International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST52310562

# A Literature Survey on Privacy Preserving in Image processing on Cloud

[1]Priyanka Valmiki, [2]Dr. Arvind Kaurav, [3]Prof. Nehul Mathur
[1]M.Tech Scholar, [2]Professor, [3]Assistant Professor
Department of Electronics and Communication, Bhopal Institute of Technology, Bhopal, Madhya Pradesh, India

ARTICLEINFO

**Article History:**

Accepted: 01 Oct 2023
Published: 09 Oct 2023

**Publication Issue**
Volume 10, Issue 5
September-October-2023

**Page Number**
460-468

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 targets. 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. INTRODUCTION

Cloud computing is a next generation technology that is used to enhance the IT world for example that provide access to share the 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 providing 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.

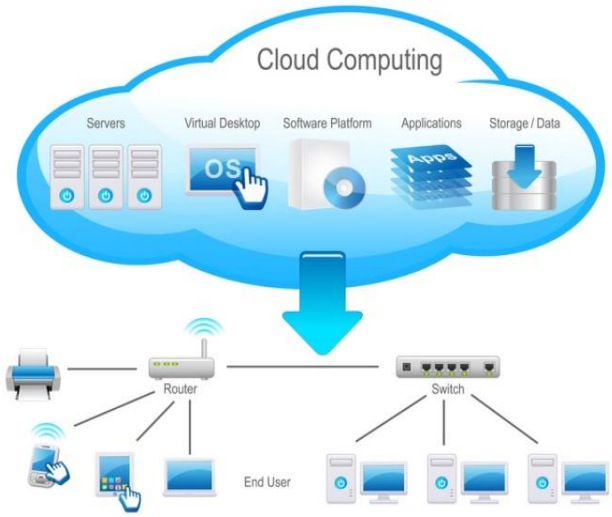



Fig. 1 Cloud Computing

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.

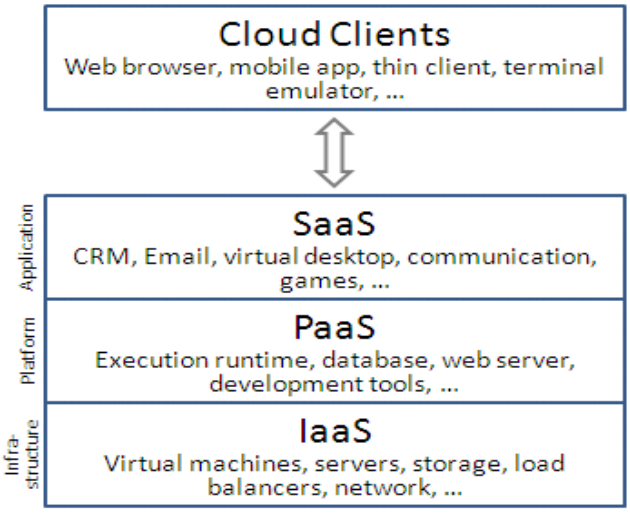


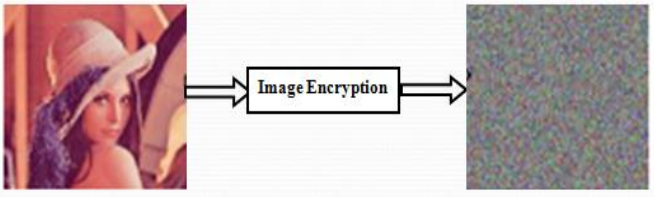

Fig. 2 Cloud computing service model

## 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.

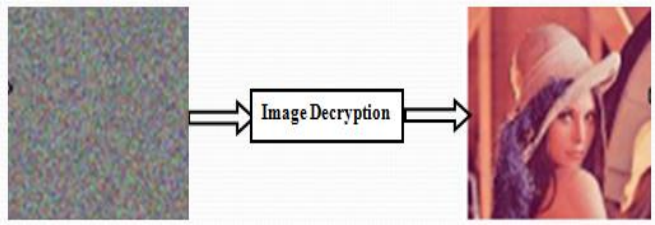



Original image Encrypted image

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.

## III. LITERATURE SURVEY

Bo Zhang et.al. [2023], A three-party computation (3-PC) privacy-preserving image retrieval scheme based on additive secret sharing techniques for cloud computing scenarios, using CNN as image feature extractor to improve retrieval accuracy, constructing hierarchical clustered index trees to improve search efficiency, and designing a series of security protocols to ensure the security of images, network models, feature extraction and search processes. Our scheme achieves a balance between security, accuracy and efficiency without loss of retrieval accuracy. The experimental evaluation results demonstrated the effectiveness and efficiency of our framework. We intend to extend this work in two directions in the future, one is to outsource feature extraction and index building to cloud servers to further reduce the computational overhead of data owners, and the other is to further improve retrieval efficiency [01].

Yuandou Wang et.al. [2023], Digitized histopathology glass slides, known as Whole Slide Images (WSIs), are often several gig pixels large and contain sensitive metadata information, which makes distributed processing unfeasible. Moreover, artefacts in WSIs may result in unreliable predictions when directly applied by Deep Learning (DL) algorithms. Therefore, pre-processing WSIs is beneficial, e.g., eliminating privacy-sensitive information, splitting a gig pixel medical image into tiles, and removing the diagnostically irrelevant areas. This work proposes a cloud service to parallelize the pre-processing pipeline for large medical images. The data and model parallelization will not only boost the end-to-end processing efficiency for histological tasks but also secure the reconstruction of WSI by randomly distributing tiles across processing nodes [02].

Qihua Feng et.al. [2022], Image retrieval systems help users to browse and search among extensive images in real-time. With the rise of cloud computing, retrieval tasks are usually outsourced to cloud servers. However, the cloud scenario brings a daunting challenge of privacy protectionas cloud servers cannot be fully trusted. To this end, image-encryption-based privacy-preserving image retrieval schemes have been developed, which first extract features from cipher-images, and then build retrieval models based on these features. Yet, most existing approaches extract shallow features and design trivial retrieval models, resulting in insufficient expressiveness for the cipherimages A novel paradigm named Encrypted Vision Transformer (EViT), which advances the discriminative representations capability of cipher-images. First, in order to capture comprehensive ruled information, we extract multi-level local [03].

**Faliu Yi et.al. (2021) -** The emergence of cloud computing, large amounts of private data are stored and processed in the cloud. On the other hand, data owners (users) may not want to reveal data

information to cloud providers to protect their privacy Moreover, decryption of big data such as images requires enormous computation resources, which is unsuitable for energy-constrained devices, particularly Internet of Things (IoT) devices. Data privacy in most popular applications, such as image query or classication, can be preserved if encrypted images can be directly classied on the cloud or IoT devices without decryption. This paper proposes a high-speed double random phase encoding (DRPE) technique of encrypting images into white-noise images. DRPE-encrypted images are then uploaded and stored in the cloud [04].

Zhijian Liu et.al. (2020) - The privacy-preserving edge-cloud inference framework, Data Mix, to bring the best of the resource-hungry edge devices and the privacy invasive cloud servers together for the model inference. We propose to delegate most of the model computations to the cloud and carefully design a mixing and de-mixing operation to protect the privacy of the data transmitted to the cloud. Our framework is ecient, accurate and privacy-preserving: extensive experiments on two computer vision datasets and a speech recognition dataset demonstrate that DataMix can greatly reduce the local computations on the edge with negligible loss of accuracy and no leakages of private information [05].

**Qi Gu et.al. (2020) -** Content-Based Image Retrieval (CBIR) techniques have been widely researched and in service with the help of cloud computing like Google Images. However, the images always contain rich sensitive information. In this case, the privacy protection becomes a big problem as the cloud always can't be fully trusted. Many privacy-preserving image retrieval schemes have been proposed, in which the image owner can upload the encrypted images to the cloud, and the owner himself or the authorized user can execute the secure retrieval with the help of cloud. Nevertheless, few existing researches notice the multi-source scene which is more practical. In this paper, we analyze the difficulties in Multi-Source Privacy-Preserving Image Retrieval (MSPPIR). Then we use the image in JPEG-format as the example, to propose a scheme called JES-MSIR, namely a novel JPEG image Encryption Scheme which is made for Multi-Source content-based Image Retrieval [06].

Zhihua Xia et.al. (2019) - Content based image retrieval (CBIR) techniques have been widely deployed in many applications for seeking the abundant information existed in images. Due to large amounts of storage and computational requirements of CBIR, outsourcing image search work to the cloud provider becomes a very attractive option for many owners with small devices. However, owing to the private content contained in images, directly outsourcing retrieval work to the cloud provider apparently bring about privacy problem, so the images should be protected carefully before outsourcing. a secure retrieval scheme for the encrypted images in the YUV color space. With this scheme, the discrete cosine transform (DCT) is performed on the Y component [07].

Haohua Du et.al. (2019) - Privacy has become one of the major concerns in cloud video surveillance. Privacy protection of the surveillance videos strive to protect users' privacy information without hampering regular security tasks of the surveillance, meanwhile retains the system's high accuracy and efficiency. The current state of the art in protecting the video privacy is mainly realized through Privacy Region Protection, which only protects the privacy regions while keeps the non-privacy regions visually intact so that processing in the cloud is still feasible. However, the problem of determining the privacy regions has been ignored and not properly addressed. a novel notion - concept graph, and with the aid of that, we develop our system – PatronuS to determine the privacy regions subject to satisfying both privacy and security requirements [08].

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 [09].

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 [10]

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 [11]

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 [12]

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. 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 [13]

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 [14]

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 [15].

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. [16]

**Table 1 Comparison Between Previous Methods**

| Ref. | Title | Method | Drawback | Advantages |
|---|---|---|---|---|
| 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 | 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 | Cloud build: | Cloud Build | Large number | Microsoft |

| | | | | |
|---|---|---|---|---|
| | Microsoft's Distributed and Caching Build Service | | of attacks are available for Micro-soft based system. | always built user friendly schemes easy to use. |
| 4 | Secure Transformation Based Approach for Outsourced Image Reconstruction Service | OIRS | Not reliable | Third party responsible security threats |
| 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 | Security protection between users and the mobile media cloud | DWT Based Watermarking | Low PSNR | Good in case of secure water mark |
| 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. |
| 9 | Image feature extraction | SIFT | SIFT algorithm store a | Easy to recover image |
| | in encrypted domain with privacy preserving SIFT | | copy of data at both end transmitter and receiver, it consume extra space. | when image are corrupted by attacks. |
| 10 | 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 |

## V. 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.

## IV. REFERENCES

[1] Bo Zhang , Yanyan Xu, Yuejing Yan1 and Zhiheng Wang, “Privacy-preserving Image Retrieval Based on Additive Secret Sharing in Cloud Environment” July 31st, (2023)

[2] Yuandou Wang, Neel Kanwal , Kjersti Engan , Chunming Rong, Zhiming Zhao "Towards a privacy-preserving distributed cloud service for preprocessing very large medical images" 12 Jul (2023)

[3] Qihua Feng, Peiya Li, Zhixun Lu, Chaozhuo Li, Zefang Wang, Zhiquan Liu "EViT: Privacy-Preserving Image Retrieval via Encrypted Vision Transformer in Cloud Computing" 31 Aug (2022)

[4] Hang Cheng , Qinjian Huang, Fei Chen , Meiqing Wang And Wanxi Yan "Privacy-Preserving Image Watermark Embedding Method Based on Edge Computing" February 22, (2022)

[5] Chiranjeevi Karri , Omar Cheikhrouhou , Ahmed Harbaoui , Atef Zaguia and Habib Hamam "Privacy Preserving Face Recognition in Cloud Robotics: A Comparative Study" Volume 10, 15 July (2021).

[6] Faliu Yi, Ongee Jeong And Inkyu Moon "Privacy-Preserving Image Classification With Deep Learning and Double Random Phase Encoding" Volume 9, October 11, 2021

[7] Zhijian Liu, Zhanghao Wu, Chuang Gan, Ligeng Zhu and Song Han "DataMix: Ecient Privacy-Preserving Edge-Cloud Inference" (2020)

[8] Qi Gu, Zhihua Xiaa and Xingming Suna "MSPPIR: Multi-Source Privacy-Preserving Image Retrieval in cloud computing" 30 Sep (2020)

[9] Zhihua Xia, Lihua Lu, Tong Qiu1, H. J. Shim, Xianyi Chen and Byeungwoo Jeon "

[10] A Privacy-Preserving Image Retrieval Based on AC-Coefficients and Color Histograms in Cloud Environment" vol.58, no.1, pp.27-43, (2019 )

[11] Haohua Du, Linlin Chen, Jianwei Qian, Jiahui Hou, Taeho Jung, Xiang-Yang Li "PatronuS: A System for Privacy-Preserving Cloud Video Surveillance" 2019

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

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

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

[15] 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.

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

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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

[24] K. Ivanova et al., "Features for art painting classification based on vector quantization of

mpeg-7 descriptors," Data Engineering and Management, Springer, 2012.

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

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

[27] 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.

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

[29] Pranay Yadav, Shachi Sharma, Prayag Tiwari, Nilanjan Dey, Amira S. Ashour and Gia Nhu Nguyen "A Modified Hybrid Structure for Next Generation Super High Speed Communication Using TDLTE and Wi-Max" 2018.

[30] Alok Kumar; Sandeep Kumar Shukla; Archana Sharma; Pranay Yadav "A Robust Approach for Image Super-Resolution using Modified Very Deep Convolution Networks" 09-11 May 2022.

[31] Pranay Yadav, Alok Upadhyay, V. B. Surya Prasath, Zakir Ali, and Bharat Bhooshan Khare "Evolution of Wireless Communications with 3G, 4G, 5G, and Next Generation Technologies in India" 2021, volume 709.

[32] Sandeep Tiwari; Nitesh Gupta; Pranay Yadav "Diabetes Type2 Patient Detection Using LASSO Based CFFNN Machine Learning Approach" 19 October 2021.

[33] Pranay Yadav "Color Image Noise Removal by Modified Adaptive Threshold Median Filter for RVIN" 2015.

[34] Pranay Yadav "Removal of Fixed Value Impulse Noise using Improved Mean Filter for Image Enhancement" NOVEMBER, 2013.

[35] Vikas Gupta, Dilip Kumar Gandhi, Pranay Yadav "Removal of Fixed Value Impulse Noise using Improved Mean Filter for Image Enhancement" 2013.

[36] Pranay Yadav, Vivek Kumar, Manju Jain, Atul Samadhiya, and Sandeep Jain "Image De-Noising For Salt and Pepper Noise by Introducing New Enhanced Filter" 25-26, 2013.

[37] Pranay Yadav and Vivek Kumar "Image De-Noising for Salt and Pepper Noise by Robust Mean Filter" 2013.

[38] Pranay Yadav, Vivek Kumar, Manju Jain, Atul Samadhiya, and Sandeep Jain "Image De-Noising For Salt and Pepper Noise by Introducing New Enhanced Filter" Dec. 25-26, 2013.

[39] Vivek Kumar, Pranay Yadav, Atul Samadhiya, Sandeep Jain, and Prayag Tiwari "Comparative Performance Analysis of Image De-noising Techniques" Dec. 25-26, 2013.

[40] Pranay Yadav, Shrinklata Patel, Dr.Kavita Khare, Dr. J. S. Yadav "High Performance Robust FIR Filter Design Using Radix-8 Based Improved Booth Multiplier For Signal Processing Application" 2013.

**Cite this article as :**

Priyanka Valmiki, Dr. Arvind Kaurav, Prof. Nehul Mathur , "A Literature Survey on Privacy Preserving in Image processing on Cloud", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 5, pp. 460-468, September-October 2023. Available at doi : https://doi.org/10.32628/IJSRST52310562
Journal URL : https://ijsrst.com/IJSRST52310562