International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 10, Issue 1, Jan. 2021, pp.140-144, ISSN 2278 -1412

Protected Anti-Collusion Data allocation design for Encryption Data in Cloud

Ranjana chaudhary[1], Chhatrapani Gautam[2]
[1]M.tech scholar, VITS Satna(M.P.) , ranjanachaudhary.93@gmail.com
[2]Assistant Professor, VITS Satna(M.P.) , acpg.77@gmail.com

Abstract- Data security is major challenges today. It plays a crucial role in modern energy infrastructure; and how to process a huge amount of data received from these devices. Cloud computing, a technology that has procedure resources on demands, could be a wise candidate to deal with these challenges since it's several smart properties like energy saving, worth saving, agility, scalability, and flexibility. Consumer can furthermore do a resourceful and inexpensive approach for info sharing among group members inside the cloud with the characters of low maintenance and small management value. Consequently, our purpose is offer security guarantees for sharing info files since they're outsourced. Unfortunately, because of the frequent modification of the membership, sharing info whereas providing privacy-preserving remains a tough issue, particularly for a scepticism cloud due to the collusion attack. During this work, we tend to tend to propose a secure info sharing scheme for dynamic members. Firstly, we tend to tend to propose a secure methodology for key distribution with none secures communication channels, and additionally the users can securely acquire their personal keys from group manager. another time once they're revoked. Thirdly, we tend to look after the design from collusion attacks that recommend that invalidate users cannot get the first file although they conspire with the untrusted cloud. Finally, our scheme will do fine efficiency, that suggests previous users needn't to update their personal keys for the case either a new user joins inside the cluster or a user is revoked from the cluster.

Keywords :Data security, Secure computing, User encryption, Data encryption, Cloud security

I. Introduction

Cloud computing refers to each the applications delivered as services over the web and therefore the hardware and computer programmer within the knowledge centers that offer those services. The services themselves have long been remarked as package as a Service (SaaS).a Some vendors use terms like IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to explain their merchandise, however we tend to shun these as a result of accepted definitions for them still very wide. The road between "low-level" infrastructure and a higher-level "platform" isn't crisp. We tend to believe the 2 square measure a lot of alike than completely different, and that we contemplate them along. Similarly, the connected term "grid computing," from the superior computing community, suggests protocols to supply shared computation and storage over long distances, however those protocols didn't cause a package atmosphere that grew on the far side its community. The info center hardware and package is what we are going to decision a cloud. Once a cloud is formed out there during a pay-asyou-go manner to the overall public, we tend to decision it a public cloud; the service being oversubscribed is utility computing. we tend to use the term personal cloud to check with internal knowledge centers of a business or alternative organization, not created out there to the overall public, after they square measure giant enough to learn from the benefits of cloud computing that we tend to discuss here. Thus, cloud computing is that add of SaaS and utility computing, however doesn't embody tiny or mediumsized knowledge centers, though these have faith in virtualization for management. Individuals are often users or suppliers of SaaS, or users or suppliers of utility computing. We tend to specialize in SaaS suppliers (cloud users) and cloud suppliers that have received less attention than SaaS users. Figure one makes provider-user relationships clear. In some cases, identical actor will play multiple roles. As an example, a cloud supplier may additionally host its own customer-facing services on cloud infrastructure.

Fig.1.1 Users and providers of cloud computing

Any application wants a model of computation, a model of storage, and a model of communication. The applied mathematics multiplexing necessary to attain elasticity and also the look of infinite capacity obtainable on demand needs automatic allocation and management. In apply; this is often finished virtualization of some type. Our view is that completely different utility computing offerings will be distinguished supported the cloud system software's level of abstraction and the level of management of the resources. Amazon EC2 is at one finish of the spectrum. Associate degree EC2 instance appearance much like physical hardware, and users can management nearly the complete software package stack, from the kernel upward. This low level makes it inherently tough for Amazon to supply automatic scalability and failover as a result of the semantics related to replication --and different state management problems are extremely application-dependent. At the other extreme of the spectrum area unit application domain-specific platforms such as Google AppEngine, which is targeted solely at ancient net applications, imposing associate degree application structure of unpolluted separation between a unsettled computation tier and a stateful storage tier. AppEngine's impressive automatic scaling and high-availability mechanisms, and the proprietary MegaStore information storage available to AppEngine applications, all consider these constraints. Applications for Microsoft's Azure area unit written using the .NET libraries, and compiled to the Common Language Runtime, a language-independent managed setting. Thus, Azure is intermediate between application frameworks like AppEngine and hardware virtual machines like EC2.

Cloud computing, the long-held dream of computing as a utility, has the potential to transform an outsized part of the IT trade, creating software even a lot of attractive as a service and shaping the approach IT hardware is designed and purchased. Moreover, corporations with large batch-oriented tasks will get results as quickly as their programs will scale, since using 1,000 servers for one hour prices no quite using one server for 1,000 hours. The framework is considerably more versatile than AppEngine's, but still constrains the user's selection of storage model and application structure. This elasticity of resources, without paying a premium for big scale, is unprecedented within the history of IT. Developers with innovative ideas for new web services not need the large capital outlays in hardware to deploy their service or the human expense to work it. They need not be concerned regarding over provisioning for a service whose quality doesn't meet their predictions, thus wasting expensive resources, or under provisioning for one that becomes wildly standard, so missing potential customers and revenue.

II. Problem and Proposed Methodology

In this presented a storage system that permits secure information sharing on untrustworthy servers supported the techniques that dividing files into file groups and encrypting every file group with a file-block key. The exploited and combined techniques of key policy attribute-based encoding, proxy re-encryption and lazy re-encryption to realize fine grained information access control while not disclosing data contents. Searchable Encryption (SE) schemes provide security and privacy to the cloud data. The existing SE approaches enable multiple users to perform search operation by using various schemes like Broadcast Encryption (BE), Attribute-Based Encryption (ABE), etc. However, these schemes do not allow multiple users to perform the search operation over the encrypted data of multiple owners.

In the proposed scheme, an image owner having a low computational power (e.g., mobile devices) connects to the cloud. The user desires to use the storage capacity and cloud computational power. He/She stores the images securely and wants to retrieve or access them afterwards. The image owner has a collection of his sensitive images. However, the image owner wants that his collection must be secure enough before outsourcing to the cloud for further processing. Figure 4.1 shows the System framework of proposed algorithm. In this figure only encryption algorithm has been explored. User authentication using image captcha is explored in section while reusing the system framework of Figure 2. The security enhancing process which performs in image owner's machine uses images obtained from social media sites such as flicker to create masks for the original image with a lightweight encryption algorithm to further enhance the security of the image. The identity of the masks called flk_ID and the keys which are used for encryption process are kept secret. The image owner creates the key matrix of the keys used for encryption and ID of the masks. Then the key matrix encryption is performed by the image owner. In key encryption λ-values and λ-vector are created with a secret index of the image. More about λ-values and λ-vector is explained in section. Here in this section λ-values and λ-vector are created. After encrypting the image and keys, image owner sends the encrypted image to the cloud for storage with the λ-values and secret index and λ-vectors are sent to the authorized cloud user. When a cloud user wants to retrieve the image, it sends the request to the cloud. For sending the request he/she extracts the keys and creates the index for searching the remotely stored image collection, and then sends the index to the cloud server. The cloud performs the requested computation on the encrypted images and returns the results in the encoded forms to the image owner. The image owner decodes the received results to get the images on which the requested computations are done by the cloud.

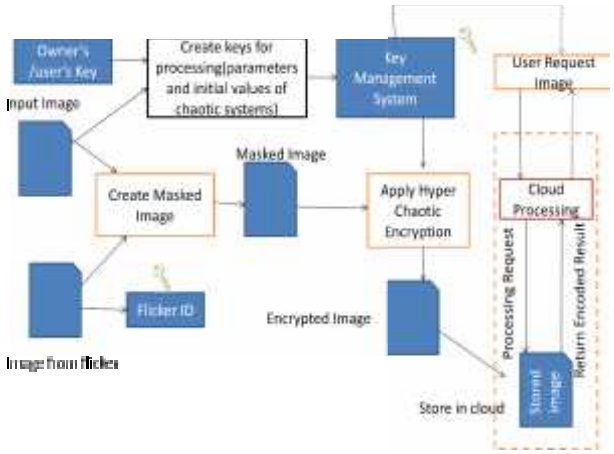

Fig.2 Basic structure of encryption process

By using the following equation flicker ID (flk_ID) is created for retrieving the images from flicker. Results show that this hash function little bit degraded the collision rate between generated IDs.

$$flk\_ID = h2(x,y,h1(I)) \quad (1)$$

$$h1(I) = mod(M \times N, E) \quad (2)$$

where I = original Image
M, N = dimension of I
x & y = coefficient of correlation of adjacent pixel
and E = entropy of pixels

Firstly, the whole masked image is divided into 8 equal blocks and then a pseudo-random array is generated from the below logistic map (equation (3)), containing 8 pseudo-random numbers which is used to disorder the actual arrangement of image blocks.

For an initial value of x0, perform some iteration(bI) and obtain a new x0 by using the following equation:

$$xn+1 = rxn(1 - xn) \quad (3)$$

where xn = population of nth generation
r = growth rate

After obtaining a new value for x0, randomly shuffle all the blocks by using the equation (4). For block permutation the initial value x0 is referred to as b0. Random permutations = [mod(b0 ×1014, 8)] (4)

Continuously iterate the logistic map and perform equation (4) until 8 different values are not obtained which are between 1 and 8. This sort of method will make the encryption process more confusing and complex as it adds an extra step to the encryption process, and moreover the length of the key will become longer.

III. Simulation Results

In this analysis on the results using encryption method implemented in HCIF tool in MATLAB, there will come on more result for image.

There are three different parts that is registration part, Hyper Chaotic Searchable Image Encryption part and verification part .

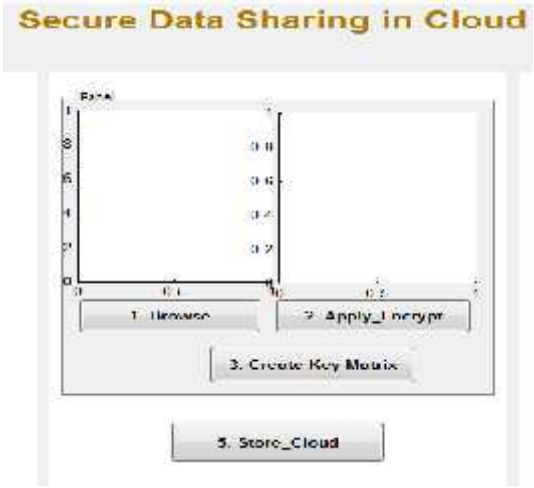

Fig.3 Hyper Chaotic Searchable Image Encryption part

Fig.3 Hyper Chaotic Searchable Image Encryption part on window of HCIF which is used in MATLAB for the implementation of the proposed work.

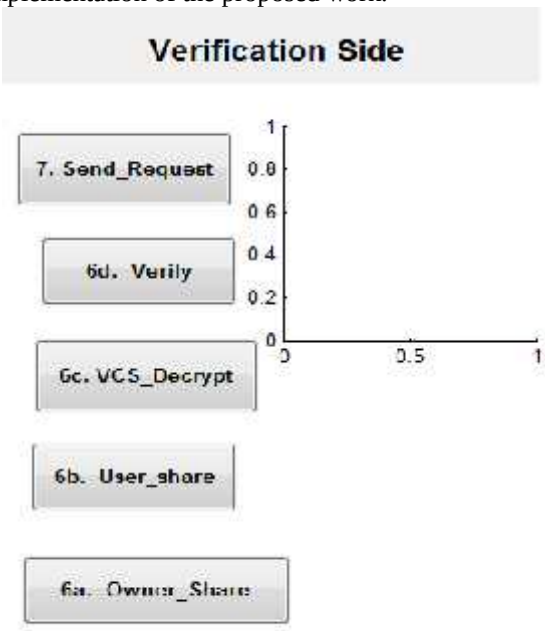

Fig.4 verification part

Fig.4 Verification part on window of HCIF which is used in MATLAB for the implementation of the proposed work.

Fig.5 Apply encrypt on input image

In this Fig.5 demonstrates the apply encryption process. In this fig. applied the encryption process on input image then we get the XoR masked image. After sharing process user take input image for transmission by browsing procedure and then encrypted image is applied on input image which gives key matrix and also store data in cloud server and all process is taken like owner shares user shares and VCS decryption technique step by step and verification is done before sending request.

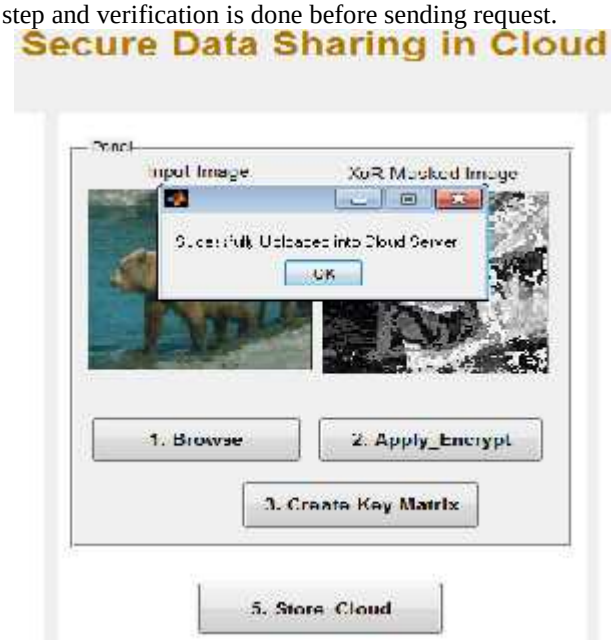

Fig.6 data successfully uploaded into cloud server

This Fig.6 represents the data successfully in cloud server. In this fig. after apply encrypt then create key matrix and then stored the data in cloud server.

Fig.7 send request window

This fig.7 shows obtain reconstructed image.

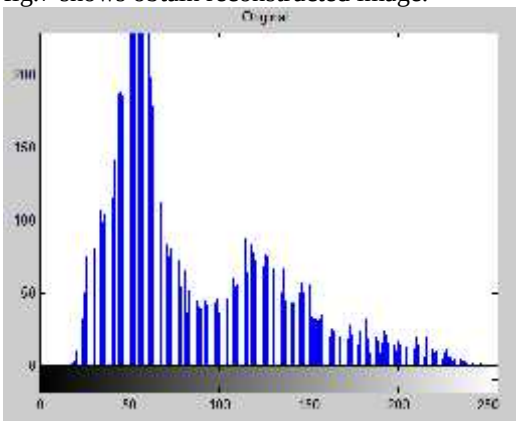

Fig.8 original data

Fig. 8 graphical representation of the amplitude level of input or original image

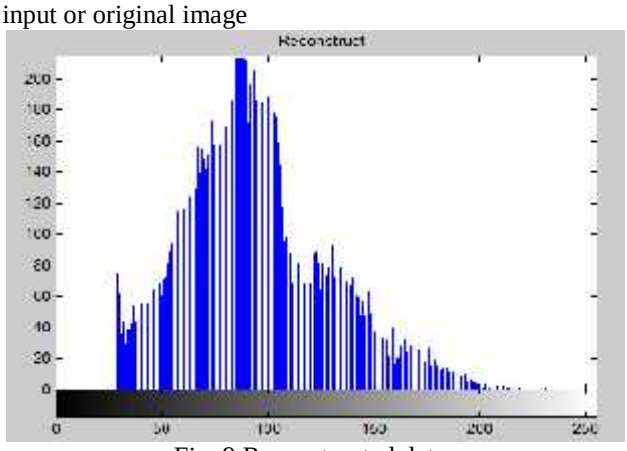

Fig. 9 Reconstructed data

Fig. 9 shows the amplitude level of reconstructed image after encryption.

.

IV. Conclusion

Data Sharing and Collaboration in the Cloud is fast becoming available in the near future as demands for data sharing continue to grow rapidly. In this section, present a survey on enabling secure and confidential data sharing and partnership using Cloud computing method.

In the research work examined definitions related to Cloud computing and privacy. Then looked at privacy and security issues affecting the Cloud followed by what is being done to address these issues.

In this proposed work a secure searchable image encryption using hyper chaos in cloud environment is proposed. Which provide the security to the images stored on the cloud server. It is the extension of the security algorithm for image .Our algorithm consists of two phases. The first phase uses the work of for first level of encryption process and the second phase uses the method presented in this dissertation using key & image encryption through hyper chaos and user authentication through image captcha. By virtue of both phases being secure because of hyper chaos, the correct results of searching to the correct user can be assured .Three layers of security is provided here instead of two layers. Two layers at the time of authentication and one layer at encryption time.

References

[1] Deepthi Rao, D.V.N. Siva Kumar and P. Santhi Thilagam . An Efficient Multi-User Searchable Encryption Scheme without Query Transformation over Outsourced Encrypted Data.. ACS/IEEE 2018.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. “A View of Cloud Computing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[7] D. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[8] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[9] M. Nabeel, N. Shang, and E. Bertino, “Privacy preserving policy based content

[10] sharing in public clouds,” IEEE Trans. on Know. and Data Eng., vol. 25, no. 11, pp. 2602-2614, 2013.

[11] Dolev, D., Yao A. C., "On the security of public key protocols", IEEE trans. On Information Theory, vol. IT-29, no. 2, pp. 198–208, 1983

[12] D. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[13] D. Boneh, X. Boyen, H. shacham, “Short group signature,” Proc. Int’Cryptology Conf. Advances in Cryptology, pp.41-55, 2004.

[14] B. den Boer, Diffie–Hellman is as strong as discrete log for certain primes in Advances in Cryptology – CRYPTO 88, Lecture Notes in Computer Science 403, Springer, p. 530, 1988.

[15] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp.136- 149, Jan. 2010.