A Literature Survey on Privacy Preserving in Image processing on Cloud

Rahul Kumar Dangarh[#1], Sunil Malviya[*2]
[1#]Research Scholar(CSE), [*2]Assistant Professor (CSE)
Sagar Institute of Science and Technology, Bhopal, M.P. (India)

Abstract – In the last decade cybercrime shows 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 survey paper discuss the different privacy preserving methods in Image Cloud, also compare these methods. In the last decade different methods was presented, in this survey discuss few of them. Most of the methods are focused on data security; few of them focus on privacy preservation. Also discuss the major issues of privacy preserving in clouds.

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

I. CLOUD COMPUTING

Cloud computing is a next generation technology that is used to enhance the IT world forexample that provide access to sharethe system resources and zenith level services that may be provisioned with lowest management effort, usually over the web. Cloud computing is an important part of human beings. It's provide facility to store data between users and admin. For uploading data use internet. There are two type of file. First one is private file and second one is sheared file. In the private file data is fully secured, rather than users on one other person can assess this type of file. Due to cloud security authentication are not allow and vise Vera of shared file. Every user can access these type of file and users get permit to access these files.

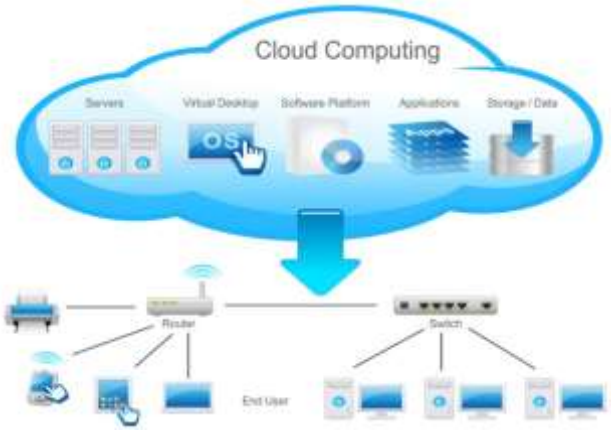


Fig. 1 Cloud Computing

Third-party clouds modify organizations to target their core businesses rather than spending resources on computer infrastructure and maintenance.

Virtualization: Virtualization software parts a physical hardware PC into one or further "virtual" machines, each of that will be merely used and managed to perform computing tasks. With operating system–level virtualization primarily making a ascendible system of multiple freelance computing devices, idle computing resources could also be assigned.

II. SERVICES OF CLOUD COMPUTING

There are different cloud services are available in the cloud computing providers provide their "services" according to different models. Cloud offer three main services SaaS, IaaSand PaaS. Cloud services are basically demand to client's basis. In the IaaS as a services cloud provide virtual hardware to clients. In the field of IaaS Amazon is one of mammoth player. The next type of cloud services is PaaS, it provides platform to serve application as well as provide infrastructure for clients. SaaS provide all these services for client's basis such as infrastructure, platform and services.

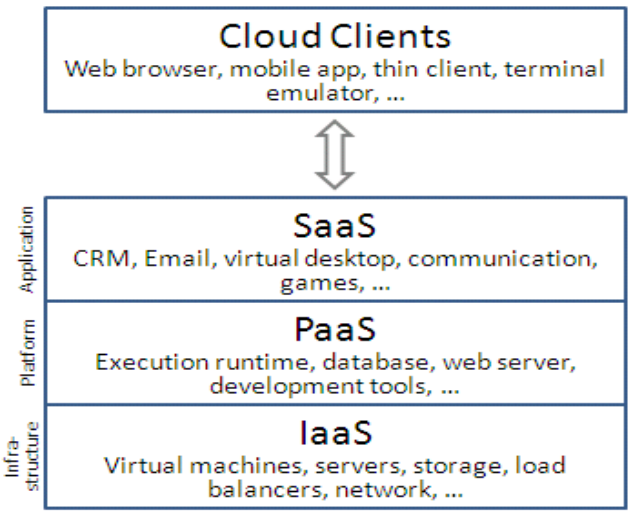


Fig. 2 Cloud computing service model

III.PRIVACY PRESERVING IN IMAGE PROCESSING ON CLOUD

Public data should not be released without preserving the privacy of each record. It should ensure that no individual is identified from the anonymized data in cloud. The conventional security systems do not ensure privacy preserving. Data encryption has its own limitation because of key sharing drawback, machine value and potency, trust violation and in transitivity of trust. A definition in states that general definition of privacy must be one that is measurable, of value and actionable. Secrecy is concern about the information that other may gather anonymity about how the information is generalized.

Image Encryption

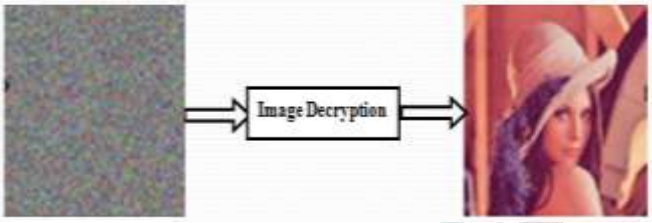
Image encryption techniques attempt to convert original image to a different image that's hard to know. To stay the image confidential between users, in different word, it's essential that no-one may get to understand the content while not a key for decryption.

Original image Encrypted image

Fig. 3 Image Encryption

Image Decryption

Image decryption is usually the reverse method of encryption. A certified user will solely decrypt information because decryption needs a secret key or password. Image decryption is that the method of decoding encrypted info so is may be accessed once more by approved users.



Encrypted image Original image

Fig. 4 Image Decryption

To make the information confidential, information (plain text) is encrypted employing a specific algorithm and a secret key. To decrypt the cipher text, similar algorithm is employed and at the top the original information is obtained again.

IV. LITERATURE SURVEY

Zhan Qinet. 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 reliableness 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. A close taxonomy of the matter statement and therefore the corresponding solutions is provided.**[01]**

ZhengYifeng, et. al, [2017],Together with the speedy advancement of digital image processing technology, image denoising remains a elementary task, that aims to recover the first image from its screaming observation. With the explosive growth of pictures on the web, one recent trend is to seek prime quality similar patches at cloud image databases and harness made redundancy and shows good performance in de-nosing. In this research work, initial discuss the privacy-preserving with image noise removal from external cloud databases. Yao's garbled circuits, and image denoising operations, wherever each is employed at a special part of the planning for the simplest performance. We formally analyze the protection strengths. **[02]**

H. Esfahaniet. al, [2016], Thousands of Microsoft engineers build and check many software product many times daily. This paper describes CloudBuild, the build service infrastructure developed among Microsoft over the previous few years. CloudBuild is responsible for all aspects of an endless integration work flow, along-side builds,check and code analysis, additionally as drops, packageand image creation and storage. CloudBuild supports multiple build languages as long as they fulfil a rough grained, file IO primarily based contract. CloudBuild uses content primarily based caching to run build-related tasks provided that needed. Lastly, it builds on many machines in parallel. It aims to quickly aboard groups and therefore needs to support non-deterministic build tools and specification languages that under-declare dependencies. **[03]**

M. Jeevitha Lakshmi S. et. al, [2015],Now-a-days image or information isn't retrieve properly in cloud because large number of drawback is formed, from this the info could losses. Data owner only need to supply compressed image samples to cloud for reduced storage overhead. OIRS provides security; potency and it additionally reduce design quality. In OIRS design the distributed image is taken because, it takes less memory within the database memory. By victimization this method the retrieved image becomes accuracy and potency. The info users will simply reconstruct the first image without any loss.**[04]**

Z. Qin et. al, [2014], The amount and convenience of user-contributed image information are dramatically increased throughout the past 10 years. For the aim of effective advertising, higher user retention and attraction, and many of others The projected system allows an interested party to perform a range of image feature detection tasks, as well as visual descriptors in MPEG-7 normal, whereas protective user privacy concerning image contents. We implement a paradigm system supported somewhat homomorphic encryption theme and also the benchmark Caltech256 information.The experimental results show that our system can guarantee effective image feature detection without sacrificing user privacy.**[05]**

H. Wang et. al, [2014], Mobile devices similar to smartphones are wide deployed within the world, and plenty of individuals use them to download/upload media similar to video and images to remote servers. On the opposite hand, a mobile device has restricted resources, and a few media process tasks should be migrated to the media cloud for additional process. However, a major question is, will mobile users trust the media services provided by the media cloud service providers? Several ancient security approaches are projected to secure the information exchange between mobile users and also the media cloud. However, first, because multimedia similar to video is large-sized information, and mobile devices have restricted capability to method media information, it's necessary to design a light-weight security method; second, uploading and downloading multi-resolution images/videos create it tough for the standard security ways to confirm security for users of the media cloud. Third, the fallible wireless surroundings can cause failure of security protection the same as authentication.The secure sharing theme permits users to transfer multiple information items to totally different clouds, creating it not possible to derive the total info from anybody cloud. Additionally, the projected scalable watermarkingalgorithm is often used for authentications between personal mobile users and also the media cloud. Our studies show that the projected approach not solely achieves sensible security performance, however can also enhance media quality and reduce transmission overhead.**[06]**

Cong Wang et. al, [2013], Large-scale image information sets are being exponentially generated these days. Alongside such information explosion is that the invasive trend to source the image management systems to the cloud for its verdant computing resources and edges. The thanks to defend the sensitive data whereas facultative outsourced image services, however, becomes a significant concern. Additionally, in OIRS, information users will harness the cloud to firmly reconstruct pictures while not revealing info from either the compressed image samples or the underlying image content. We begin with the OIRS design for distributed information that is that the typical application situation for compressed sensing, and so show its natural extension to the overall information for substantive tradeoffs between potency and accuracy. For completeness, we additionally discuss the expected performance speeding of OIRS through hardware inbuilt system design.**[08]**

Chao-Yung Hsu et. al, [2012], Privacy has received considerable attention however remains mostly neglected within the transmission community. Visible of the particular actual fact that scale-invariant feature transform (SIFT) has been wide adopted in various fields. In this research work is that the initial to focus on the importance of privacy-preserving based SIFT algorithm.We show through the safety analysis supported the discrete logarithm drawback and RSA that PPSIFT is secure against cipher text solely attack and familiar plaintext attack. Experimental results obtained from completely different case studies demonstrate that the planned homomorphic encryption-based privacy-preserving SIFT performs comparably to the initial SIFT which our technique is helpful in SIFT-based privacy-preserving applications.**[11]**

Chun-Shien Lu et. al, [2011], Privacy has received a lot of attention however is still for the most part neglected within the multimedia system community. Contemplate a cloud computing state of affairs, wherever the server is resource-abundant and is capable of finishing the designated tasks, it's visualized that secure media retrieval. In sight of the actual fact that scale invariant feature transform (SIFT) has been wide adopted in numerous fields. Since all the operations in SIFT ought to be affected to the encrypted domain, we propose a homomorphic encryption-based secure SIFT methodology for privacy preservingfeature extraction and illustration supported Paillier cryptosystem. Particularly, homomorphic comparison may be a should for SIFT feature detection however remains a difficult issue for homomorphic encryption methods. **[14]**

Table 1 Comparison between previous methods

S.No.	Ref.	Title	Method	Drawback	Advantages
1	1	Privacy-Preserving Image Processing in the Cloud	SIFT with Holomorphic Encryption	Complex and difficult to implement	Shows good result in case of privacy
2	2	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
3	3	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.
4	4	Secure Transformation Based Approach for Outsourced Image Reconstruction Service	OIRS	Not reliable	Third party responsible security threats
5	5	Privacy-preserving outsourcing of image global feature detection	Image Global Feature Detection	Focus on quality image transmission	Good PSNR and low level of security
6	6	Security protection between users and the mobile media cloud	DWT Based Watermarking	Low PSNR	Good in case of secure water mark
7	8	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.
8	11	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.
9	14	Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction	SIFT based encryption with privacy preservation	Without reference image decryption not possible	HE based method shows better result for encryption

VI. CONCLUSION

In this survey cum comparative analysis of privacy preserving in cloud computing discuss the different methods survey as well as shows comparison of different methods. In this comparison shows the advantages of different previous methods.In this survey paper gives the fundamental principle of different privacy preserving in image processing methods has been introduced systematically. Also shows the short summery of different methods and discuss the major problem in cloud related to privacy preserving. For the improvement of previous problem double layer encryptionof image is a good idea. In this way perform secure image transmission between user and cloud. This paper gives the comparison of previous methods in the above table 1.

REFERENCE

[1] Qin, Zhan, et al. "Privacy-Preserving Image Processing in the Cloud." *IEEE Cloud Computing* (2018).

[2] Zheng, Yifeng, et al. "Privacy-preserving image denoising from external cloud databases." *IEEE Transactions on Information Forensics and Security* 12.6 (2017): 1285-1298.

[3] H. Esfahani et al., "Cloudbuild: Microsoft's Distributed and Caching Build Service," Software Engineering in Practice (SEIP 16), 2016.

[4] 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.

[5] Z. Qin et al., "Privacy-preserving outsourcing of image global feature detection," Proceedings of the Global Communications Conference (GLOBECOM 14), 2014.

[6] H. Wang et al., "Security protection between users and the mobile media cloud," IEEE Communications Magazine, 2014.

[7] Z. Qin et al., "Towards efficient privacy-preserving image feature ex-traction in cloud computing," Proceedings of the 2014 ACM on Multimedia Conference (MM 14), 2014.

[8] C. Wang et al., "Privacy-assured outsourcing of image reconstruction service in cloud," IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, 2013, pp. 166–177.

[9] 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.

[10] C. Modi et al., "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, no. 1, 2013, pp. 42–57.

[11] C.-Y. Hsu et al., "Image feature extraction in encrypted domain with privacy preserving SIFT," IEEE Transactions on Image Processing, vol. 21, no. 11, 2012, pp. 4593–4607.

[12] 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.

[13] K. Ivanova et al., "Features for art painting classification based on vector quantization of mpeg-7 descriptors," Data Engineering and Management, Springer, 2012.

[14] C.-Y. Hsu et al., "Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction," Proceedings of SPIE (SPIE 11), 2011.

[15] M. Naehrig et al., "Can homomorphic encryption be practical?," Proceedings of ACM Cloud Computing Security Workshop (CCSW 11), 2011.

[16] 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.

[17] M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, 2010, pp. 50–58.

[18] W. Lu et al., "Secure image retrieval through feature protection," Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP 09), 2009.

[19] W. Lu et al., "Enabling search over encrypted multimedia databases," Proceedings of SPIE (SPIE), 2009.

[20] Z. Erkin et al., "Privacy-preserving face recognition," Proceedings of Privacy Enhancing Technologies Symposium (PETS 09), 2009.

[21] C. Gentry, "Fully homomorphic encryption using ideal lattices," Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC 09), 2009.

[22] M. Malkin and T. Kalker, "A cryptographic method for secure watermark detection," Proceedings of the 8th International Workshop on Information Hiding, 2006.

[23] T. Sikor, "The MPEG-7 visual standard for content description-an overview," IEEE Transactions on Circuits and Systems for Video Technology, vol. 11, no. 6, 2001, pp. 696–702.

[24] J. Eggers, J. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," Proceedings of the European Symposium on Security and Privacy (Euro SP), 2000.

[25] O. Goldreich, Secure multi-party computation Manuscript, 1998.