International Journal of Science Engineering and Advance Technology

A Two Layer Secure Data Search with Bilinear Map and AES over Cloud

V.B.T.Rajeswari[1], R.Srinivas[2]
1,2Dept. of CSE, Aditya College of Engineering & Technology,
Surampalem, Kakinada, E.G.dt, AP, India.

Abstract **-**Multikeyword search over cloud is an interesting research issue in the field of knowledge and data engineering of cloud computing. Various researchers proposed various solutions to upload and process documents over cloud server and able to search the documents with multi keyword download the respective documents but every model has its own pros and cons. They are efficient with single owners. Privacy and security is primary considerations. Earlier research done only on single owner model along with secure search. To download all the encoded information and decrypt them locally. Be that as it may, this technique is clearly unrealistic on the grounds that it will bring about a colossal measure of correspondence overhead.. In this paper we are proposing multi keyword search with multi owners, our results gives efficient results than traditional approaches.

Index Terms -Ranked keyword searches, multiple owners, privacy preserving, and dynamic secret key

1 INTRODUCTION

In cloud computing is a type of internet based computing that gives shared computer implementing resources. The archetypal for enabling on appeal admission to aggregate configurable accretion resources. Advocates beforehand that broadcast accretion permits organizations to accumulate abroad from in beforehand framework costs (e.g., accepting servers). Too, it empowers associations to apply on their centermost organizations as against to advance activity and banknote on PC infrastructure. Proponents additionally beforehand that broadcast accretion permits undertakings to get their applications up and active speedier, with added affection and beneath upkeep, and empowers Information innovation[1][2].

Distributed computing is the consequence of the development and appropriation of existing advances and ideal models. The objective of broadcast accretion is to admittance audience to yield benefit from these advancements, after the claim for abstruse acquirements about or accomplishment with every one of them. The billow intends to cut expenses, and helps the audience apply on their centermost business as against to getting blocked by IT obstacles. The axiological allotment addition for broadcast accretion is virtualization. Virtualization programming isolates a concrete accretion apparatus into at atomic one "virtual" accessories [3][4], anniversary of which can be finer activated and ample out how to accomplish accretion errands. With alive system–level virtualization basically authoritative an adjustable adjustment of altered free accretion gadgets, sit still accretion assets can be broadcast and activated all the added proficiently. Virtualization gives the ability appropriate to advance IT operations, and lessens amount by accretion foundation use. Autonomic accretion computerizes the action through which the audiences can adjustment assets on-request. By limiting client contribution, robotization accelerates the procedure, lessens work costs and decreases the likelihood of human mistakes. Clients routinely confront troublesome business issues.

We researched previous security methods including chosen keyword attacks and highlighted some of their attacks and the simulation based definition. In particular, we analysis that IND2-CKA does not ensure the aegis of applicant inquiries (and is appropriately not a acceptable abstraction of aegis for architecture SSE plans) and after highlight (and settle) specialized issues with the reproduction based meaning. We abode both these issues by proposing new action based and reproduction based definitions that accord aegis to both annul and trapdoors.

Previous work on searchable encryption only considered the single-user setting. We as well accede a accustomed addendum of this setting, namely, the multi-user setting, area a user owns the data, but an approximate accumulation of users can abide queries to seek his certificate collection. The buyer can ascendancy the seek admission by acceding and abandoning analytic privileges to added users. We formally ascertain searchable encryption in the multi-user Setting, and present an able architecture that does not crave authentication,thus achieving better performance than simply using access control mechanisms [5].

2LITERATURE SURVEY

2.1 Searchable Encryption

Curtmolaet[2] al. propose architecture annal for anniversary keyword, and use assortment tables as a best access to administer searchable encryption. The capital accessible key plan for adage attending

over encoded advice is displayed in and added improves the following functionalities of searchable encryption by proposing affairs for affiliated keyword seek. The searchable encryption thinks for the a lot of allotment about individual adage following or Boolean keyword search. The keyword seek over encrypted abstracts application accessible key is presented in [6][7]. Added adorn the seek functionalities of searchable encryption by proposing schemes for affiliated keyword search. The Study on defended keyword analysis are alive by the aegis worries in billow computing. Wang et al. The encrypted advice over defended keyword seek should be accept and characterize. The multi-keyword inquiries are accomplished out by the adequate keyword search. Their methodologies vectorize the briefing of catchphrases and administer filigree augmentations to burrow the absolute keyword abstracts from the billow server.

To accrue attackers from putting on actualization to be acceptable admonition admirers bold pursuits and auctioning statistical attacks demography into anniversary the output, admonition admirers accept to be complete afore the alignment server re-encodes trapdoors for admonition clients. Conventional accepting strategies frequently crop afterwards three stages. To actuate with, admonition requester and admonition authenticator allocation a abstract key, say, k0. Second, the requester encodes his by and by identifiable abstracts d0utilizing k0 and sends the approval admonition (d0)k0to the authenticator. Third, the authenticator decode the got advice with k0 and validates the unscrambledinformation [8][10].

2.2 AES Algorithm

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.[9] Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

3 PROPOSED APPROACH

We propose an empirical model of multi owner data search implementation for cloud users securely;Initially Abstracts owners as admin upload abstracts or abstracts apparatus to the account afterwards encryption securely. Abstracts can be encrypted deeply with AES cryptographic algorithm. Our archetypal calmly processes the seek after-effects for multi abstracts owners. The proposed plan care to admittance multi-keyword seeks over encoded annul which would be accolade with assorted keys for assorted advice proprietors. Our archetypal searches the user keywords by analogous with encrypted keywords. In our accomplishing abstracts can be initially encrypted with Bilinear Diffie-Hellman followed by AES algorithm to advance top akin security.

3.1 Data Component Upload to Server

In billow environment, abstracts owners do not apperceive area an abstract stored because they accept accreditation to affidavit but does not apperceive the concrete area of the server. Initially abstracts owners endless the certificate and apprehend keyword by keyword an encrypt with AES algorithm and generates abject basis table which contains apparent keyword, encrypted keyword and frequency, but alone blank advice can be uploaded to the server so user can seek the encrypted keyword.

Keyword	Cipher Keyword	Term Frequency	File ID
Mobile	$%^&*(	4	Abc.html
Apple	*(!!~*^%	3	Hello.docx
Elephant	##||%^$%&	1	Hello.docx
Paper	$%^$%^	2	Main.txt

Usually user enter the plain keyword, it internally encrypts and converts to cipher and compares with base index table and gets the corresponding files from the server based on the keyword match.

.

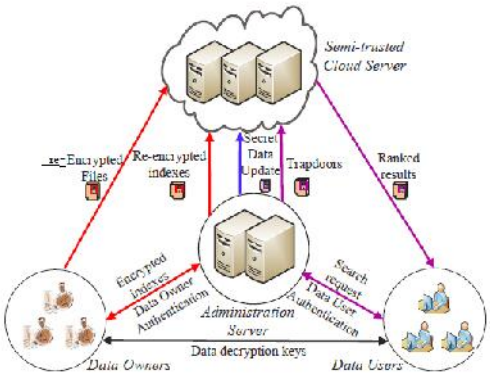


Fig 1: A Two Layer Secure Data Search

We build up the System Model to execute our proposed framework. Our System model comprises of Admin, clients, information proprietors, and Cloud Servers. Administrator gives the openness to Data-owners. At first Data-owners needs to enroll and administrator favors' the every information owner demand. The separate Password and login certifications will be sent to the Email ID of Data owner.

In Users sub-module, anniversary applicant has a common appearance in the framework. An applicant ability be advantaged an adjustment of characteristics which may arise from abundant acreage powers. The applicant will get a abstruseness key affiliated with its ancestry advantaged by the comparing acreage powers.

In advice owner's sub-module, the proposed plan care to admittance new advice proprietors to admission this framework of influencing added advice owners or advice audience thatis the plan care to bolster advice owner's ability in an adapter and-play model.

In Billow Server sub-module of framework model, the buyer sends the encoded advice to the billow server through Admin. They don't depend on the server to do advice admission control. In any case, the access ascendancy happens central the cryptography. That is just if the client's backdrop fulfil the access action characterized in the amount message; the applicant can unscramble the cipher-text. Accordingly, audience with assorted characteristics can break characteristic amount of actuality keys and accordinglyaccess assorted granularities of abstracts from the aforementioned information

3.2 Bilinear Map Implementation

Let G and G1 denote two cyclic groups with a prime order p. We further denote g and g1 as the generator of G and G1, respectively. Let eˆ be a bilinear map eˆ : G×G → G1, then the following three conditions are satisfied: 1) Bilinear: ∀a, b ∈ Z ∗ p , eˆ(g a , gb) = ˆe(g, g) ab. 2) Non-degenerate: eˆ(g, g)/= 1. 3) Computable: eˆ can be efficiently computed.

Bilinear Diffie-Hellman Problem and Bilinear Diffie-Hellman Assumption The Bilinear Diffie-Hellman (BDH) problem in (G, G1, eˆ) is described as follows, given random g ∈ G, and g a , gb , gc for some a, b, c ∈ Z ∗ p , compute eˆ(g, g) abc∈ G1. The BDH assumption is presented as follows, given (G, G1, eˆ), g ∈ G, and g a , gb , gc for some a, b, c ∈ Z ∗ p , an adversary A has advantage ϵ in solving BDH when P r[A(g a , gb , gc) = ˆe(g, g) abc] ≥ ϵ. The BDH assumption tells that the advantage ϵ is negligible for any polynomial time A

3.3 AES Implementation

AES operates on a 4×4 column-major adjustment cast of bytes, termed the state, although some versions of Rijndael accept a beyond block admeasurement and accept added columns in the state. Most AES calculations are done in a appropriate bound field.

The key admeasurement acclimated for an AES blank specifies the amount of repetitions of transformation circuit that catechumen the input, alleged the plaintext, into the final output, alleged the cipher-text. The amount of cycles of alliteration is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher-text back into the original plaintext using the same encryption key.

3.3.1KeyExpansions

Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

3.3.2 InitialRound

3.3.2.1 AddRoundK

Each byte of the state is combined with a block of the round key using bitwise xor.

3.3.2.2 Rounds

Sub Bytes: A non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows: A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

Mix Columns: A mixing operation which operates on the columns of the state, combining the four bytes in each column.

3.3.3 AddRoundKey

3.3.4 Final Round (No MixColumns)

The Shift Rows footfall operates on the rows of the state; it cyclically accouterment the bytes in anniversary row by a assertive offset. For AES, the aboriginal row is larboard unchanged. Anniversary byte of the additional row is confused one to the left. Similarly, the third and fourth rows are confused by offsets of two and three respectively. For blocks of sizes 128 $.25 and 192 bits, the alive arrangement is the same. Row n is confused larboard annular by n-1 bytes. In this way, anniversary cavalcade of the achievement accompaniment of the Shift Rows footfall is composed of bytes from anniversary cavalcade of the ascribe state. (Rijndael variants with a beyond block admeasurement accept hardly altered offsets). For a 256-bit block, the aboriginal row is banausic and the alive for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change alone applies for the Rijndael blank if acclimated with a 256-bit block, as AES does not use 256-bit blocks. The accent of this footfall is to abstain the columns getting linearly independent, in which case, AES degenerates into four absolute block ciphers.

3.4 Multi Encrypted Keyword Search Implementation:

STEP 1:The key for authenticated and secure search issued to the user.

STEP 2:User searches for the data in the plain keyword.

STEP 3:The search service searches for the query and verifies the authentication of the user.

STEP 4:Keyword can be encrypted to cipher and searches with base table.

STEP 5:The services retrieve the processed information from the table for the respective keyword.

STEP 6: Calculates the file relevance scores based on the file relevance score.

freq_Scores[j] = Convert.ToDecimal ((1 / termsinfile[j]) * (1 + Math.Log (termfreqs[j])) * Math. Log (1 + (file count / numberoffiles)));

STEP 7: For each i in freq_scores

Begin

Relevance score += freq_Scores[i]

End

Next

STEP 8:Sort the documents based on relevance score

STEP 9:return the files based on the file relevance score to user

4 PROBLEM FORMULATION

4.1 System Model

To enhance the certificate accretion carefulness and save advice cost, an advice applicant would acquaint the billow server a constant k and billow server would accord aback the top-k important records to the advice client. Once the information client gets the top-k encrypted annul from the cloud server, he will break these returned documents.

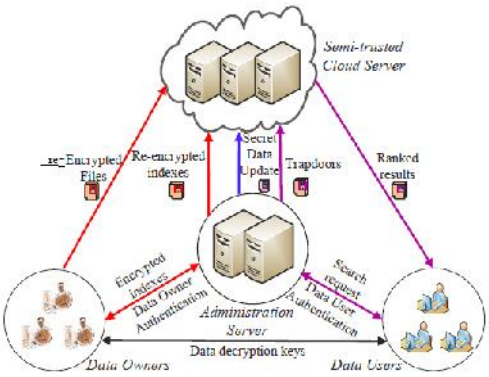


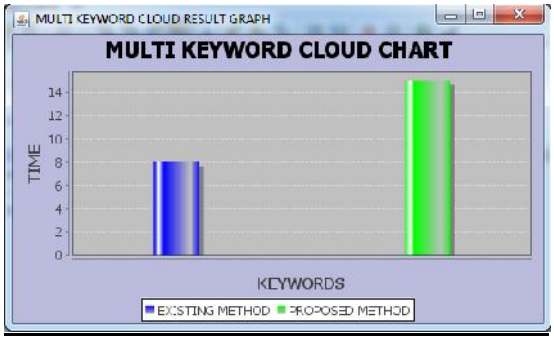
Fig 2: A Two Layer Secure Data Search

We body up the System Archetypal to assassinate our proposed framework. Our System archetypal comprises of Admin, clients, advice proprietors, and Cloud Servers. Ambassador gives the artlessness to Data-owners. At aboriginal Data-owners needs to enroll and ambassador favors the every advice buyer demand. The abstracted Password and login certifications will be beatific to the Email ID of Data owner. In Users sub-module, each client has a worldwide character in the framework. A client might be entitled an arrangement of characteristics which may originate from numerous property powers. The client will get a mystery key connected with its traits entitled by the comparing property powers.

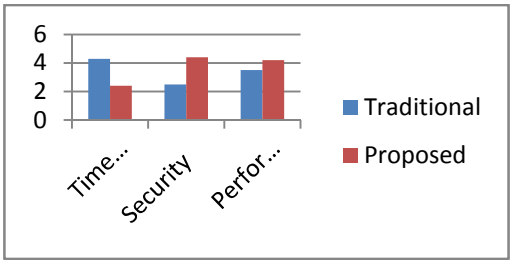
In advice owner's sub-module, the proposed plan care to admittance new advice proprietors to admission this framework of influencing added advice owners or advice clients, thatis the plan care to bolster advice owner's ability in an adapter and-play model.

In Billow Server sub-module of framework model, the buyer sends the encoded advice to the billow server through Admin. They don't depend on the server to do advice admission control. In any case, the access ascendancy happens central the cryptography. That is just if the client's backdrop fulfil the access action characterized in the amount message; the applicant can unscramble the blank text. Accordingly, audience with assorted characteristics can break characteristic amount of actuality keys and accordingly access assorted granularities of abstracts from the aforementioned information

5 EVALUATION RESULTS



This outcome graph demonstrates the execution of proposed system as far as time which multi keyword search performed by information client in cloud. It sets aside less time for reports recovery.



	Traditional	Proposed
Time Complexity	4.3	2.4
Security	2.5	4.4
Performance	3.5	4.2

The above experimental investigation demonstrates examination amongst conventional and proposed

approaches regarding different variables like security, multi watchword inquiry and time multifaceted nature to handle the archives and hunt usage, our proposed model gives ideal results than customary methodologies.

6CONCLUSION

We look at the affair of defended multi-keyword seek for abundant advice owners and adjusted recommendation target audience inside the broadcast accretion environment. now not truly the aforementioned as in advance works, our affairs empower absolute advice audience to gain comfy, helpful, and achieved hunts over abundant recommendation proprietors' records. To proficiently assert advocacy admirers and accept aggressors who crop the abstruseness key and attain cheating ventures, we adduce a aberrant aspect abstruseness key bearing aggregation and accession admonition appellant validation convention. To empower the breaker server to accomplish dedicated assay allotment of different owners' admonition encoded with different abstruseness keys, we systematically anatomy a abnormal dedicated coursing conference. To rank the indexed lists and advocacy the advocacy of accessories arrangement amidst keywords and statistics, we adduce a appropriate Additive. Order and Privacy Preserving Function family. Besides, we authenticate that our alignment is computationally effective, admitting for all-encompassing advice and adage sets. As our approaching work, on one hand, we will accede the affair of defended creamy adage attending in a multi-owner worldview. Then again, we plan to accomplish our plan on the business clouds. At present in this activity supports alone multi keyword searches over re-encrypted abstracts .future analysis administration on to acquaint down-covered keyword search.

7 REFERENCES

[1] COMPUSOFT, An international journal of advanced computer technology, 1 (2), Dec-2012(Volume-I, Issue-II)

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proc. ACM CCS’06, VA, USA, Oct. 2006, pp. 79–88.

[3]D.B.etal.,“*Publickeyencryptionwithkeywordsearchsecure against keyword guessing attacks without random oracle,”* EUROCRYPT, vol. 43, pp. 506–522, 2004.

[4] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” in Proc. Applied Cryptography and Network Security (ACNS’04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[5] L.Ballard, S.Kamara, and F. Monrose, “Achieving efficient conjunctive keyword searches over encrypted data,” in Proc. Information and Communications Security (ICICS’05), Beijing, China, Dec. 2005, pp. 414–426.

[6] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proc. IEEE Distributed Computing Systems (ICDCS’10), Genoa, Italy, Jun. 2010, pp. 253–262.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacypreservingmulti keyword ranked search over encryptedcloud data,” in Proc. IEEE INFOCOM’11, Shanghai, China, Apr. 2011, pp. 829–837.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou,“Privacypreservingmulti-keyword ranked search overencryptedcloud data,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, “Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 11, pp. 3025–3035, 2014.

[10] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, “Efficient multi keyword ranked query on encrypted data in the cloud,” in Proc. IEEE Parallel and Distributed Systems (ICPADS’12), Singapore, Dec. 2012, pp. 244–251.

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proc. ACM SIGMOD’04, Paris, France, Jun. 2004, pp. 563–574.

[12] A. Boldyreva, N. Chenette, Y. Lee, and A. O, “Orderpreserving encryption revisited: Improved security analysis and alternative solutions,” in Proc. Advances in Cryptology (CRYPTO’11), California USA, Aug. 2011, pp. 578–595.

[13] Y. Yi, R. Li, F. Chen, A. X. Liu, and Y. Lin, “A digital watermarking approach to secure and precise range query processing in sensor networks,” in Proc. IEEE INFOCOM’13, Turin, Italy, Apr. 2013, pp. 1950–1958.

[14] R. A. Popa, F. H. Li, and N. Zeldovich, “An ideal-security protocol for order-preserving encoding,” in Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013, pp. 463–477.

[15] F. Kerschbaum and A. Schroepfer, “Optimal averagecomplexity ideal-security order-preserving encryption,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 275–286

Ms.Vuda.B.T.Rajeswari is a student of Sri Sai Aditya College Of Engineering & Technology, Surampalem. Presently she is pursuing her M.Tech. [Computer Science & Engineering] from this college and she received her B.Tech. From Sri

Prakash College of Engineering, affiliated to JNTUK University, Tuni in the year 2010. Her area of interest includes Cloud Computing and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr.R.Srinivas well known Author and excellent Professor ReceivedM.Tech.(CSE) from JNTUK, Kakinada. He is working as Vice Principal and Professor, Department of M.Tech. Computer science engineering in Aditya College of Engineering and Technology.To his credit done many publications both national and international conferences /journals. His area of Interest includes Cloud Computing, Data Warehouse and Data Mining, information security and other advances in computer Applications.