Secure and Efficient Attribute Based Encryption and Keyword Search in Public Cloud for Multi Owner Access

Bukya Ravindra Naik
M. Tech, Department of CSE, JNTUACE
Anantapur, India

S. Vasundra
Professor, Department of CSE,
Anantapur, India

Abstract

The framework develops a novel protection saving hunt convention, which permits the cloud worker to play out a productive secure multi-catchphrase positioned search without knowing information proprietors' delicate data and each property is encoding and will be put away in the public cloud. The framework performs broad examinations to assess the proficiency of the ABKS-SM plot on a genuine real time data and accomplish a log details hunt time. To accomplish an effective hunt, for every information proprietor, Attribute based encryption with an added substance request and security safeguarding capacity is built and afterward an encoded information will be put away in the public cloud.

Index Terms: -*Multi keyword Search, Attribute Based Encryption, security, secure storage, shared multi-owner setting.*

I. INTRODUCTION

Distributed Cloud computing has become another registering worldview. Presently, an expanding number of people and endeavors are creating a tremendous measure of information regular. It is not, at this point financially achievable to keep up their own equipment and staffs for information the executives. As of late, a sensible and famous decision to relieve the weight of information the executives are to redistribute the mind-boggling information the board undertaking to the cloud with the significant advantage of cost investment funds. One may have worry that the cloud can't generally be believed; it might intentionally and unsolicited analyze the re-appropriated information. To maintain the benefit of cost reserve funds and secure the information protection, the information, before moved operations to the cloud, should be encoded. Notwithstanding the achievement in picking up the information protection, information encryption doesn't permit the cloud to answer the clients' questions on the information. A direct answer for the client to defeat such a trouble is to just download the whole informational index. This, be that as it may, is for all intents and purposes infeasible in view of the colossal volume of the acquired data transmission utilization.

The issue of recovering data from the scrambled documents has just been testing. With regards to re-appropriated cloud information, the issue is even disturbed by an enormous number of on-request clients and a colossal measure of redistributed information documents. Accordingly, with the given contemplations, it is incredibly hard to meet the prerequisites of both recovery attainability and framework execution.

In the current use, text information that can be seen wherever would be the one conveying most of data. A significant technique for recovering data on the content information is the watchword search, in which just the content records containing the particular catchphrases are gotten back to the client. Be that as it may, perhaps because of the absence of the records totally coordinating the information catchphrases, the watchword search may restore an unfilled outcome. In this sense, the client normally goes to look for the comparative outcome. Here, the comparative outcome could be the documents containing part of info catchphrases or containing the words like the information watchwords. Such comparable catchphrase search can discover various applications, for example, record linkage and natural information base. Because of its capacity in upgrading framework convenience and generally client experience, the examination on the comparative watchword search has been directed broadly. Lamentably, a large portion of them is considered without security and protection concerns. In any case, just a couple of exploration endeavors on comparable catchphrase search are done under the imperative of scrambled writings.

II. EXISITING WORK

The multi-watchword positioned search permits clients to include various inquiry catchphrases for customized inquiries. In [9], Cao [3] et al. proposed the main secure multi-catchphrase positioned search plot over scrambled cloud information (MRSE), and the reports are positioned by the "internal item" between file vectors and question vectors. Nonetheless, they don't think about the heaviness of various catchphrases. Vasundara by [4][6] advanced the multi-watchword [4] search.

- Wang et al. [1], Chuah and Hu [7] proposed multi-watchword fluffy pursuit plot focused on the resistance of both slight grammatical errors and configuration irregularities for clients' information. Zhang et al. [12] proposed a safe positioned multi watchword search conspire in a multi-proprietor model (PRMSM) that not just permits the cloud worker to play out a multi catchphrase search without knowing any touchy data, yet in addition empower the information proprietor to deftly change the encryption key. In any case, these plans infrequently center around inquiry effectiveness.

- Practically, question proficiency is one of the most significant markers of the client experience. Wang and Vasundara [11] proposed a safe hunt plot dependent on the tree-based record, which can effectively perform look. Be that as it may, it is planned uniquely for a solitary watchword search.

- Later, Xu et al. [5], [11] introduced a productive multi-watchword positioned search plot (MKQE) that empowered a powerful catchphrase word reference and improved the exactness of the hunt. Sun et al. [16] made a protection saving multi-catchphrase text search [4] conspire. They isolated the vector list into different layers and proposed a tree-based file structure by applying the MD-calculation [10] that acknowledged more proficient pursuit usefulness, yet bringing about lost accuracy.

- Liu et al. [2] developed a tree-based record structure and proposed a covetous profundity first inquiry (GDFS) calculation that accomplished higher pursuit effectiveness. Tragically, these works don't consider various information proprietors' situation. Dong et al. [15] considered a reasonable situation where various clients share information through an untrusted outsider.

- Vasundara [6] To actualize it, the creators proposed a novel multi-client accessible information encryption plot dependent on intermediary cryptography. Unique in relation to the current accessible encryption conspires, their plan permitted the clients to refresh the mutual informational index and every client can be per user and essayist all the while. Moreover, the rigorous confirmation had been spoken to demonstrate the security of their plan.

- Chen and Wang et al. [10] zeroed in on web applications and proposed another stage Mylar which is a blend of framework strategies and novel cryptographic natives, including information sharing, processing over encoded information and confirming application code. The outcomes with 6 applications indicated that Mylar is a decent multi-client web application with information sharing.

□ Li et al. [13] proposed a safe and successful Near-copy identification (NDD) framework over scrambled in-network stockpiling which upheld multi-client and multi-key accessible encryption. [14] Nonetheless, those plans can't comprehend the multi-catchphrase positioned search issue in the multi-client setting.

DISADVANTAGES

- The cloud has to give unique key for each file encryption which will be more computational cost.
- Data users need to generate multiple trapdoors for data owners' data even for the same query condition.

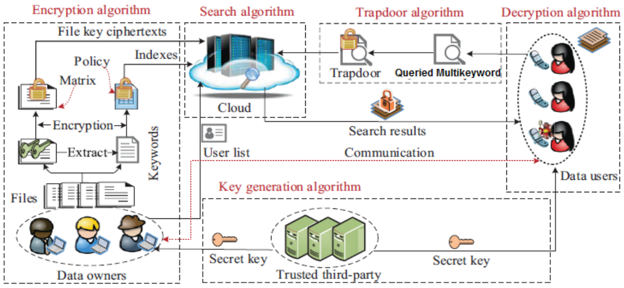
III. PROPOSED WORK

In the proposed work, the framework considers a multi-source cloud framework, in which every information proprietor (saw as a source) creates a trait-based encryption for his/her information records and encodes this information with his/her relating key. To actualize both protection safeguarding and proficiency look, we propose an effective Attribute based positioned multi-catchphrase search plot. In this plan, the cloud worker is permitted to successfully consolidate various encoded credits, and safely play out the multi-catchphrase search without uncovering the information proprietors' delicate data, neither information documents nor the questions. We develop a novel hunt convention dependent on bilinear matching, which empowers diverse information proprietors to utilize various keys to scramble their catchphrases and hidden entrances.

ADVANTAGES

- ❖ The system is more effective due to present of attribute based multi keyword search.
- ❖ The system is more efficiency due to presence of efficient search by keyword and Multi Owner Data Access.

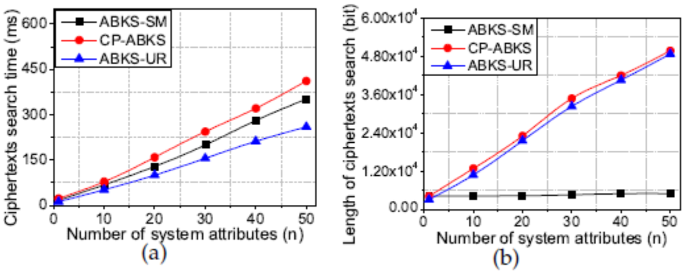
IV. ARCHITECTURE



We additionally present the design of fundamental ABKS-SM framework Above Fig. The Setup calculation plays out the framework instatement, for example, producing the public keys and ace keys. The Key generation calculation incorporates Key generation Data Owner and Key-GenDUsub algorithms, which produce public/mystery key sets for various Data Owners and Data Users, individually. Concerning Enc calculation, various Data Owners first concentrate watchwords from the records before yielding the document key ciphertexts and encoded lists, by utilizing LSSS and access strategy separately. In Trap calculation, a Data User presents the hidden entrance created by his/her questioned watchword to Cloud Service Provider. From that point onward, the Cloud Service Provider conducts Search calculation and sends the approved list items to Data User. Before decoding the scrambled query items in Dec calculation, Data User requires to get the significant approvals by associating with

Data Owners, which is appeared by the red spotted line in the above Fig. In the wake of being certified by different Data Owners, Data Users gets the plaintext results.

V. Results



(a)

(b)

In Above Fig. (a) and (b) shows the calculation and capacity costs for Multi Keyword Search calculation, separately. For data search time, the fundamental ABKS-SM framework needs to direct extra matching activities nP, dissimilar to the ABKS-UR plot. As the CP-ABKS acquires extra exponentiation tasks .NET, the computational expense of essential ABKS-SM framework is more than that of ABKS-UR, however it is somewhat not as much as that of CP-ABKS. When setting n = 30, the essential ABKS-SM framework takes 200 ms to perform figure text search activity, and both CP-ABKS and ABKS-UR plans require 244 ms and 156 ms, individually. For Multi key word Search calculation, the capacity cost of essential ABKS-SM framework remains practically unaltered while the capacity expenses of CP-ABKS and ABKSUR plans increment directly with the quantity of framework ascribes (n). For instance, when n = 50, the capacity cost of the ABKS-SM framework is 0.61 KB, and those of the CP-ABKS and ABKS-UR plans are 6.57 KB and 6.69 KB, separately.

VI. CONCLUSION

The measure of information created by people and undertakings is quickly expanding. With the rising distributed computing worldview, the information and comparing complex administration errands can be moved operations to the cloud for the administration adaptability and cost reserve funds. Tragically, as the information could be touchy, the immediate information re-appropriating would have the issue of protection spillage. In our framework, the encryption can be utilized, before the information re-appropriating, with the worry that the activities can at present be refined by the cloud. The proposed framework likewise considers the Attribute based multi catchphrase closeness search over redistributed cloud information. Specifically, with the thought of the content information just, Attribute based numerous catchphrases are determined by the client. The cloud restores the documents containing in excess of an edge number of information watchwords or comparable catchphrases, where the comparability here is characterized by the alter separation metric.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, ``Secure ranked keywordsearch over encrypted cloud data,'' in Proc. IEEE 30th Int. Conf. Distrib.Comput. Syst., Genova, Italy, Jun. 2010, pp. 253262.

[2] C. Liu, L. Zhu, and J. Chen, ``Efcient searchable symmetric encryptionfor storing multiple source dynamic social data on cloud,'' J. Netw. Comput.Appl., vol. 86, pp. 314, May 2017.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ``Privacy-preserving multikeywordranked search over encrypted cloud data,'' in Proc. INFOCOM,Shanghai, China, Apr. 2011, pp. 829837.

[4] Dr. S. Vasundra, CSE, JNTUACEA, published a paper “A Secure Multi-Keyword Search Over Encrypted data in Mobile Cloud Computing" IJAEMA- international journal of analytical and experimental modal analysis, ISSN NO: 0886-9367, Vol XI, Isuue VIII, Aug-2019, (An UGC-CARE Approved Group-A journal) (Scopus indexed).

[5] Z. Shen, J. Shu, and W. Xue, ``Preferred keyword search over encrypteddata in cloud computing," in Proc. IWQoS, Montreal, QC, Canada,Jun. 2013, pp. 16.

[6] Dr. S. Vasundra, CSE, JNTUACEA, Published a paper “Enhanced Public Key Encryption with Keyword Search in Cloud" IJERT-International journal of Engineering Research & Technology, ISSN NO: 2278-0181, Volume. 8 Issue. 8, Aug-2019.

[7] M. Chuah and W. Hu, ``Privacy-aware bedtree based solution forfuzzy multi-keyword search over encrypted data," in Proc. ICDCSW,Minneapolis, MN, USA, Jun. 2011, pp. 273281.

[8] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, ``An efcient and secureprivacy-preserving approach for outsourced data of resource constrainedmobile devices in cloud computing," J. Netw. Comput. Appl., vol. 64, pp. 1222, Apr. 2016.

[9] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen,“Enabling fine-grained multi-keyword search supporting classifiedsub-dictionaries over encrypted cloud data,” IEEE Transactionson Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325,2016.

[10] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “Dual-serverpublic-key encryption with keyword search for secure cloud storage,”IEEE transactions on information forensics and security, vol. 11,no. 4, pp. 789–798, 2016.

[11] Dr. S. Vasundra et.al, CSE, JNTUACEA, Published a paper” Efficient & Secure Privacy Preserving Public Auditing Scheme For Cloud Storage”, International Journal of Advanced Research in Computer Engineering & Technology ISSN: 2278 – 1323 September 2016.

[12] J. Li, Y. Wang, Y. Zhang, and J. Han, “Full verifiability for outsourced decryption in attribute based encryption,” IEEE Transactions on Services Computing, vol. PP, pp. 1–1, 2017.

[13] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, “User collusion avoidance cp-abe with efficient attribute revocation for cloud storage,” IEEE Systems Journal, vol. 12, no. 2, pp. 1767–1777, 2018.

[14] T. V. X. Phuong, G. Yang, andW. Susilo, “Hidden cipher text policy attribute-based encryption under standard assumptions,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 35–45, 2016.

[15] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, “m2-abks: Attribute-based multi-keyword search over encrypted personal health records in multi-owner setting,” Journal of medical systems, vol. 40, no. 11, p. 246, 2016.

[16] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187– 1198, 2016