International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Advance Search Using Bloom Filter and Asymmetric Key Algorithm

Mr.Mukkara Varun Teja Chowdary[1], Mr.Venkatesh K[2], Mr. Nikhil Sai K[2], Mr. M. S. Murali Dhar[3]
[1]Student, Department of CSE, Velammal Engineering College, Chennai, Tamil Nadu, Inida
[2]Student, Department of CSE, Velammal Engineering College, Chennai, Tamil Nadu, Inida
[3]Assistant Professor-II, Department of CSE, Velammal Engineering College, Chennai, Tamil Nadu, Inida

ABSTRACT

Cloud Computing is most various number advantages in cloud platform. In is this concern there are also lot of security problem arises and privacy concerns are there. Data Accessing and integration confidential documents have been identified as one of the central problems in this area. Many researchers tried to find solutions to search over encrypted documents stored on remote cloud servers. While many schemes have been proposed to perform Bloom filter search, less attention has been noted on more specialized searching techniques. In this paper we proposed, a phrase search technique based on Bloom filter that is significantly faster than existing solutions. Bloom filters tied to hashed keywords and n-grams are attached. The contents are then encrypted using Asymmetric-key Encryption method and uploaded to the cloud server. To upload content to the cloud server then keyword is attached with Bloom filters. To remove a content from the cloud server. The data owner simply sends the request to the cloud server, it removes the content along with the attached Bloom filters. Using Asymmetric-key to encrypt and decrypt content. Asymmetric key is a cryptographic algorithm in which there are two different keys are used to encrypt and decrypt the content. When User registers in cloud then that password hashed stored in the cloud server. When we type the login password then it is also hashed and compared with the registered password then it redirects to the Client page. That hashing and encryption technique are used to secure the data in cloud.

I. INTRODUCTION

CLOUD COMPUTING

Cloud computing is accessing the computing assets basically hardware and software which are the facility over a system which is typically the Internet. The name created from the use of a cloud-shaped figure as an abstraction organization it contains in system illustrations. Cloud computing assigns remote services with the user's information, software and computation.

Cloud computing is a prototypical technology for enabling ubiquitous, expedient, on-demand network access to a shared configurable computing assets (e.g., networks, servers, storage, applications and services) that can be rapidly liable and released with minimal management effort.

1.1.1 CHARATERISTICS OF CLOUD COMPUTING

- **On-demand self-service**. A consumer will individually flair computing proficiencies.
- **Broad network access**: Heterogeneous thin or thick platforms are the standard mechanisms that helps to access the capabilities available over the network.
- **Resource pooling**: With different physical and virtual resources dynamically assigned and

reassigned based on the demand will help the providers to serve for the multiple consumers to satisfy their needs.

- **Rapid elasticity**: Capabilities are elastically as well as rapidly liable, in some cases in order to quickly scale in and out are rapidly released in some conditions. The resources available for the optimization process often appear to be limitless and can be bought in any extent at any while.
- **Measured service**: Cloud systems will automatically switch and enhance resource use by some maximum advantage with a measurable arrangement capability at some level of idea suitable to the type of service and what type of resources need for the implementation.

II. LITERATURE SURVEY

2.1 PUBLIC KEY ENCRYPTION WITH KEYWORD SEARCH

Public key encryption with keyword search (PEKS) is a classification for understanding the keyword search over encrypted data, but communication must depend on a protected station. In PEKS, a sender like to share data with a receiver through a storage server. For security and privacy purpose, he must upload the encrypted data to the server, and further the server can search encrypted data by using a keyword trapdoor. In the literature, a new system, server-designation public key encryption with keyword search (dPEKS), is introduced to eliminate the assumption of the secure channel in PEKS.

2.2 PUBLIC KEY ENCRYPTION WITH CONJUNCTIVE KEYWORD

The Public Key Encryption with Conjunctive Keyword Search (PECK)
scheme enables one to search a document included multiple encrypted keywords without compromising any original data information. The existing PECK schemes mostly depend on pairings and authenticated channel to achieve searchable encryption. In this paper, we propose a new PECK scheme based on pairings, where no pairing operations are involved in the encryption and trapdoor phases and no secure channel is needed between server and users. In comparison with previous schemes, our scheme can achieve high efficiencies in both computation and communication.

2.3 ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption is an extreme encryption technology. In this a set of sequence attributes is available in order for the protection of the privacy of receivers. An encryptor can guarantee that only the receivers who match the restrictions on predefined attribute values associated with the ciphertext only can decrypt the ciphertext. However, maintaining the correctness of all users' attributes will take huge cost because it is necessary to renew the users' private keys whenever a user joins, leaves the group, or updates the value of any of her/his attributes. Since user joining, leaving, and attribute updating may occur frequently in real situations, membership management will become a quite important issue in an ABE system. In this paper, we will present an ABE scheme which is the first ABE scheme that aims at dynamic membership management with arbitrary states, not binary states only, for every attribute. Our work also keeps high flexibility of the constraints on attributes and makes users be able to dynamically join, leave, and update their attributes. It is unnecessary for those users who do not change their attribute statuses to renew their private keys when some user updates the values of her/his attributes.

III. EXISTING SYSTEM

- In existing system, Conjective keyword are used to search the content and are symmetrically encrypted and uploaded to the cloud server.
- To upload content then it is assigned with Conjective keyword attached to the cloud server.

- To remove content, then data owner simply sends the request to the cloud server, it removes the content along with the attached Conjective keyword.
- Symmetric-key algorithms are used for cryptography that uses the same cryptographic keys for both encryption of Data and decryption of data.

3.1. DRAWBACKS OF EXISTING SYSTEM

- The keys are identical
- Searching with keywords that might contain errors in existing method of conjunctive keyword search
- Stored data are not secured while storing in Cloud
- In absence of accurate data, it displays noisy data related to it.

IV. PROPOSED SYSTEM

- In proposed system we overcome the existing system by using Bloom filters
- Bloom filters tied to hashed keywords and n-grams are attached.
- The contents are then encrypted using Asymmetric Key Encryption method and uploaded to the cloud server. To upload content to the cloud server then keyword is attached with Bloom filters
- To remove a content from the cloud server. The data owner simply sends the request to the cloud server, it removes the content along with the attached Bloom filters.
- Using Asymmetric-key to encrypt and decrypt content.
- Asymmetric key is a cryptographic algorithm in which there are two different keys are used to encrypt and decrypt the content
- When User registers in cloud then that password hashed stored in the cloud server.
- When we type the login password then it is also hashed and compared with the registered password Then it redirects to the Client page.
- That hashing and encryption technique are used to secure the data in cloud

ADVANTAGES OF PROPOSED SYSTEM

- Bloom filter store Single Key Multiple Values.
- Asymmetric key is used to secure the data More securable Password hashed

V. ARCHITECTURE DIAGRAM

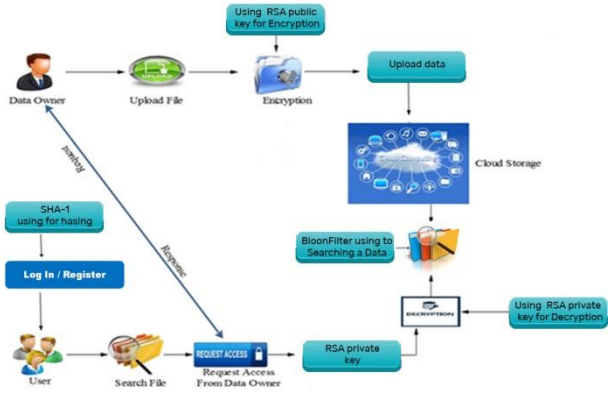

Figure 1

VI. IMPLEMENTATION

6.1 A STANDARD BLOOM FILTER

Let U denote the universe of finite binary numbers and let S = {x1, x2, . . ., xn} be a subset of U. We shall say that an element x ∈ U is "valid" if x ∈ S; else, we shall say that x is "invalid." A Standard Bloom Filter (denoted SBF) is an m-bit vector, B. Available to us are k (random hash) functions h1(·), ..., hk (·) each of which maps an x ∈ U to a randomly chosen element of the set {e1, ..., em}, where ei is an m-bit vector with only its i th bit set to 1. Let h(x) be the logical OR of h1(x), ..., hk(x). We refer to h(x) as the "signature" of x. 1 Notation: For two binary words a and b of equal length a b denotes that b has a 1 in each location where a has a 1. The use of an SBF involves the following two operations. Training. Given S and h (·), the vector B is set equal to the logical OR of h(x1), ..., h(xn). Equally, the bits

corresponding to the signatures of elements in S are set to 1 in the bitmap vector B. Querying. To determine whether a y in U belongs to S, compute h(y). If h(y) B, declare y ∈ S, else declare y ∈/ S. Clearly, the declaration y ∈/ S can never be false1) however, the declaration that y ∈ S can be false2) sometimes. 3)

6.2CONSTRUCTING BLOOM FILTERS

Consider a set $A = \{a_1, a_2, ..., a_n\}$ of n elements. Bloom filters describe information of A by using a bit vector V of length m. For this, k hashed functions, $h_1, h_2, ..., h_k$ with $h_i : X \rightarrow \{1..m\}$, are used.

Below is the procedure:

The following procedure builds an m bits Bloom filter, corresponding to a set A and using $h_1, h_2, ..., h_k$ hash functions:

Procedure Bloom Filter (set A, hash functions, integer m)

returns filter

filter = allocate m bits initialized to 0

foreach a in A:

foreach hash function h_j:

filter[$h_j(a)$] = 1

end foreach

end foreach

return filter

if a_i is member of a set A, in the result Bloom Filter V all bits corresponding to the hashed values of a_i are set to 1. Testing for membership of an element *elm* is equal to testing that all corresponding bits of V are set:

Procedure Membership Test (elm, filter, hash functions)

returns yes/no

foreach hash function h_j:

if filter[$h_j(elm)$]! = 1 **return** No

end foreach

return Yes

features: filters can be built in an incremental order: as new elements are added to a set the corresponding positions are computed through the hash functions and bits are set in the filter. Moreover, the filter expressing the reunion of two sets is simply computed as the bit-wise OR applied over the two corresponding Bloom filters.

Bloom Filters – the Math

Feature of Bloom filter is a clear balance between the size of the filter and the rate of wrong positives. After observing the addition of n keys into a filter of size m using k hash functions, the probability that a specific bit is still 0 is:

$$p_0 = \left(1 - \frac{1}{m}\right)^{kn} \approx 1 - e^{-\frac{kn}{m}}.$$

we undertake that hashed functions spread the elements of A consistently throughout the space {1...m}. In practice, good result have been achieved using MD5 and other hashed functions.

Hence, the probability of a false positive is:

$$p_{err} = (1 - p_0)^k = \left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^k \approx \left(1 - e^{-\frac{kn}{m}}\right)^k$$

p_{err} is minimized for $k = \frac{m}{n} \ln 2$ hash functions. In practice however, only a smallest number of hash functions are used. Addition of a new hashed function shrinkages after a certain threshold ,it is described in Figure 1.

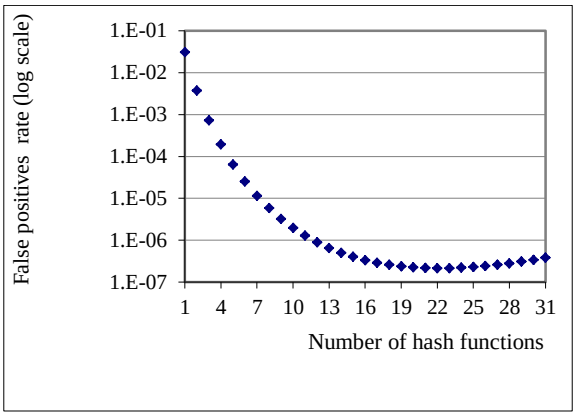

Figure 1. False positive rate as a function of the number of hashed functions used. The size of the Bloom filter is 32 bits per pass (m/n=32). In this situation using 22 hashed functions reduces the false positive rate.however, that adding a hash function does not

decrease the error rate when more than 10 hashes are already used.

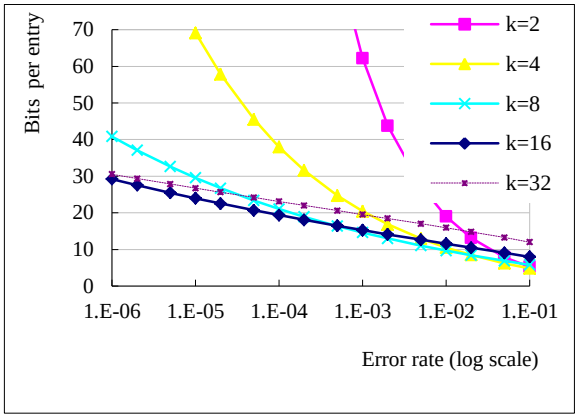

Figure 2. Bloom filter size as a function of the error rate chosen. Different lines represent different numbers of hashed keys used. For the error rates considered, using 32 keys does not bring substantial benefits over using only 8 keys.

The base formula for engineering Bloom filters. It allows, for example, computing minimal memory requirements (filter size) and number of hash functions given the maximum acceptable wrong positives rate and number of elements in the set as we given a detail in Figure 2.

$$\frac{m}{n} = \frac{-k}{\ln\left(1 - e^{\frac{\ln p_{err}}{k}}\right)} \text{ (bits per pass)}$$

VII. CONCLUSION

In existing system, Conjective keyword are used to search the content and are symmetrically encrypted and uploaded to the cloud server. To upload content then it is assigned with Conjective keyword attached to the cloud server. To remove content, then data owner simply sends the request to the cloud server, it removes the content along with the attached Conjective keyword. Symmetric-key algorithms are used for cryptography that uses the same cryptographic keys for both encryption of Data and decryption of data.

In our proposed system we overcome the existing system by using Bloom Filters Bloom filters tied to hashed keywords and n-grams are attached. The contents are then encrypted using Asymmetric-key Encryption method and uploaded to the cloud server. To upload content to the cloud server then keyword is attached with Bloom Filters To remove a content from the cloud server. The data owner simply sends the request to the cloud server, it removes the content along with the attached Bloom filters. Using Asymmetric-key to encrypt and decrypt content. Asymmetric key is a cryptographic algorithm in which there are two different keys are used to encrypt and decrypt the content When User registers in cloud then that password hashed stored in the cloud server. When we type the login password then it is also hashed and compared with the registered password Then it redirects to the Client page. That hashing and encryption technique are used to secure the data in cloud.

VIII. REFERENCES

[1]. Prof. H.Poon and A.Miri, "An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems," in IEEE International Conference on Cloud Computing, 2015.

[2]. "A low storage phrase search scheme based on bloom filters for encrypted cloud services," to appear in IEEE International Conference on Cyber Security and Cloud Computing, 2015.

[3]. Z.Fu, X.Sun, N.Linge, and L.Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Transactions on Consumer Electronics, vol.60, pp.164–172, 2014

[4]. M.Yoon, J.Son, and S.-H.Shin, "Bloom tree: A search tree based on Bloom filters for multiple set membership testing," in Proc.2014 IEEE Conference on Computer Communications (INFOCOM '14), 2014, pp.1429–1437.

[5]. K.Rabieh, M.M.E.A.Mahmoud, K.Akkaya, and S.Tonyali.Scalable Certificate Revocation Schemes for Smart Grid AMI Networks Using Bloom Filters.IEEE Transactions on Dependable and Secure Computing, 14(4):420–432, 2017

[6]. J.Lu, Y.Wan, Y.Li, C.Zhang, H.Dai, Y.Wang, G.Zhang, and B.Liu.Ultra-Fast Bloom Filters using SIMD techniques.In 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), pages 1–6, 2017.

[7]. Y.Zhang, Z.Zheng, and X.Zhang.Efficient Bloom Filter for Network Protocols Using AES Instruction Set.IET Communications, 11(11):1815–1821, 2017.