A Multi-Keyword Searchable Encryption Scheme Based on Probability Trapdoor over Encryption Cloud Data

Anushya S and R. Chennappan
Department of MCA, Karpagam Academy of Higher Education, India

Keywords: Searchable Encryption, Multi- Keyword Search, Probability Trapdoor, Indistinguishable Attacks.

Abstract: The rapid evolution of cloud computing has prompted the substantial migration of data to cloud servers for efficient storage and management. To address privacy concerns, encryption of data before upload is imperative. However, conventional data processing methods face challenges in encrypted domains (ED). Data retrieval stands as a significant hurdle for cloud storage services, particularly when seeking sensitive information encrypted for traditional data usage based on plaintext keyword searches. The approval of a cloud data encrypted search service becomes crucial in this context. Given the expansive user base and document repository in the cloud, facilitating multiple keywords in search requests and presenting documents in relevance order is essential. Unlike existing mechanisms focusing on single or Boolean keyword searches, our proposed method, termed "Multi-keyword Ranked Search over Encrypted Data in Cloud Computing (MRSE)," incorporates a well-organized similarity measure known as "coordinate matching." This measure aims to maximize matches for effective data document retrieval based on search queries. In this paper, we establish stringent privacy requirements for such a secure cloud data utilization system, emphasizing the significance of enabling multi-keyword inquiries and delivering results in accordance with their relevance to the keywords.

1 INTRODUCTION

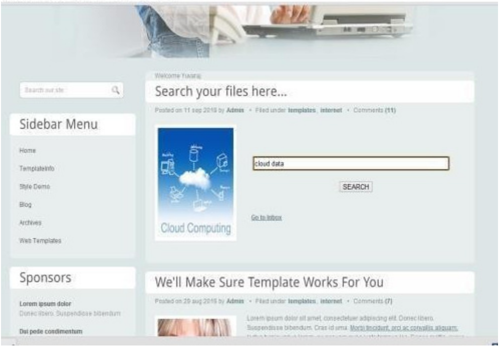
These days, data storing in third party capacity is expanded. Outsourcing the information to other capacity gadget or servers which may addressed to the secure environment. In any case, touchy information like restorative data ought to require an protection when it is put away in cloud capacity (Song 2000). In this paper, a secure watchword look which give the resultant information in a scrambled frame where theconclusion client can decode utilizing the key given to them. It employments the Blowfish to scramble the information and it moreover bolsters the information proprietor to erase or adjust the substance of their archive(Boneh 2004, Curtmola 2006). It too guarantee precise significance score calculation between scrambled list and inquiry vectors. The advantage of capacity as a benefit numerous ventures are moving their important informationto the cloud, since it costs less, effortlessly adaptable and can be gotten to from anyplace any time (Golle 2004, Boneh and Waters 2007, Cao et al 2011). The believe between cloud client and supplier is foremost. They utilize security as a parameter to set up believe. Cryptography is one way of establishing trust. Searchable encryption could be a cryptographic strategy to supply security. In writing numerous analysts have been working on creating proficient searchable encryption plans. To secure information protection, the delicate information ought to be scrambled by the information proprietor some time recently outsourcing, which makes the conventional and productive plaintext catchphrase look procedure futile**.**

2 RELATED WORKS

The searchable encryption scheme has, for the most part, begun to take shape and may be broadly divided into three categories: Fluff catchphrase searches, multiple-keyword searches, and single-keyword searches. The specific research study is presented as follows.

S, A. and Chennappan, R.
A Multi-Keyword Searchable Encryption Scheme Based on Probability Trapdoor over Encryption Cloud Data.
DOI: 10.5220/0012611000003739

In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 206-209
ISBN: 978-989-758-661-3


Search our site
Welcome Yuvaraj
Search your files here...
Posted on 11 sep 2016 by Admin • Filed under templates, internet • Comments (11)
Sidebar Menu
Home
Templateinfo
Style Demo
Blog
Archives
Web Templates
Cloud Computing
cloud data
SEARCH
Go to Inbox
Sponsors
Lorem ipsum dolor
Donec libero. Suspendisse bibendum
Dui pede condimentum
We'll Make Sure Template Works For You
Posted on 29 aug 2016 by Admin • Filed under templates, internet • Comments (7)

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec libero. Suspendisse bibendum. Cras id urna. Morbi tincidunt, orci ac convallis aliquam,

Figure 1: File Search.

2.1 Single Keyword Search

The concept of searchable encryption was presented by (Cao et al. 2014) moreover presentedthe primary symmetrically searchable encryption conspire for ciphertext information recovery. In any case, the complexity of patternlookup increments directly with the estimate of the record collection. As it were straightforwardwatchword look is conceivable, taken a toll is tall but productivity is moo. Boneh et al. proposed the primary searchable public-key cryptosystem (PKES) based on bilinear mapping operations. This expanded computational control and diminished look effectiveness. Considering the security given bytrapdoors, Curtmola et al. embraced a switch ordering procedure to progress look proficiency.With the presentation of altered records, patternlook complexity is presently related as it were to the number of catchphrases and not to the measure of the document collection. Note that this plot characterizes for the primary time the security objectives of a symmetrically searchable encryption scheme. Of course, a single-keyword searchable construction cannot meet the user's ought to recover information for numerous catchphrases. In 2004, Golle et al. proposed the primary searchable multikeyword encryption plot that underpins straightforward inquiries. A more commonsense inquiry his conspire was before long created by Boneh et al.Proposed. It underpins common questions like .

B. Compare and refine inquiries. In reality, Caoet al.presented the primary searchable encryption scheme that really bolsters numerouswatchword looks. I have a sorted yield Decreases the relative weight of records and spares organize transfer speed. At that point, in 2014, Cao et al. The concept of searchable encryption was presented by Melody et al. introduced the primary symmetric searchable encryption conspire for ciphertext information recovery. In any case, the complexity of pattern lookup increments directly with the estimate of the record collection. As it were basic watchword look is conceivable, taken a toll is tall but efficiency is moo. Boneh et al. proposed the primary public-key-based searchable encryption conspire (PKES) based on bilinear mapping operations, but this come about in expanded computationalcomplexity and reduced look productivity. Considering the protection given by trapdoors, Curtmola et al embraced a invert ordering method to move forward look efficiency. With the presentation of modified records, pattern look complexity is presently related as it were to the number of watchwords and not to the size of the archive collection. Note that this conspire characterizes for the primary time the security objectives of a symmetrically searchable encryption plot.

2.2 Multi Keyword Search

A searchable multi-keyword encryption plot that makes a difference secure your protection. This can be the primary strategy that presents facilitate framework coordinating look to numerous catchphrase sort look, but the accuracy is insufficient because the contrast in weight between watchwords isn't taken into consideration. In 2015, an modified file was to begin with utilized to perform multikeyword looks by Wang et al.. To extend the proficiency of the multi-keyword conspire, Xia et al. outlined an file based on a tree structure agreeing to the vector demonstrate, word recurrence show, and converse archive recurrence show of the construction, and presented the record into the look prepare. As of late, Ding et al. proposed a random-his traversal calculation that builds an record based on the tree structure inside the conspire and permits the plot to total ciphertext looks speedier. Once level. Boneh (2007) proposed a searchable encryption conspire based on probabilistic trapdoors that not as it were underpins numerous watchword looks, but too stands up to vague assaults. The development of a probabilistic trapdoor makes our conspire flexible to indistinguishable assaults. In expansion, by presenting a catchphrase vector when building a trapdoor, it is conceivable to rummage around for different catchphrases within the ciphertext look handle. At last, the comes about of comparing this conspire with other searchable encryption plans demonstrate that our scheme clearly outperforms the others in terms of look capabilities and capacity complexity.

2.3 Fuzzy Keywords Search

Fluffy catchphrase look permits clients to input substance with inconspicuous mistakes or organize inconsistency.It incredibly progresses the commonsense of the plot and client involvement. In 2010, the fluffy catchphrase look plot was firstly proposed by Wang et al. and Xia et al The likenesses of watchwords were measured by altering separate. This strategy is unworkable for large data collections since the estimate of the fluffy watchword set may grow exponentially, leading to excessive memory usage and resource waste. The Region Touchy Hashing (LSH) was presented to progress as a solution to this problems the fuzzy search by Wang et al. In this method, the voluminous phrase set that uses a lot of memory can be abandoned.

Tragically, expensive performance costs cannot be strategically avoided due to a predefined seed channel or vector requirement. Subsequently, it cannot work well when the objective information set is as well huge. In Fu et al. utilizes a gram based fluffy set to actualize a fluffy keyword search that comes to distant better much better higher stronger improve an improved effectiveness. In any case, the scheme cannot withstand the unclear attacks because of the deterministic catchphrase trapdoor produced within the conspire Tahir et al. proposed a watchword look conspire based on a likelihood trapdoor, which can stand up to unclear attacks. This plot underpins deterministic single-keyword look, but may not total multi-keyword look. To back rationale questions over scrambled information, ref. displayed a fluffy look plot which is anticipated to be combined with correct look.

3 PROPOSED SYSTEM

Cloud offers capacity benefit to clients withvarious benefits such as decreased sending and upkeep costs, adaptability, progressed execution, gadget and area freedom, etc. The utilization of cloud capacity to store secret information increments the hazard of data revelation by numerous folds. The outsourced information is persistently observed by foes (noxious insiders and pariahs) for profitable bitsof knowledge. So, end-users utilizing these thired-party administrations consider information security (counting both capacity and computation security) as the most obstruction in cloud appropriation as information is continually beneath security dangers all through its life cycle, i.e., in several stages to be specific, information era and collection, information transmission, information capacity, information sharing, information application, and pulverization.

4 CONCLUSION

In this research work, a searchable encryption plot basedon probabilistic trapdoors is proposed, which cannot as it were bolster multi-keyword look buttoo stand up to unclear attacks. The development of likelihood trapdoors makes our conspire safe to unclear attacks. Besides, by presenting the catchphrase vector when building the trapdoor, the plot can realize the multikey word look within the ciphertext look handle. At last, comparison comes about between this plot and other searchable encryption plans demonstrate that our conspire has particular points of interest over other plansin terms of look usefulness and capacitycomplexity. In this research work we depict and unravel the issue of multikey word positioned look overscrambled cloud information, and set up a run ofsecurity prerequisites. Among different multikey word semantics, we select the effective likeness degree of "coordinate matching," i.e., as numerous comparable as conceivable, to viably capture the Pertinence of outsourced reports to the inquiry Watchwords, and utilize "inner item similarity" to quantitatively calculate such comparison degree. In arrange toprocure the test of supporting multikey word semantic without protection infringement, we offer a basic Idea of MRSE utilizing secure inward item calculation. At that point, we granttwo moved forward MRSE plans to achievedifferent extreme protection needs in two diverse risk models. We help utilize "internal thing likeness" to quantitatively evaluate practically equivalent to closeness degree. We to start with propose a essential ponder for the MRSE predicated on secure internal thing computation, and after that permit two essentially moved forward MRSE plans to accomplish diverse inflexible securityprerequisites in two particular trap models. To advance see bother of the data see advantage, we offer assistance extend these two plans to support more distant see semantics. add up to examination investigating security and capability guarantees of proposed plans is given. Tests on the genuine- world data setempower show up proposed plans truly show moo mass migration on computation and communication. we handpick the beneficial likeness degree of misalign planning as various matches as conceivable, to capture the importance of data records to the see request. In this each library is related with a twofold vector as a sub record where each bit talks to whether Comparing catchphrase is containedinside the record. The see request is additionally depicted as a twofold vector whereeach bit infers whether comparing watchword appears up in this see inquire, so the closeness could be absolutely measured by the inside thing of the request vector with the data vector.

REFERENCES

Song, D. Practical Techniques for Searches onEncrypted Data. In Proceedings of the 2000 IEEE Security and Privacy Symposium (SP), San Jose, CA, USA, 22–26 May 2017; pp. 44–55.

Boneh,D.Publickey Encryption with Keyword Search. In Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—Eurocrypt 2004, Interlaken, Switzerland, 2–6 May 2004; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3027, pp. 506–522.

Curtmola, R. Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. In Proceedings of the 2006 ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, USA, 30 October–3 November 2006; pp.79–88.

Golle, P. Secure Conjunctive Keyword Search Over Encrypted Data. In Proceedings of the 2004 Applied Cryptography and Network Security Conference (ACNS), Yellow Mountain, China, 8–11 June 2004; pp. 31–45.

Boneh, D.; Waters, B. Conjunctive, Subset, and Range Queries on Encrypted Data. In Proceedings of the International Conference on Theory of Cryptography (TCC), Amsterdam, The Netherlands, 21–24 February 2007; pp. 535–554.

Cao, N.; Wang, C.; Li, M.; Ren, K.; Lou, W. Privacy-preserving Multi-keyword Ranked Search over Encrypted Cloud Data. In Proceedings of the 2011 IEEE INFOCOM, Shanghai, China, 10– 15 April 2011; pp. 829–837.

Cao, N.; Wang, C.; Li, M.; Ren, K.; Lou, W. Privacypreserving Multi-keyword Ranked Search over Encrypted Cloud Data. IEEE Trans. Parallel Distrib. Syst. 2014, 25, 222–333.

Wang, B.; Song, W.; Lou, W.; Thomas, Y.H. Inverted Index based Multi-keyword Public-key Searchable Encryption with Strong Privacy Guarantee. In Proceedings of the 2015 IEEE INFOCOM—IEEE Conference on Computer Communications, Hong Kong, China, 26 April–1 May 2015; pp. 2092–2100.

Xia, Z.; Wang, X.; Sun, X.; Wang, Q. A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data. IEEE Trans. Parallel Distrib. Syst. 2015, 27, 340–352.