefutable watchword search [28] can confirm whether the outcomes are right or not. To additionally limit the indexed lists, positioned watchword search [29], [30] can restore the outcomes in the request of pertinence scores to keywords.

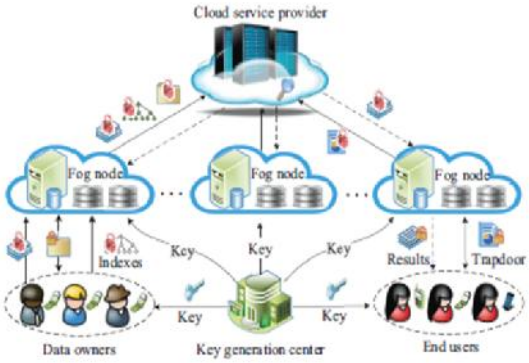
4] PROPOSED APPROACH:

In the proposed system, the system expect that KGC is a completely confided in substance, while the CSP and FNs are straightforward however inquisitive outsiders which genuinely execute the pre-characterized conventions yet are interested to conclude delicate data from put away ciphertexts and trapdoors, which can enable them to obtain extra data. Contingent upon what data the CSP and FNs know, we receive the accompanying two danger models [29]. The pernicious EUs may connive with one another to get to unapproved ciphertexts, though EUs can't scheme with FNs in LFGS system.

Known figure content model. In this model, the CSP and FNs can acquire the encoded documents, documents and trapdoors.

Realized foundation show. In this more grounded model, the CSP and FNs should have more learning (i.e., connection relationship of given trapdoors, dataset related measurable data, and so forth.) than that in the known figure content model.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

Data Owner

The information proprietor performs activities, for example, Upload, View All Your Files, Check Remote Data Integrity

User

He signs in by utilizing his/her client name and secret phrase. After Login recipient will perform tasks like Request Sk, Search Data By Keyword, Download

Key Generation Centre

The area can do following tasks View Request and Generate Key, View Transactions

Fog Node

The division can do following tasks View Request and Authorize PKC, View Transactions

Cloud Server

The Cloud Server deals with a server to give information stockpiling administration and can likewise do the accompanying tasks, for example, View Data Owners, View End Users, and View All Cloud Files, View all Transactions, View All

Attackers, View Results, View Time Delay Results, and View Throughput Results

7] ALGORITHM NOTATIONS:

U = System attribute set
PKFN, PKEU Public keys of FNs and EUs
K1, K2, K3 FN's secret key
K0 EU's secret key
F = File set
W = Keyword set
Kt=Encryption key of F
CT Intermediate ciphertext of k
It Index of F
TW′ =Trapdoor for keyword

FINE GRAINED SEARCH ALGORITHM:

INPUT: U, PKFN, PKEU, K1,F,W, CT,TW

STEP1: DO first sends the access policy to the chosen FN.
STEP2: FN returns the encrypted access policy described by a access tree to DO, outputs the final ciphertexts.
STEP3: file content ciphertexts, file key ciphertexts and index ciphertexts, returns to CSP via the chosen FN.
STEP4: KGC generates the secret keys for the EU and his chosen FN according to his attributes.
STEP5: After gaining his secret key, the EU sends his attributes to the chosen FN, and the FN outputs the Intermediate trapdoor.
STEP6: EU further generates the intermediate trapdoor and sends it to the FN.
STEP7: the FN outputs the final trapdoor and returns it to CSP.
STEP8: the CSP issues the search operation and returns the relevant search results to the FN.
STEP9: FN first conducts the majority of operations and then returns the intermediate results to the EU.
STEP10: the EU decrypts the ciphertexts without high computational and storage burden.

8] RESULTS:

Data Owner upload file

End User Request file with Secret key

9] CONCLUSION:

We exhibited a Lightweight Fine-Grained Search (LFGS) system for the asset constrained EUs in mist registering. From one perspective, the essential LFGS system could enormously lessen the computational and capacity weight of EUs by re-appropriating incomplete algorithm and capacity to the legitimate however inquisitive FNs without releasing delicate data; then again, the all-inclusive LFGS system could bolster conjunctive watchword pursuit and attribute update to additionally limit the hunt scope and dodge unapproved gets to, individually. Besides, the formal security investigation demonstrated that the LFGS system is specifically secure against CKA and CPA, and the exact examinations utilizing a genuine world dataset represented the proficiency and practicality of LFGS system in fog computing.

10] REFERENCES:

[1] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine grained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, 2017.

[2] H. Yan, J. Li, J. Han, and Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 78–88, 2017.

[3] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of iot and cloud computing," Future Generation Computer Systems, vol. 78, pp. 964–975, 2018.

[4] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog–cloud computing," Future

Generation Computer Systems, vol. 78, pp. 825–837, 2018.

[5] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," Future Generation Computer Systems, 2017.

[6] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," IEEE Internet of Things Journal, 2017.

[7] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution," IEEE Transactions on Multimedia, vol. 19, no. 8, pp. 1908–1920, 2017.

[8] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based iot: challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.

[9] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'11). Springer, 2001, pp. 213–229.

[10] F. Guo, Y. Mu, W. Susilo, H. Hsing, D. S. Wong, and V. Varadharajan, "Optimized identity-based encryption from bilinear pairing for lightweight devices," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 2, pp. 211–220, 2017.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM conference on Computer and Communications Security (CCS'06). ACM, 2006, pp. 89–98.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symposium on Security and Privacy (S&P'07). IEEE, 2007, pp. 321–334.

[13] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (S&P'00). IEEE, 2000, pp. 44–55.

[14] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT'04), vol. 3027. Springer, 2004, pp. 506–522.

[15] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute based keyword search over outsourced encrypted data," in Proc. IEEE Conference on Computer Communications (INFOCOM'14). IEEE, 2014, pp. 522–530.

G.Ramya Sri is a student of P.G. Department of Computer Science in Ideal College of Arts and Sciences, Kakinada. Presently she is in final year Master of Science(Computer Science) in this college and affiliated to Adikavi Nannaya University, Rajamhendravaram, Andhra Pradesh. She received her B.Sc(CS) from P.R. Government(Autonomous) college, Kakinada in the year 2017. Her areas of interests include Data Mining, Cloud Computing, Web Designing and all current trends and techniques in Computer Science.

Ms. P. Radhika Krupalini is presently working as Associate Professor in P.G. Department of Computer Science, Ideal College of Arts and Sciences, Kakinada. 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 13+ years of teaching experience at Post Graduate Level. Her areas of interests are Cloud Computing, Big Data, Network Security and Cryptography, Operating Systems and Artificial Intelligence.