Practical Privacy-Preserving In Cloud Image Repositories

M.Sivaprakash, R. Vidyavathi and G. Nagarajan

Abstract: ***Cloud computing is an emerging technology utilized widely due to its various advantages. However the major issue faced here is security in maintaining files. Our proposed work focuses on storing and retrieving of image data in secure way in cloud through double step verification. In general, cryptography is utilized to store data in secure way. The key logic is when there is less security automatically data will be reveal to unauthorized users. In our proposed method, these issues are overcome through double step verification. Initially image has been encrypted through Attribute Based Encryption (ABE). In addition to provide better security repository encryption has been implemented by RC4 approach. This will provide better security for user data in cloud through this two step verification. To ensure originality of user image watermarking technique has been implemented. Therefore it ensures without user knowledge an unauthorized user could not get the original image. Hence our system achieves maximum security compared to other existing approaches.***

Index Terms: security, cloud, ABE, repository encryption and watermarking.

I. INTRODUCTION

The cloud is designed to hold a large number of encrypted documents. With the appearance of distributed computing, developing number of customers and driving associations have begun adjusting to the private stockpiling redistributing. This permits asset compelled customers to secretly store a lot of encoded information in cloud requiring little to no effort. Distributed storage administrations have a few focal points, for example, convenience and cost sparing, and they are generally utilized in numerous fields. Be that as it may, a few difficulties are related with them. With the expanding notoriety of distributed storage, security issues have turned into a critical factor confining its advancement. To counter the data spillage, information proprietors and endeavors normally re-appropriate the encoded business information, instead of the plaintext information, to distributed storage servers. Visual information is in charge of one of the biggest offers of worldwide Internet traffic in both corporate and individual use situations. The measure of pictures, designs, and photographs being produced and shared each day, particularly through cell phones, is developing at a regularly expanding rate. The regular way to deal with location protection in this setting is to scramble touchy information before re-appropriating it and run all calculations on the customer side. Anyway this forces unsuitable customer overhead, as information should ceaselessly be downloaded, decoded, prepared, and safely re-transferred.

To address these difficulties we propose another safe structure for protection safeguarding redistributed capacity, pursuit, and recovery of vast scale, progressively refreshed picture archives. We base our proposition on IES-CBIR, a novel Image Encryption Scheme (IES) with Content-Based Image Retrieval (CBIR) properties. Key to the structure of IESCBIR is the perception that in picture preparing, unmistakable component types can be isolated and encoded with various cryptographic calculations. For instance, picture shading and surface information can be isolated so that CBIR in the scrambled space can be performed on one component type while alternate remains completely randomized and ensured with semantically-secure cryptography.

Data Security Properties:

As mentioned earlier there are some properties we need to ensure with data when utilizing the cloud:

Privacy:

Privacy is one of the more imperative issues to manage in the cloud and in system security when all is said in done. Security guarantees that the individual data and character of a CSC are not uncovered to unapproved clients. This property is most vital to the CSC, particularly when they manage delicate information.

Confidentiality:

This is identified with information security since this is the property guaranteeing that the information that has a place with a CSC isn't uncovered to any unapproved parties. In open mists, the CSP is essentially in charge of verifying the CSC's information. This is especially troublesome due to multi occupancy, since various clients approach a similar equipment that a CSC stores its information. A few suppliers use work booking and asset the board, however most suppliers utilize virtualization to expand the utilization of equipment. These two techniques enable assailants to have full access to the host and cross-VM side channel assaults to separate data from an objective VM on a similar machine.

Integrity:

The integrity of information alludes to the certainty that the information put away in the cloud isn't modified in any capacity by unapproved parties when it's being recovered, for example you get out what you put in. To guarantee this, CSPs must ensure that no outsider approaches information in travel or information away. Just approved CSCs ought to most likely change their information.

Availability:

This property guarantees that the CSC approaches their information, and are not denied access incorrectly or because of vindictive assaults by any element. Assaults like refusal of-administration are

Revised Manuscript Received on July 05, 2019.

R.Vidyavathi, Department of Computer Science, K.S.R. College of Engineering(A), Tiruchengode, India,

M.Sivaprakash,, Department of Computer Science, K.S.R. College of Engineering(A), Tiruchengode, India,

commonly used to preclude accessibility from securing information..

II. RELATED WORKS

W. Lu, et al (2009), describes the issue of picture recovery from an encoded database, where information classification is saved both in the capacity and recovery process. The paper centers around picture include insurance systems which empower comparability correlation among ensured highlights. By using both flag preparing and cryptographic methods, three plans are researched and thought about, including bit-plane randomization, irregular projection, and randomized unary encoding. Exploratory outcomes demonstrate that protected picture recovery can accomplish tantamount recovery execution to customary picture recovery strategies without uncovering data about picture content. This work advances the region of secure data recovery and can discover applications in secure online administrations for pictures and recordings.

C.-Y. Hsu, et al (2012), security has gotten extensive consideration however is still generally disregarded in the sight and sound network. Consider a distributed computing situation where the server is asset bottomless, and is fit for completing the assigned errands. It is imagined that protected media applications with security conservation will be dealt with truly. In perspective on the way that scale-invariant component change (SIFT) has been generally received in different fields, this paper is the first to focus on the significance of protection saving SIFT (PPSIFT) and to address the issue of secure SIFT include extraction and portrayal in the encoded area. As the majority of the tasks in SIFT must be moved to the scrambled space, we propose a protection saving acknowledgment of the SIFT strategy dependent on homomorphic encryption. We appear through the security investigation dependent on the discrete logarithm issue and RSA that PPSIFT is secure against ciphertext just assault and known plaintext assault. Test results acquired from various contextual analyses exhibit that the proposed homomorphic encryption-based security saving SIFT performs equivalently to the first SIFT and that our strategy is valuable in SIFT-based protection saving applications.

M. Naehrig, et al (2011), presents data recovery assignments while saving information privacy is an attractive capacity when a database is put away on a server kept up by an outsider specialist co-op. This paper tends to the issue of empowering content-based recovery over encoded sight and sound databases. Pursuit lists, alongside sight and sound records, are first scrambled by the substance proprietor and after that put away onto the server. Through mutually applying cryptographic systems, for example, request safeguarding encryption and randomized hash capacities, with picture handling and data recovery strategies, secure ordering plans are intended to give both security insurance and rank-requested inquiry ability. Recovery results on a scrambled shading picture database and security investigation of the safe ordering plans under various assault models demonstrate that information secrecy can be safeguarded while holding exceptionally great recovery execution. This work has promising applications in secure sight and sound administration.

Z. Qin, et.al (2014) describes the sum and accessibility of client contributed picture information have been drastically expanded amid the previous ten years. Well known interactive media interpersonal organizations, for example Flash, regularly use client picture information to develop client conduct models, social inclinations, and so on., with the end goal of powerful promotion, better client maintenance and fascination, and numerous others. Existing practices of information use, be that as it may, genuinely disintegrate clients' close to home protection and have prompted expanding reactions and enactment weights. In this paper, we expect to build a protection saving component discovery conspire over encoded picture information. The proposed framework empowers an invested individual to play out an assortment of picture highlight discovery assignments, incorporating visual descriptors in MPEG-7 standard, while securing client protection identifying with picture substance. We actualize a model framework dependent on fairly homomorphic encryption conspire and the benchmark Caltech256 database. The exploratory outcomes demonstrate that our framework can ensure viable picture highlight location without giving up client protection.

Qia Wang, Wenjun Zeng presents protection is a basic issue when the information proprietors redistribute information stockpiling or handling to an outsider figuring administration, for example, the cloud. In this paper, we distinguish a distributed computing application situation that requires all the while performing secure watermark discovery and protection safeguarding interactive media information stockpiling. We at that point propose a compressive detecting (CS)- based structure utilizing secure multiparty calculation (MPC) conventions to address such a prerequisite. In our system, the mixed media information and mystery watermark design are introduced to the cloud for secure watermark recognition in a CS space to ensure the protection. Amid CS change, the security of the CS framework and the watermark design is ensured by the MPC conventions under the semi-genuine security display. We infer the normal watermark recognition execution in the CS area, given the objective picture, watermark design, and the measure of the CS lattice (yet without the CS grid itself). The accuracy of the inferred execution has been approved by our trials. Our hypothetical examination and test results demonstrate that safe watermark recognition in the CS area is plausible. Our system can likewise be stretched out to other community oriented secure flag preparing and information mining applications in the cloud.

III. PROPOSED SYSTEM

In this section, the implementation of our proposed system is explained briefly. Images are stored in our system in secure way through encryption and to ensure originality of user water marking has been implemented. In addition to provide more security in our system repository encryption has been implemented.

Need for securing data:

- Securing data in cloud is a difficult process because the cloud is honest but curious server.
- Encrypting and outsourcing data in cloud ensures data security in cloud, but leakage of key leads to disclosure of data.
- Recent incidents have

provided clear evidence that privacy should not be expected to be preserved by cloud providers.

- Proper authentication and key management is not available.

Working process of our proposed method:

User module:

In this module, users are the client. Client can create account in the cloud and can create a repository for individual. User can store their image on their respective repository and can store their image with privacy using encryption scheme and they can search the image through key with respective query. Where they can both add their own images and/or search using a query image. Users can also request access to stored images from their creators/owners.

Key distribution service and watermarking:

Key distribution and management process are handled in this module. User requests the key to encrypt the image and stored in repository. Here separate key is generated for storage space of image and for image encryption is generated. Therefore image is stored in repository in encrypted format. Before storing data in cloud water marking is done by owner of the data and then encrypted and stored in cloud.

Image storing and indexing:

When the cloud receives an encrypted image for storage it extracts its relevant features and indexes the image based on these features. The same action is performed for a query image, which after being encrypted by a user with repository key, is then processed by the cloud and has its features extracted and matched with the repository's index.

Decrypting the image:

User searches the image through query. The reply to a query will contain k number of encrypted images and respective metadata. Initially user gets the result of image with watermarked content. With the decryption key of respective user image can be obtained with originality assurance. If a user needs original image of particular data he/she should need respective repository key to obtain original image. To achieve this user should request particular repository key to respective user therefore without owners knowledge original image cannot be shared in cloud.

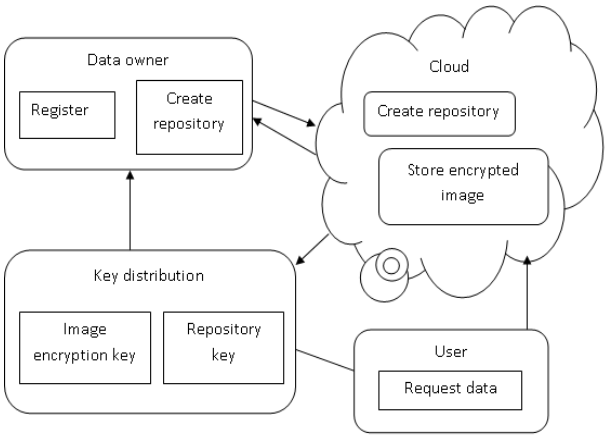

Fig 1: Proposed System Architecture

Attribute-Based Encryption (ABE):

Attribute - based encryption (ABE) is a public – key algorithm based one to numerous encryptions that enables clients to encrypt and decode information dependent on client qualities. In their unique circumstance, the job of the gatherings is taken by the characteristics. Consequently, the access structure will contain the approved arrangements of properties. They confine the consideration regarding monotone access structures. Be that as it may, it is likewise conceivable to acknowledge general access structures utilizing the procedures by having the property as a different trait through and through. Hence, the quantity of qualities in the framework will be multiplied. Starting now and into the foreseeable future, except if expressed something else, by an entrance structure we mean a monotone access structure.

In ABE conspire both user secret key and the cipher - text are related with a lot of characteristics. A client can unscramble the figure content if and just if no less than an edge number of qualities cover between the figure content and client mystery key. Unique in relation to conventional open key cryptography, for example, Identity-Based Encryption, ABE is executed for one-to numerous encryption in which figure writings are not really scrambled to one specific client, it might be for more than one number of clients.

RC4 ALGORITHM:

RC4 is a stream cipher type. It processes unit or input data at one time. Unit or data is a byte or even sometimes bits. In this way, the encryption or decryption can be implemented on the length of the variable. This algorithm does not have to wait a certain amount of data input before it is processed or add extra bytes to encrypt. Another type is a block cipher that processes at the same time a certain amount of data (typically a 64-bit or 128-bit blocks).

In cryptography, RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output key stream is not discarded, nonrandom or related keys are used, or a single key stream is used twice; some ways of using RC4 can lead to very insecure cryptosystems such as WEP.RC4 generates a pseudorandom stream of bits (a key stream) which, for encryption, is combined with the plaintext using bit - wise exclusive - or; decryption is performed the same way (since exclusive - or is a symmetric operation).

IV. EXPERIMENTAL ANALYSIS

Hence our proposed work has been implemented using java swing and my SQL data base. It will be connected to real time cloud to show accuracy of result. The performance has been analyzed using the parameter called security. As we discussed before encrypting and storing image in cloud will provide security however if encrypted key is identified to attackers automatically entire data will be revealed. Experimental setup of our proposed is shown below.

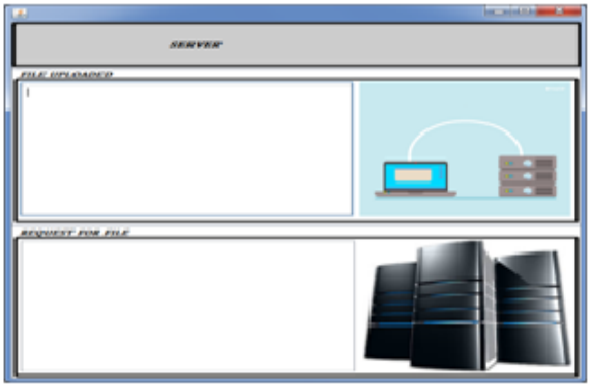

Fig 4.1: Main server

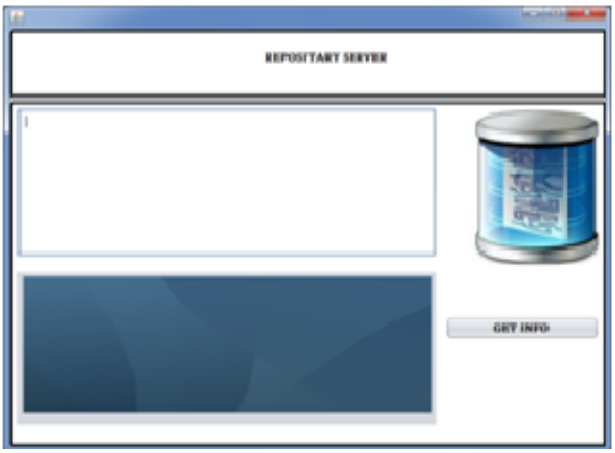

Fig 4.2: Repository server

Fig 4.3: Water marking and encryption

Fig 4.4: Watermarked image

Fig 4.5: Original image request transmitted to user

Fig 4.6: Retrieval of image

Fig 4.1 and fig 4.2 shows the utilization of main server and repository server which is utilized in our system. Image encrypted and stored in main server and repository key is generated for enhancing security. Fig 3 shows water marking approach and encryption key to encrypt the file. If user need particular image respective key is needed to decrypt the file even though watermarked image will be shown. To attain original image respective image repository key should be needed and should be requested to original user of image and with the knowledge of original user particular image will be retrieved.

V. RESULT AND DISCUSSION

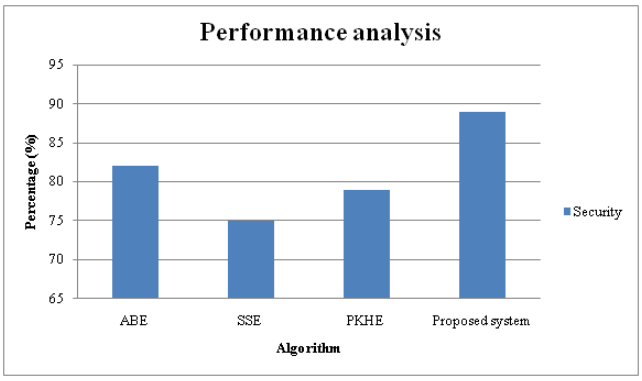

Fig 5.1: Performance analysis

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

However existing methods provide better security to store and retrieve our data from cloud. As we discussed before the key logic of extracting user data can be done if respective key has been identified by any attackers. Hence to overcome this issue we propose double step verification such as encrypting image as well as encrypting repository. If an authorized user wants a particular image he or she should have respective repository key. If key is not available then, water marked image will be delivered to user. Hence our system level of security is shown in above graph.

VI. CONCLUSION

In this paper, the main objective of securing data in cloud has been implemented. However existing methods secures data in efficient way by utilizing various cryptography approaches, the key point of drawback is if the encryption key is identified by attacker or misbehaving persons then user own data will be revealed to an unauthorized person. Therefore an efficient approach should be needed to ensure secure data storing and retrieving process. Hence our proposed system achieves better security in terms of double step verification. In addition the originality of data also ensured through watermarking approach. Hence these shows without owner's information unauthorized user could not access original data of other users.

REFERENCES

1. W. Lu, et al. Secure image retrieval through feature protection. In Proc. of ICASSP, 2009.
2. C.-Y. Hsu, et al. Image feature extraction in encrypted domain with privacy-preserving SIFT. IEEE TIP, 21.11 (2012): 4593-4607.
3. C.-Y. Hsu, et al. Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. In Proc. of SPIE, 2011.
4. M. Naehrig, et al. Can homomorphic encryption be practical?. In Proc. of CCSW, 2011.
5. W. Lu, et al. Enabling search over encrypted multimedia databases. In Proc. of SPIE, 2009.
6. Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft. Privacy-preserving face recognition. In Proc. of PET, 2009.
7. M. K. Khan, J. Zhang, and K. Alghathbar. Challenge-response-based biometric image scrambling for secure personal identification, Future Generation Computer Systems. 27.4 (2011): 411-418.
8. Z. Qin, J. Yang, K. Ren, C. W. Chen, and C. Wang. Towards efficient privacy-preserving image feature extraction in cloud computing. In Proc. of MM, 2014.
9. Z. Qin, J. Yan, K. Ren, C. W. Chen, C. Wang, and X. Fu. Privacy-preserving outsourcing of image global feature detection. In Proc. of GLOBECOM, 2014.
10. T. Sikor. The mpeg-7 visual standard for content description-an overview. IEEE TCSVT, 11.6 (2001): 696–702.

AUTHORS PROFILE

S. Sivaprakash, Assistant Professor, Department of Computer Science and Engineering, K.S.R College of Engineering, K.S.R Kalvi Nagar, Tiruchengode- 637 215.

R. Vidyavathi, , Department of Computer Science and Engineering, K.S.R College of Engineering, K.S.R Kalvi Nagar, Tiruchengode- 637 215.

G. Nagarajan, Assistant Professor, Department of Computer Science and Engineering, K.S.R College of Engineering, K.S.R Kalvi Nagar, Tiruchengode- 637 215.