International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

AN EFFECTIVE PROTECTION ON CONTENT BASED RETRIEVAL IN CLOUD STOREHOUSE

Mr.T. Roger Jees Smith[1], Ms.K. Akshaya Dhevi[2], Ms.V. Madhumadhi[3]

[1]Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College Chennai, TamilNadu 603103, India
[2,3]UG student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College Chennai, TamilNadu 603103, India

---

Abstract - *Cloud computing makes computer system resources, particularly storage and computing power, obtainable on demand without direct active management by the user. The term is mostly accustomed describe information centers obtainable to several users over the web. Massive clouds, predominant nowadays, usually have functions distributed over multiple locations from central servers. If the affiliation to the user is comparatively shut, it's going to be selected an Edge server. Cloud Computing may be a model of net primarily based computing wherever the resources like cupboard space, on-line software package are provided by completely different cloud service suppliers to differing types of cloud users United Nations agency wants cloud services. A cloud user outsources the information on cloud, it's to supply additional security for outsourced information preventing data manipulated or accessed by unauthorized users. So as to maintain information integrity, every and each cloud service has got to be keep firmly. For easier accessing of files and to get file indexes, every file is keep in cloud server. The information user decrypts these within the mobile shopper and recovers the first data. To overcome this, the encrypted file and therefore the file indexes are keep in storage node, key and supply image are keep in cloud server and key image is passed to file owner. Whenever file users wish to transfer or access files then perform search then place key as AN input. If valid, it matches the key with the supply image and later it will be downloaded by submitting the key image.*

***Key Words*: cloud, key generation, OPE keyword, File, Encryption, AES, Authentication, verification, source image, key image, BVCS, RSA.**

1. INTRODUCTION

Cloud computing paradigm makes computer system resources, especially storage and computing power, available on demand without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an Edge server.

1.1 Introduction To Cloud

The term Cloud refers to a Network or net. In alternative words, we are able to say that Cloud are a few things, that is gift at remote location. Cloud will give services over network, i.e., on public networks or on personal networks, i.e., WAN, LAN. Applications like e-mail, net conferencing, client relationship management (CRM), all run in cloud.

Public Cloud: the general public Cloud permits systems and services to be simply accessible to the overall public. Public cloud is also less secure due to its openness, e.g., e-mail.

Private Cloud: The personal Cloud permits systems and services to be accessible inside a company. It offers augmented security due to its personal nature. Community Cloud: The Community Cloud permits systems and services to be accessible by cluster of organizations.

Hybrid Cloud: The Hybrid Cloud is mixture of public and personal cloud. However, the crucial activities are performed exploitation personal cloud whereas the non-critical activities are performed using the public cloud.

1.1.2 Service Models

Service Models are the reference models on that the Cloud Computing is predicated.

These will be classified into 3 basic service models as listed below:

1. Infrastructure as a Services (IAAS)
2. Platform as a Service(PAAS)
3. software package as a Service(SAAS)

There are several alternative service models all of which may take the shape like XaaS, this could be Network as a Service, Business as a Service, Identity as a Service, info as a Service or Strategy as a Service. The Infrastructure as a Service (IaaS) is that the most elementary level of service. every of the service models create use of the underlying service model, i.e., every inherits the safety and management mechanism from the underlying model, as shown within the following diagram:

Infrastructure as a Service (IAAS): IaaS provides access to basic resources like physical machines, virtual machines, memory board, etc.

Platform as a Service (PAAS): PaaS provides the runtime surroundings for applications, development & preparation tools, etc.

Software as a Service (SAAS): SaaS model permits to use software package applications as a service to finish users.

1.1.3 Benefits Cloud Computing has Numerous Advantages

- Some of them are listed below: One will access applications as utilities, over the web.
- Manipulate and piece the appliance on-line at any time.
- It doesn't need to put in a particular piece of software package to access or manipulate cloud application.
- Cloud Computing offers on-line development and preparation tools, programming runtime environment through Platform as a Service model.
- Cloud resources are obtainable over the network in an exceedingly manner that has platform freelance access to any sort of shoppers.
- Cloud Computing offers on-demand self-services to the users.
- The resources will be used while not interaction with cloud service supplier.
- Cloud Computing is extremely price effective as a result of it operates at higher efficiencies with bigger utilization.
- It simply needs an online affiliation. Cloud Computing offers load equalisation that produces it additional reliable.
- Risks though Cloud Computing may be a nice innovation within the world of computing, there conjointly exist downsides of cloud computing. a number of them are mentioned below:
- Security & privacy it's the most important concern concerning cloud computing. Since information management and infrastructure management in cloud is provided by third-party, it's continually a risk to relinquishment the sensitive info to such suppliers.

Although the cloud computing vendors guarantee safer watchword protected accounts, any sign of security breach would end in loss of shoppers and businesses. LOCK-IN it's terribly tough for the purchasers to change from one Cloud Service supplier (CSP) to a different. It ends up in dependency on a selected CSP for service.

Isolation Failure: This risk involves the failure of isolation mechanisms that separates storage, memory, routing between the various tenants.

1.2 Introduction Of The Project

The recent advent of cloud computing has pushed the boundaries of knowledge sharing capabilities for various applications that transcend geographical boundaries and involve countless users. Governments and companies nowadays treat information sharing as a significant tool for increased productivity. Cloud computing has revolutionized education, health care and social networking. maybe the foremost exciting use case for cloud computing is its ability to permit multiple users across the world share and exchange information, whereas saving the pangs of manual information exchanges, and avoiding the creation of redundant or noncurrent documents. Social networking sites have used the cloud to make a additional connected world wherever individuals will share a range of knowledge as well as text and multimedia system. Cooperative tools ordinarily supported by cloud platforms and are extraordinarily well-liked since they cause improved productivity and synchronization of effort. The impact of cloud computing has conjointly pervaded the sphere of health care, with smartphone applications that permit remote observance and even designation of patients. In short, cloud computing is dynamical numerous aspects of our lives in unprecedented ways that. Despite all its benefits, the cloud is liable to privacy and security attacks, that are a serious hindrance to its wholesome acceptance because the primary suggests that of knowledge sharing in todays world. Consistent with a survey meted out by IDC Enterprise Panel in August 2008 [1], Cloud users regarded security because the high challenge with seventy five of surveyed users distressed concerning their crucial business and IT systems being susceptible to attack. Whereas security threats from external agents are widespread, malicious service suppliers should even be taken into thought. Since on-line information nearly always resides in shared environments (for instance, multiple virtual machines running on the identical physical device), ensuring security and privacy on the cloud may be a non trivial task. Once talking concerning security and privacy of knowledge in the cloud, it's vital to get down the necessities that a knowledge sharing service should give so as to be thought-about secure.

We list down here a number of the foremost primary necessities that a user would wish in an exceedingly cloud primarily based information sharing service:

Data Confidentiality: Unauthorized users (including the cloud service provider), shouldn't be ready to access data at any given time. Information ought to stay confidential in transit, at rest and on backup media.

User revocation: the information owner should be ready to revoke any users access rights to data the while not poignant alternative licensed users within the cluster.

Scalability and Efficiency: maybe {the biggest|the most important|the giantst} challenge faced by information

management on the cloud is maintaining measurability and potency within the face of vastly large user bases and dynamically dynamical data usage patterns.

2. FILE RETRIEVAL IN CLOUD STORAGE

2.1 Traditional Encrypted Search over Cloud Data

The process of authentication is employed by the information owner to attest the data users. The file set and its index are keep within the cloud when being encrypted by the information owner throughout the preprocessing and compartmentalisation stages. The information user searches the files similar to a keyword by causation a call for participation to the cloud server within the search and retrieval processes

The file will be retrieved by after conniving the connection scores, the position of the files similar to the keyword is picked and therefore the high k relevant files are sent back to the information user s mobile shoppers while not playacting any cryptography on these files.

The information user decrypts these files within the mobile shopper and recovers the first data

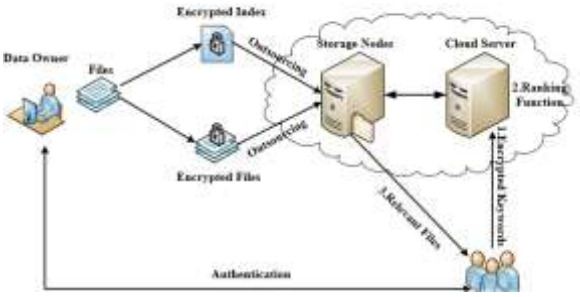


Fig -1: File Retrieval in Cloud Storage

2.1.1 Limitations

- File owner can access the other owner's file.
- It has increased time complexity and retrieval time.
- The key generated can be easily hacked.
- The unauthorised user has a vulnerability to attack the cloud.
- There is a statistics information leak.
- It is difficult to maintain, manage our deployed applications.

3. SYSTEM DESIGN

The most aim is to secure the user files in cloud storage. Initially, user uploads the files with their several Login id. The main purpose is to transfer the files with secured image and generating OPE (Order preserving Encryption) watchword. The aim of secured image is that unauthorized user cannot access the move into cloud. Files are encrypted into 2 elements like encrypted Index and encrypted files by exploitation FHS algorithmic rule.

The secured image is spitted into two image like source and key image by BVCS (Binocular Visual Cryptography schemes) algorithmic rule.

The encrypted file, source image and OPE are keep in cloud with encrypted file. If the user has to read or choose the actual file, the request should first be sent to the cloud service supplier. The supplier verifies the user id and file request, later it'll send OPE watchword and key image to user. Currently the user has got to send the key image to the cloud for accessing the files. The cloud matches the key image with the supply image it already has. Once each matches, it'll send the move into the shape of a Captcha and it will be downloaded. Hackers cannot hack the supply image or key image and Captcha are made only if it's a sound user.

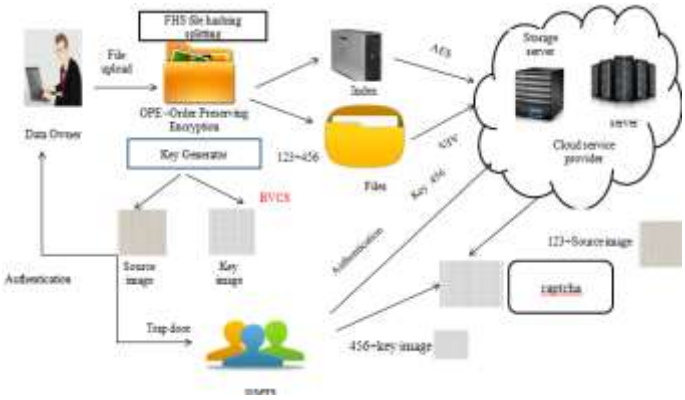


Fig-2: Proposed System Architecture

3.1 Unassailable File Procurement

To reduce the safety leakages, it's enforced with security sweetening in thought of the changed encrypted search procedure for statistics info leak and keywords-files association leak.

The file is uploaded with secured pictures and watchword that is generated exploitation File homomorphic secret writing algorithmic rule. (Order conserving Encryption).

The main goal of those modules is to forestall the unauthorized user gaining the access of this file.

Order Preserving Encryption

STEP 1: Encryption is an injective mapping (F) from the set of plaintexts (P) into the set of ciphertext (C): **F:P →C.**

STEP 2:is the deterministic encryption scheme with a symmetric key which preserves the order of plaintexts.

STEP 3: Let **m≤n, P={i| 1≤i≤m}** - is the set of plaintexts, **C= {i| 1≤i≤n}** - is the set of ciphertexts. **SEm,n= (Km,n, Em,n, Dm,n)** is the deterministic symmetric encryption scheme,

where **Km,n : {0,1}*→ {0,1}*** is the key generation function, **Em, n:P×{0,1}*→C** is the deterministic symmetric encryptionalgorithm, **Dm,n:C×{0,1}*→P** is the decryption algorithm, such that **∀ x ∈ P** and any valid key **k, x < x` ⇔ Em,n(x,k)< Em,n(x`,k).**

Input: tf

Output: E(tf)

1: for ti ∈T and 1 ≤ j ≤|F| do
2:Get E(tfij), E(tfij) R←{G(tfij),G(tfij)+1,...,H(tfij)}.
3: end for 4: return E(tf).

3.2 Bifurcate Ascription File

The primary purpose of encryption is to protect the confidentiality of digital information stored on computer system or transmitted via the internet or other computer system.

Modern encryption algorithm plays a vital role in the security assurance of IT system and communication as they can provide not only confidentiality but also the integrity.

The Cloud provider uploaded the User files that will be splitted into two parts using FHS(Files Hashing Algorithm) like encrypted Index and encrypted files by using AES (Advanced Encryption Standard)Algorithm before sending them to the cloud.

The encrypted file have been stored in storage node with their respective file Id.

Advanced Encrption Algorithm

STEP 1:KeyExpansion—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 one more.

STEP 2:Initial round key addition:

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

STEP 3:9, 11 or 13 rounds:

SubBytes— non-linear substitution step where each and every byte is replaced with another according to a lookup table.

ShiftRows— transposition step where the last three rows of the state are shifted cyclically a certain number of steps in shiftrows.

MixColumns— linear mixing operation which operates on the columns of the state, combining the four bytes in each and every column.

AddRoundKey

STEP 4:Final round (making 10, 12 or 14 rounds in total):

SubBytes

ShiftRows

AddRoundKey

3.3 Image Split-up Using BVCS

Image splitting is a technique most often used to slice a larger images into smaller fragments to make it load faster .Cloud provider upload the user file with secured image, that image should be splitting into two images like source and key image with the help of BVCS (Binocular Visual Cryptography schemes) algorithm rule. The key image and the password will be send to the particular user and the necessary file can then be downloaded. The password is generated which s then splitted into source image and key image and they are stored to the user and cloud server.

Binocular Visual Cryptography Scheme Algorithm

STEP 1: The model is that it maximize the recovered image in (2, n)-BVCSs.

STEP 2: The objective is that it reduces the interference in the SIRDSs, hence it minimizes the alternation probability of SIRDSs.

STEP 3: The (2, n)-BVCS encryptor.

STEP 4: The Hiding of the shared pixel in single image random dot stereogram (SIRDSs)by using a encryption algorithm and an binocular VCS (BVCS) called(2,n) BVCS.

STEP 5: The construction rule generator produces construction rules based on the structure of the BVCS and also the pixel density d of SIRDSs.

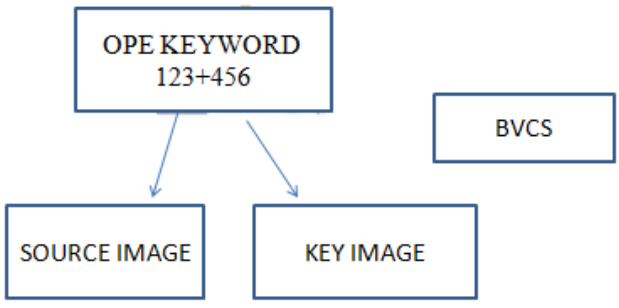


Fig- 3: BVCS scheme

3.4 File Substantiational Data

Verification is that the act of reviewing, inspecting or testing a technical standards. Currently the user has got to send the key image to the cloud for accessing the files. The cloud matches the key image with the supply image it already has. Once each matches, it'll send the move into the shape of a captcha. It will be downloaded simply. It is the act of reviewing, inspecting or testing in order to determine service or system meets regulative or technical standards.

4. RANKING FUNCTION:

Cloud server calculates the relevance scores and return top-k relevant files according to the searching query from data user. The calculation scheme in [31] is used in our scheme. Note that due to the order preserving index, any other relevance scores calculation method [31], [32], [33], [47] can also be employed. TEES calculates the relevance score as Equation (7): Score(Ws,Fc) = X w∈Ws 1 |Fc|×(1 + lnfc,w)×ln(1 + D fw) (7) Here Ws is the keyword set to be searched; Fc is a certain file in the file set; fc,w denotes the TF of the keyword w in the file Fc; |Fc| is the total length of Fc; fw is the number of files containing the keyword w and D is the total number of files. When performing a single keyword search, the IDF factor in Equation (7) is constant. Thus, we simplify the equation as follows:

Score(w,Fc) =

1 |Fc|×(1 + lnfc,w) (8) The cloud server sends back the top-k relevant files after ranking the scores using this relevance score calculation algorithm.

Top-k Ranking Function

Input: w,k

Output: topFiles

if this request is sent by a ”legal” user then for each file Fc ∈ F do Calculate Score(w,Fc

end for

end if

if this request is sent by a overdue user then

for each file Fc ∈ F do Calculate Score(w,Fc) but with a warning.

end for

else Return ”No Permission”.

end if

Rank the scores to get top-k files topFiles = {topF1,topF2,...,topFk}.

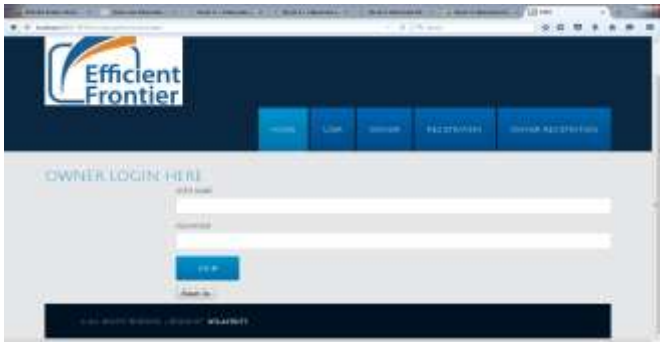
return topFiles.

5. EXPERIMENTAL ANALYSIS

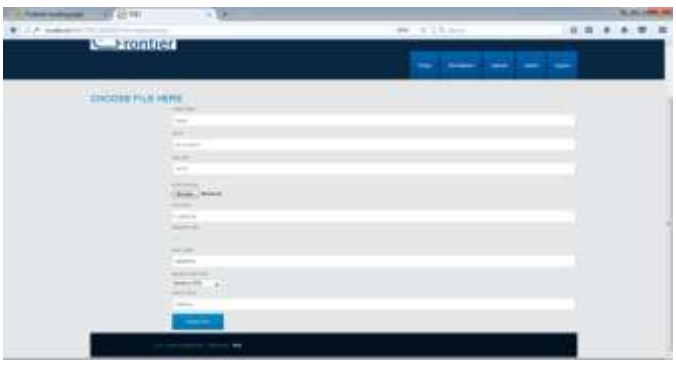
5.1Homepage

5.2 User Login

5.3 Owner Login



5.4 Owner Uploading Files



5.5UserRequestingFiles

5.6 Entering File Key

5.7 Final Output

6. SYSTEM ANALYSIS

- It is reducing File Search and Retrieval Time.
- The encryption is identity based cryptography scheme
- It has server information acquisition control.
- The design is to prevent the attacker to obtain the information in the cloud.
- Reducing Traffic Overhead in the cloud.
- It provides more secure to the service.
- Unauthorised users cannot be accessed the files in the cloud.

6.1 Performance Measures

Existing system:

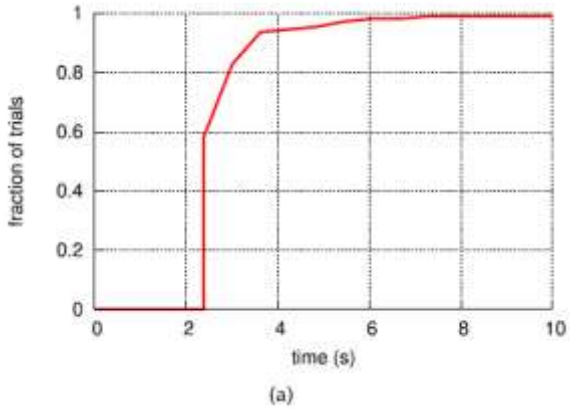


Chart-1: existing system

Proposed System:

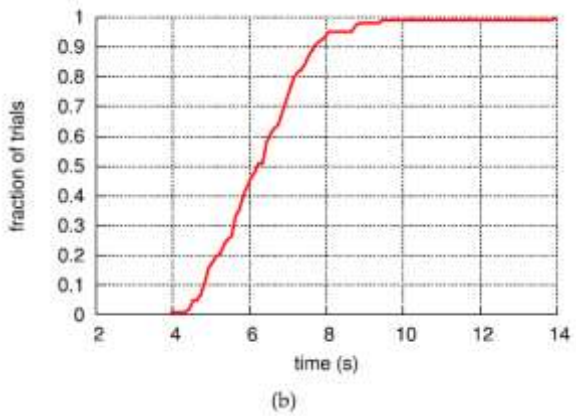


Chart-2: proposed system

6.2 Applications

- It achieves the efficiencies through employing and modifying the ranked keyword search as the encrypted search platform basis, which has been widely employed in the cloud storage systems.
- It saves significant energy compared to the traditional strategies featuring a similar security level.
- It enables the user to retrieve the files in a secured manner and protect from the unauthorized users.

7. CONCLUSION AND FUTURE ENHANCEMENT

Data owners can remotely store their data to the cloud and realize the data sharing with users. The proposed work is an identity based data integrity scheme for secure cloud storage, which supports data sharing with the sensitive information. The Cryptography scheme is used for secure protection. It started with a thorough analysis of the traditional encrypted search system, network traffic and search time efficiency.

Encryption is the most effective way to achieve the data security. Hackers cannot hack the source image or key image and Captcha will be produced only when it is a valid user. It can provide data integrity and authentication for the service in the cloud.

8 REFERENCES

[1].Sanjeet kumar nayak, somnath tripathy, secure and economical privacy conserving obvious information possession in cloud storage, IEEE transactions on service computing, vol: 14, no.8, Oct 2018.

[2]. B. Wang, S. Yu, W. Lou & Y. T. Hou h, Privacy-Preserving Multi-Keyword Fuzzy Searchover Encrypted information within the Cloud IEEE transation on cloud computing,vol.22,no.9,aug 2017.

[3]. S. Hou, T. Uehara, S. Yiu, L. C. Hui, & K. Chow. Privacy conserving Multiple Keyword look for Confidential Investigation of Remote Forensics, IEEE transactions on info Foresnsics and Security.,vol.5,no.3,sep 2016.

[4]. N. Cao & C. Wang, M. Li, K. Ren, & W. Lou, Privacy-Preserving Multi-Keyword hierarchical Search over Encrypted Cloud information IEEE transactions on Parallel and Distributed System,vol.10,no.7,sep 2016.

[5]. FairouzSher ALI, Songfeng metal, Searchable secret writing with Conjunctive Field Free Keyword Search theme, ACM conference on pc and communicative security,vol.20,no.8,oct 2016.

[6]. Q. Chai & G. Gong, Verifiable rhombohedral Searchable secret writing For Semi-honest-but-curious Cloud Servers, ACM conference on pc and communicative security,vol.4,no.3,sep 2014.