http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-10, Issue-1,January, 2021
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-06

PRIVACY PRESERVATION FRAMEWORK IN PAAS FOR SECURE MEDIA TRANSMISSON USING RPSM

Gunjan Kumar Shandilya[1], Prof. Nitesh Gupta[2]
Research Scholar(CSE) 1#, Assistant Professor (CSE)*2
NRI Institute of Information Science and technology Bhopal, M.P. (India)
shandilyagunjan.kumar@gmail.com

Abstract*—In the last few years cyber-crime showed tremendous growth. There are different platforms available, in which cyber-attacks are performed, data servers one of the most laid-back target. Due to these attacks users important information leaked such as personal documents and other private documents. Due to this problem researchers are focused on secure and privacy preserved image transmission system, in which images are send to cloud server in encrypted form and avoid the privacy linking problems in cloud services. There are different types of services provide by cloud IaaS, PaaS and, SaaS all required a trustful and secure method for the encryption of users data. In this research work discuss the different privacy preserving methods in Image Cloud, also compare these methods. Also present a novel approach to target this problem in this proposed method use random pixel shifting method. In this method image pixels are shifted on different place on the basis on fixed formula that is key of encryption. Use this key at the time decryption, this key is only unknown by user so no one can decrypt the encrypted image. In this thesis work also discuss the different attacks on encrypted image. The proposed novel approach shows better result as compare other method in terms of encryption and decryption of secure image. There are different result parameters to see the standard of encrypted and decrypted image like peak signal to noise ratio (PSNR), mean sq. error (MSE), similarity index measurement (SSIM) and mean absolute error (MAE)

***Keywords*— –IaaS, PaaS, SaaS, Privacy Preservation, Homomorphism Encryption (HE), Virtual Machine Servers (VMS) and Swift algorithm etc. Etc …**

I. INTRODUCTION

High Cloud is the new computing platform in which provide different IT services for Clint. Cloud provide a shared control pools of configurable system that may be quickly provisioned with lowest management effort, usually over the internet Cloud computing

Now a day's most of cloud services providers are known as CSP or third party services provider. They are provide different type of cloud services that is used in the real world such SaaS, IaaS and PaaS. Proponents place along claim that cloud computing permits enterprises to encourage their applications up and run quicker, with improvised flexibility and lesser maintenance, and which it permits IT groups to earlier change resources to fulfill unsteady and unpredictable demand. IaaS is one of the famous platform of cloud services. In the IaaS CSP provide real time hardware support to clients such as high speed hardware, Big data storage and high speed RAM. Cloud suppliers usually bill IaaS services on a utility computing basis: value reflects the quantity of resources allotted and consumed.

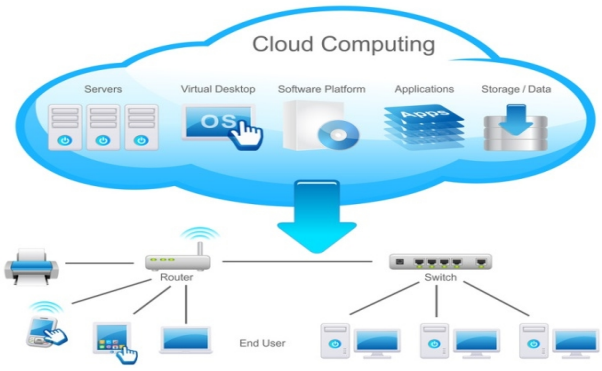

Fig. 1.Cloud Computing

Virtualization: Virtualization package separates the electronic computer into one or additional "virtual" devices, of which will be just used to do computer work. With operating system–level virtualization primarily making a ascendible system of multiple freelance computing devices, idle computing resources could also be assigned and used more expeditiously. Virtualization provides the lightness needed to hurry up IT operations, and reduces worth by increasing infrastructure utilization. Abstraction: Abstraction is one in every of the foremost vital ideas of cloud computing. It store specified description of operation and implementation which are being performed by the user. User's application, location wherever information is store and source information isn't outlined.

A. **Objective**

A To design privacy preserving image processing, to provide cloud user the confidence to store and retrieve sensitive data on cloud storage. To improve privacy and response time with less compromise on the client site communication and computation cost and time.To improve our system in redundancy privacy preserving over the data store along with security. It reveals that our system is protected in terms of the definitions per the projected security model. To propose a privacy preserving system that hides users' identity from both the CSP and other cloud users. There are different places available there cloud computing use for various economic solutions by giving alternative services like cloud storage, computing resources, digital watermarking and many more. There is great demand for sharing private information on the internet for various purposes. An appropriate methodology for protecting communicated or keeping information involves utilization of cryptographic techniques. A cipher text is an encrypted message which is the method of turning cipher text again into plain text is cryptography. In a cloud data location is dynamic and depends on various factors such as network, speed and availability of storage location. In such a scenario standard information security which is meant to protect the data at a known location fails due to location uncertainty of user's data .

II. LITERATURE REVIEW

Li, J. S., Liu [2020] - In this work, in order to achieve secure search for the encrypted image retrieval system, we develop a new privacy preserving image retrieval system in which we combine ASPE and HE schemes. Furthermore, to the best of our knowledge, our proposed scheme is the _rst work that assuming that all the entities are semi-trusted in this system. However, ASPE implements kNN for searching dataset, which also cause serious computation overhead. In order to improve the performance of the search time, k-means algorithm is applying in ASPE to simplify the descriptors of large-scale database containing over 10k images. Furthermore, our proposed scheme also utilize HE scheme to keep the secret key of ASPE confidential. In our scheme we also apply trapdoor verification in searching phase to conform the validation of trapdoor. Hence, through combination of ASPE and HE, our scheme provide a more secure image retrieval in cloud. In our scheme, each image is represented by the single vector. However, for the high dimensional descriptor, it leads to huge computation overheads, especially in executing the encrypted function. Hence, in the future, we continue this study to propose a privacy-preserving image retrieval system based on both local feature and global feature. In this work try to develop a decision scheme to optimize lower codebook size to improve the system efficiency and ensure the high accuracy meanwhile.[01].

Domingo-Ferrer, [2019], The increasing volume of personal and sensitive data being harvested by data controllers makes it increasingly necessary to use the cloud not just to store the data, but also to process them on cloud premises. However, security concerns on frequent data breaches, together with recently upgraded legal data protection requirements (like the European Union's General Data Protection Regulation), advise against outsourcing unprotected sensitive data to public clouds. To tackle this issue, this survey covers technologies that allow privacy-aware outsourcing of storage and processing of sensitive data to public clouds. Specifically and as a novelty, we review masking methods for outsourced data based on data splitting and anonymization, in addition to cryptographic methods covered in other surveys. We then compare these methods in terms of operations supported on the masked outsourced data, overhead, accuracy preservation, and impact on data management. Furthermore, we list several research projects and available products that have materialized some of the surveyed solutions. Finally, we identify outstanding research challenges. [02].

Zhan Qin et. al, [2018], Millions of personal pictures are generated in varied digital devices each day. The resultant large process employment makes individuals communicate cloud computing platforms for their economical computation resources. In fact, once uploaded to cloud, the protection and privacy of the image content will solely presume upon the reliability of the cloud service suppliers. Lack of reassuring security and privacy guarantees becomes the most barriers to additional preparation of cloud primarily based image processing systems. This paper studies the planning targets and technical challenges belong constructing cloud-based privacy-preserving image processing system. We found many tasks of image processing, moreover as image feature detecting, digital watermarking, content-based image search etc. A close taxonomy of the matter statement and therefore the corresponding solutions is provided. [03].

S. No.	Ref.	Title	Method	Drawback	Advantages

1	1	Secure Content-Based Image Retrieval in the Cloud With Key Confidentiality	large-scale image retrieval method	Focus on privacy preserving only, Low security	Key Confidentiality
3	3	Privacy-Preserving Image Processing in the Cloud	SIFT with Holomorphic Encryption	Complex and difficult to implement	Shows good result in case of privacy
4	4	Privacy-preserving image de-noising from external cloud databases	Secure Locality-Sensitive Hashing (SLSH)	Focus on privacy preserving only	Hash based image encryption provide good security
5	5	Cloud build: Microsoft's Distributed and Caching Build Service	Cloud Build	Large number of attacks are available for Micro-soft based system.	Microsoft always built user friendly schemes easy to use.
6	6	Secure Transformation Based Approach for Outsourced Image Reconstruction Service	OIRS	Not reliable	Third party responsible security threats
7	7	Privacy-preserving outsourcing of image global feature detection	Image Global Feature Detection	Focus on quality image transmission	Good PSNR and low level of security
8	8	Security protection between users and the mobile media cloud	DWT Based Watermarking	Low PSNR	Good in case of secure water mark
9	11	Privacy-assured outsourcing of image reconstruction service in cloud	OIRS	OIRS dependent to 3rd party, there is no monitoring unit available for security purpose.	If any issues are generated OIRS dependent for all faults.
10	14	Image feature extraction in encrypted domain with privacy preserving SIFT	SIFT	SIFT algorithm store a copy of data at both end transmitter and receiver, it consume extra space.	Easy to recover image when image are corrupted by attacks.

III. PROPOSED ALGORITHM

Decimal For privacy preservation a framework is been suggested for retrieval of pictures in large-scale, storage outsourcing, search, and dynamically updated repositories. Here the framework is made of two things: privacy preserving that is been executed in the outsourcing server and an image encryption component which is been executed on client devices. We base this framework on anew encryption scheme specifically designed for images, Random Pixel shifting method that is based on Gyrator transform while protecting the privacy of both image owners and other users issuing queries.

For the enhancement of previous problem use the following methodology. In this method use some terminology: a repository (Image Data Server) is a collection of images which is stored in the infrastructure of a cloud provider; the cloud server, or just cloud. The cloud server is based third type of cloud services that IaaS infrastructure that acts as a server both for storage and computation over images. In the proposed system both client and servers provide use this server, and its easily

used and access by any place by using mobile phone, tablet. In the proposed method more than one users are use this services, they also upload there different images to secure cloud. Each and every user having own secret key, user id and password, with the help of this log in in the system, when upload any image on cloud server, it create a key for encryption of image, when user want to decrypt this image, require a decryption key without decryption key, it is not possible to decrypt image. If one user want to share a secret image with different user, it can easily done just simply send the image with decryption key. Other user apply decryption with user's decryption key and decrypt this image.

For Decryption of Encrypted image user share decrypted key with other users Decrypted-Key (DE)

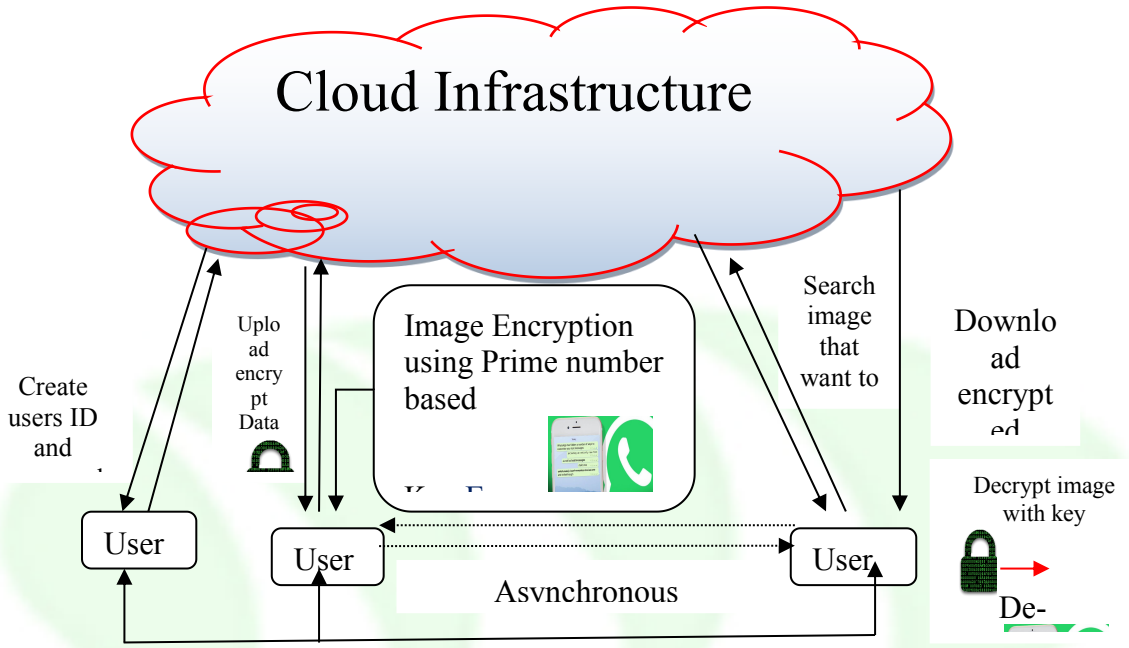

Fig. 2 Block diagram of Proposed Method

Block diagram

In the above figure 2 now describe the system block diagram of proposed system and architecture envisioned for using our framework and image encryption. In the proposed system there are two important parts user or client and service provider server. Personal Images are easily transferred from one place to cloud and one user to other user.

In the above figure 4.1 shows the block diagram of proposed work. First user create log in ID and password with the help of create a new user sign process and send request to admin. After admin approval user convert its personal image into encrypted form and send to the server. In the above figure 4.1 shows the user 2 process of send and receive the secret data using random pixel shifting method encryption and decryption method. User can also send and receive this encrypted image to different user using any public and private channel. User's data already in encrypted form so user can communicate data with other with any tension. Because in random pixel shifting method based on prime number and there is no limit of prime number. In the similar process user can easily download the encrypted image and decrypt it, with the help of decryption. Remember without prime number based decrypt key user cannot decrypt the personal data. That is the major advantage and drawback of this method. If user forget the encryption key decryption is not possible because it's based on second order homomorphic equation. That is the over explanation of proposed method. Now discuss the proposed method by user and services provider end.

IV. SIMULATION RESULT

For the implementation of proposed algorithm use Matrix laboratory. Matrix laboratory is a well-known tool for such kind of algorithm implementation related to data encryption and decryption. MATLAB contain a rich function family of computer vision tool box functions, image accusation tool boxes and large image processing library.

Simulation setup and parameters to be analyzed The result of proposed method for privacy preserved secure data encryption and decryption shown in this section, simulation of our proposed method and result calculation. For the implementation proposed work simulate with the help the MATLAB R2013a (8.1.0.602) software and simulate our whole proposed methodology in graphical user interface (GUI). The

performance of the proposed algorithm is tested for different data file size that is shown in GUI windows. Basic configuration of our system is: Processor: Intel (R) Quad Core (VM) i3 – 3110 Central Processing unit @, 2.40 GHz 64 b OS. MATLAB based simulation result shows good timing value for different file size images are compare to other method that is shown in table 5.1. These criteria can be evaluated by PSNR in dB, Mean square error (MSE), encryption time E(t), decryption time D(t) For calculate the similarity of the encrypted image and decrypt-ed image calculate the structural similarity index measurement (SSIM) of the both images. Performance of our proposed method are quantitatively measured by PSNR, MSE, and SSIM values defined by:

Encryption Time

The time taken when image are encrypt. It is calculate by the total time taking of the encryption algorithm. In the proposed Work use random pixel shifting method.

E(t) = Time consumption in encryption 1

Decryption Time

The time taken when image are Decrypt. It is calculate by the total time taking of the Decryption algorithm. In the proposed Work use random pixel shifting method.

D(t) = Time consumption in decryption 2

Peak Signal to Noise Ratio (PSNR)

The PSNR is computed as:

$$PSNR = 10\ log_{10}\left(\frac{S^2}{MSE}\right) \qquad 3$$

Where S is that the size of actual image.

The PSNR is higher for an excellent worth image and lower for a poor quality image. This parameters is use to analysis the quality degradation of image. In this proposed research work on the basis of our image size 255x255, we mentioned PSNR and MSE are as follows.

Table 5.2 Result Comparison of Proposed Method

Name of Images	Previous Method SSIM [02]	Proposed SSIM	Previous Method PSNR [02]	Proposed PSNR(db
d test	0.804	0.855652	30.592	31.2684
e test	0.772	0.832815	30.945	31.752
g test	0.793	0.822901	31.053	31.5752
b test	0.843	0.873666	29.779	30.8961
a test	0.773	0.850544	30.038	319081

NAME OF IMAGES	ENCRYPTION TIME	DECRYPTION TIME
BARBERA	1.460404SEC.	1.482298SEC.
GOLDENHILL	1.421142SEC.	1.488713SEC
GOLDENHILL2	1.460646SEC.	1.431713SEC.
MANDIAL	1.441131SEC	1.454886SEC.
PARROT	1.427261SEC	1.433380SEC.
PEPPER	1.412815SEC.	1.392034SEC

V. CONCLUSION

In this research paper conclusion of proposed method. The proposed based on random pixel shifting method shows better result for privacy preserve secure image encryption and decryption in public channel. The proposed method mainly focus the privacy preservation of the images as compare to other previous method most of the methods are based on third party based encryption and decryption. Now a day's cybercrime are increase rapidly. So the third party CSP are not very secure, the solution of this problem is our proposed method, in this method encryption and decryption done at user end cloud and private channel are only use for encrypted data send and receive. The proposed method is less complex as compare to previous methods. The main advantage of proposed method is random number based secure key. As we know that Random number are infinite, so it's difficult of crack by hackers.

REFERENCES

[1]. Area-Li, Jung-Shian, et al. "Secure Content-Based Image Retrieval in the Cloud With Key Confidentiality." IEEE Access 8 (2020): 114940-114952..

[2]. Domingo-Ferrer, Josep, et al. "Privacy-preserving cloud computing on sensitive data: A survey of

methods, products and challenges." Computer Communications 140 (2019): 38-60.
[3]. Qin, Zhan, et al. "Privacy-Preserving Image Processing in the Cloud." IEEE Cloud Computing (2018).
[4]. Zheng, Yifeng, et al. "Privacy-preserving image denoising from external cloud databases." IEEE Transactions on Information Forensics and Security 12.6 (2017): 1285-1298.
[5]. H. Esfahani et al., "Cloudbuild: Microsoft's Distributed and Caching Build Service,"Software Engineering in Practice (SEIP 16), 2016.
[6]. M. Jeevitha Lakshmi S. , Umapriya , R. Ramya M., SivaSindhu. "Secure Transformation Based Approach for Outsourced Image Reconstruction Service" International Journal of Scientific and Research Publications, Volume 5, Issue 3, March 2015 ISSN 2250-3153.
[7]. Z. Qin et al., "Privacy-preserving outsourcing of image global feature detection,"Proceedings of the Global Communications Conference (GLOBECOM 14), 2014.
[8]. H. Wang et al., "Security protection between users and the mobile media cloud," IEEECommunications Magazine, 2014.
[9]. Z. Qin et al., "Towards efficient privacy-preserving image feature ex-traction in cloudcomputing," Proceedings of the 2014 ACM on Multimedia Conference (MM 14),2014.
[10]. C. Wang et al., "Privacy-assured outsourcing of image reconstruction service incloud," IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, 2013, pp.166–177.
[11]. C. Lin, C. Lee, and S. Chien, "Digital Video Watermarking on Cloud Computing Environments," Proceedings of the Second International Conference on Cyber Security (CyberSec 13), 2013.
[12]. C. Modi et al., "A survey of intrusion detection techniques in cloud," Journal ofNetwork and Computer Applications, vol. 36, no. 1, 2013, pp. 42–57.
[13]. C.-Y. Hsu et al., "Image feature extraction in encrypted domain with privacypreservingSIFT," IEEE Transactions on Image Processing, vol. 21, no. 11, 2012, pp.4593–4607.
[14]. S. Pandey et al., "An autonomic cloud environment for hosting ECG data analysis services," Future Generation Computer Systems, vol. 28, no. 1, 2012, pp. 147–154.
[15]. K. Ivanova et al., "Features for art painting classification based on vector quantization of mpeg-7 descriptors," Data Engineering and Management, Springer, 2012.
[16]. C.-Y. Hsu et al., "Homomorphic encryption-based secure SIFT for privacy-preservingfeature extraction," Proceedings of SPIE (SPIE 11), 2011.
[17]. M. Naehrig et al., "Can homomorphic encryption be practical?," Proceedings of ACM Cloud Computing Security Workshop (CCSW 11), 2011.
[18]. M.K. Khan, J. Zhang, and K. Alghathbar, "Challenge-response-based biometric image scrambling for secure personal identification," Future Generation Computer Systems, vol. 27, no. 4, 2011, pp. 411–418.
[19]. M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol.53, no. 4, 2010, pp. 50–58.
[20]. W. Lu et al., "Secure image retrieval through feature protection," Proceedings of theInternational Conference on Acoustics, Speech, and Signal Processing (ICASSP 09),2009.
[21]. W. Lu et al., "Enabling search over encrypted multimedia databases," Proceedings of SPIE (SPIE), 2009.
[22]. Ribaric, Slobodan, Aladdin Ariyaeeinia, and Nikola Pavesic. "De-identification for privacy protection in multimedia content: A survey." Signal Processing: Image Communication 47 (2016): 131-151.

