An Efficient Framework for Secure Query Search to Verify Consequences by Using Verification Object

AUTHOR: A.PRIYANKA
CO-AUTHOR: CH.SRAVANTHI

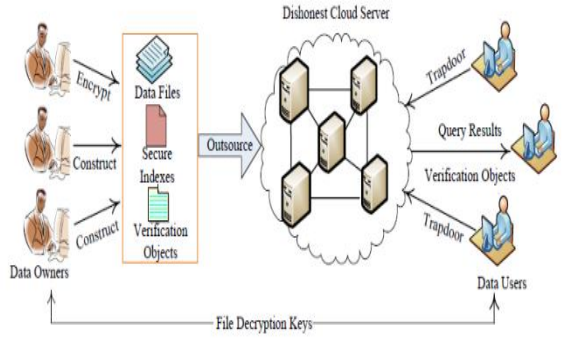
ABSTRACT— protect search for strategies more encrypted cloud information permit an authorized character to query facts documents of hobby with the aid of submitting encrypted query key phrases to the cloud server in a privacy-preserving manner. However, in workout, the lower back query outcomes may also be wrong or incomplete inside the dishonest cloud environment. For instance, the cloud server may additionally intentionally omit some certified outcomes to save computational sources and verbal exchange overhead. Thus, a well-functioning at ease question device need to offer a question outcomes verification mechanism that allows the records person to verify consequences. In this paper, we layout a safe, without issues blanketed, and first-rate-grained question effects verification mechanism, with the useful resource of which, given an encrypted question outcomes set, the query client now not simplest can verify the correctness of every data record within the set however also can further check what number of or which licensed statistics files aren't again if the set is incomplete in advance than decryption. The verification method is loose-coupling to concrete secure searching for strategies and may be very without troubles included into any secure question method. We accumulate the reason through building comfortable verification object for encrypted cloud information. Furthermore, a brief signature technique with noticeably low storage charge is proposed to assure the authenticity of verification item and a verification object request method is provided to permit the question purchaser to soundly gain the favored verification item. Performance evaluation indicates that the proposed methods are sensible and inexperienced.

Keywords:Bloom Filter, Paillier Encryption,Verification Mechanism,Confidentiality

1. INTRODUCTION

Cloud computing is a version for allowing ubiquitous, halong withy, on-call for community access to ashared pool of configurable computing assets (e.g., networks, servers, storage, applications, along with offerings)that may be all of sudden provisioned along with launched with minimum control attempt or issuer organization interplay. Pushed through the abundant advantages delivered via the cloud computing inclusive of fee saving, brief deployment, bendy useful resource configuration, along with so on.Morealong with more firms along with individual users are taking into account migrating their non-public data along with local packages to the cloud server. A be counted variety of public difficulty is the way to guarantee the protection of information that is outsourced to a ways flung cloud server along with breaks far from the direct manage of facts proprietors. Encryption on personal facts before outsourcing is an effective degree to protect facts confidentiality. However, encrypted records make effective facts retrieval a

very difficult task. To deal with the venture, tune et al. First brought the idea of searchable encryption along with proposed a sensible approach thatlets in users to appearance over encrypted data thru encrypted question keywords in.



A system model of verifiable secure search over encrypted cloud data

Later, many searchable encryptionmethods have been proposed primarily based totally on symmetric keyalong with public-key placing to boost protection along with enhance question efficiency. Recently, with the growing popularity of cloud computing, how to securely along with correctly seek over encrypted cloud facts turns into research recognition. A few procedures had been proposed based totally on conventional searchable encryption methods, which goal to protect information protection along with question privacies with better query green for cloud computing. But, all of those methods are primarily based on a really perfect assumption that the cloud server is a "sincere-however-curious" entity along with keeps strong along with secure software program application/hardware environments. As a stop end result, accurate along with entire query outcomes constantly be unexceptionally back from the cloud server whilst a question ends every time. But, in practical applications, the cloud server might also moreover go lower back faulty or incomplete query results once he behaves dishonestly for unlawful earnings collectively with saving computation along with verbal exchange fee or because of possible software program/hardware failure of the server. Therefore, the above truth usually motivates information clients

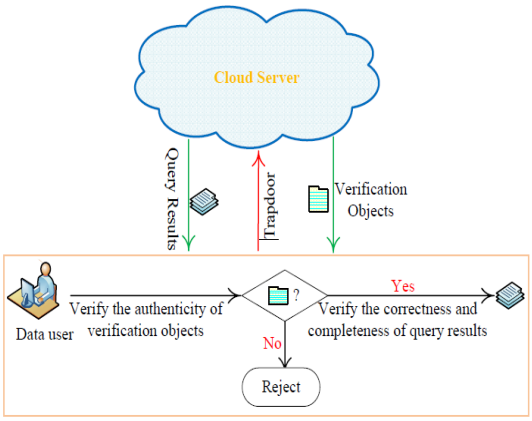
to verify the correctness along with completeness of question consequences. Some researchers proposed to mix the question effects verification mechanisms to their relaxed are searching for methods Upon receiving question effects, information users use precise verification statistics to verify their correctness along with completeness. There are two boundaries in the ones methods.

2. METHODOLOGY

1.Bloom Filter:

A bloom filter begins as an array of a set duration, with all arrayfactors set to zero. Firstly, bigramsof the matching variables are created. Padding has been used to offer the first along with remaining letters their own bigrams.

Each of the bigrams is passed thru a hash function. The hash characteristic is an algorithm which produces a fixed period output with several vital properties. Firstly, given the identical enter;it'll usually produce the identical output. The hash features is likewise one-way, which means it isn't always feasible to determine the encoded bigram from the given hash value. The modulus of these hashes is then computed with admire to the length of the bloom filter. This results in each bigram having a variety which corresponds to a function inside the bloom filter. These positions in the bloom filter out are then modified to 1. When all required bigrams are delivered in this manner, the bloom clear out is completed along with prepared for assessment. Each bigram can be hashed multiple times, resulting in more than one positions within the bloom filter out being set-to one for every bigram. This can be beneficial to lessen the effects of false positives.



The process of query results verification

2. Paillier Encryption:

By use the Paillier encryption method to layout hence a at ease verification object request mechanism. Now, we describe our proposed verification object request method in element.

Gen(1^n): The probabilistic polynomial time algorithm take the protectedconstraint n seeing thatkey inoutputs $(N, p, q, \psi(N))$ somewhere N = pq, p along with q are n-bitsprime. The public keyis pk = N along with the private key is sk =< N,$\psi(N)$>.

Enc(pk,m): The Enc is a probabilistic polynomial timeTechnique, which take the open key pk along witha point m as contributionas well asoutput the cipher text ofm.

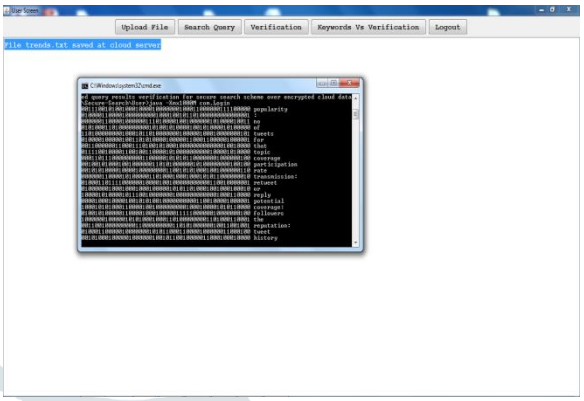
$$c = [(1+N)^m \cdot r^N \mod N^2]$$

Dec(sk; c): The Dec is a deterministic polynomial timetechnique, which takes the private key sk along withthe cipher text c of the message m as effortalong with output m

$$m = \left[\frac{[c^{\psi(N)} \mod N^2] - 1}{N} \cdot \psi(N)^{-1} \mod N\right]$$

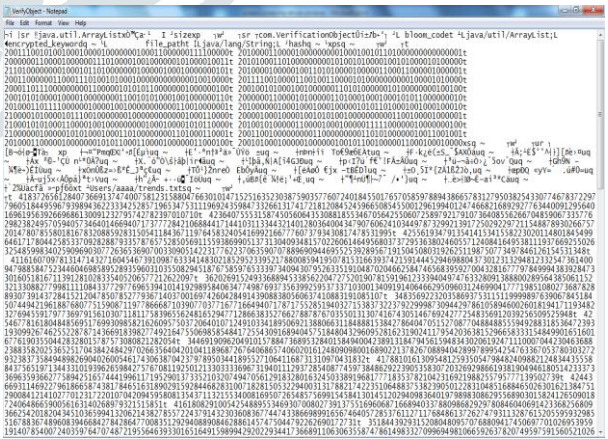
3. RESULTSALONG WITHDISCUSSION

After uploading the file on to cloud



The generated bloom filter. First for the given word get the bigrams, then generate hash for each bigram by using Paillier Encryption technique then generate some integer value for each hash code (here we are taking the array range up to 50) then generate bloom filter signature. Cloud server after uploading the file: the file will be saved at cloud in encrypted format by using AES algorithm.

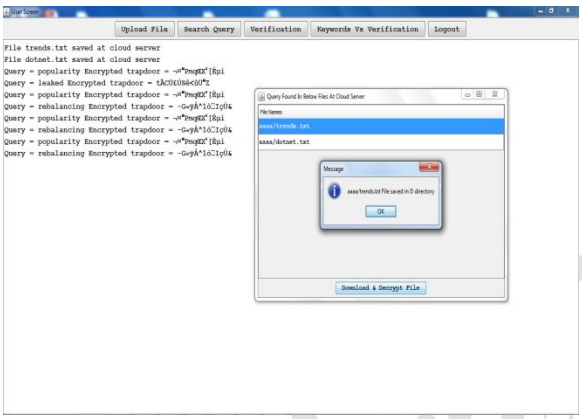
The verification object for the uploaded files will be created along with saved at server side:



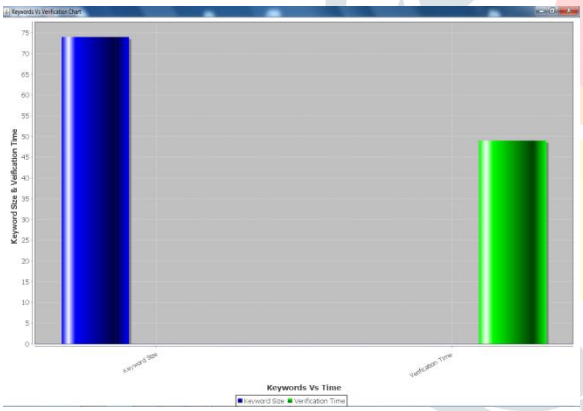
Search query as per this project to reduce the resources, we can give the search results from few of the uploaded files if the client is satisfied with that then he can download that file otherwise he will keep

on search until he will receive the required information.

Select the required file along with decrypt along with download:



Keywords Vs verification chart:



How many keywords are there in the uploaded files along with how much time it has taken to verify.

4. CONCLUSION

In this term paper, we planned a systemsimply incorporated along with high-quality-grained query effects authentication plan intended forat effortlessness be looking for above encrypted cloud information. exceptional from previous works, our plan can verify the appropriateness of every encrypted issue end result or else in addition exactly determine what number of or which certified information files are back by way of the cheating cloud server. A short signature technique is designed to assure the authenticity of verification item itself. Furthermore, we design a at ease verification item request method, by means of which the cloud server is aware of now not anything approximately which verification objectis asked by way of using the statistics person along with in fact once more by using the cloud server. Overall performance along with correctness experiment exhibits the validity along with overall performance of our planned system.

5.REFERENCES

[1] M. Bellare, A. Boldyreva, along with A. O'Neill, "Deterministic along with efficiently searchable encryption," in Springer CRYPTO, 2007.

[2] M. Bellare along with P. Rogaway, Introduction to Modern Cryptography. Lecture Notes, 2001.

[3] K. Kurosawa along with Y. Ohtaki, "Uc-secure searchable symmetric encryption," Lecture Notes in Computer Science, vol. 7397, pp. 258– 274, 2012.

[4] K. Ren, C. Wang, along with Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[5] S. Kamara along with K. Lauter, "Cryptographic cloud storage," in Springer RLCPS, January 2010.

[6] S. Al-Riyami along with K. Paterson, "Certificateless public key cryptography," in Springer ASIACRYPT, 2003, pp. 452–473.

[7] X P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Springer EUROCRYPT, 1999, pp. 223–238.

[8] B. Bloom, "Space/time trade-offs in hash coding with allowable errors," Commun. ACM, vol. 12, no. 7, pp. 422–426, 1970.

JETIR