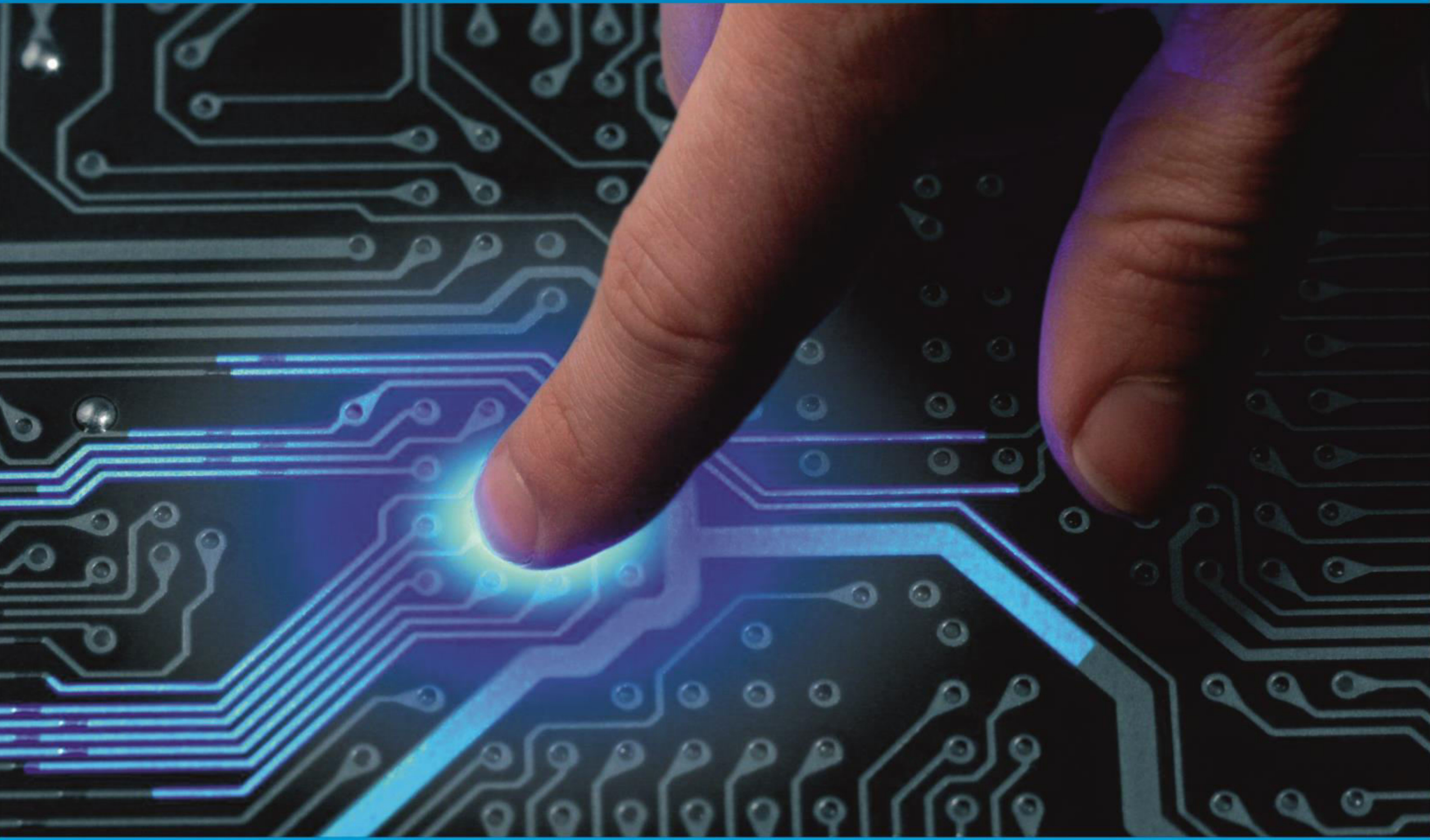
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903203|

Similarity Search for Encrypted Images Using Multi Key in Secure Cloud

Dr. S. Soundararajan[1], Kavitha S[2], Vaishnavi P[3], Vinothini R[4]

Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1]

UG student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [2,3,4]

ABSTRACT: Content-based Image Retrieval (CBIR) strategies have been broadly considered with the fast development of computerized pictures. For the most part, CBIR administration is very costly in computational and capacity assets. Along these lines, it is a decent decision to re- appropriate CBIR administration to the cloud server that is furnished with colossal assets. Notwithstanding, the security insurance turns into a major issue, as the cloud server can't be completely trusted. In This paper, we propose a redistributed CBIR conspire dependent on a novel pack of-scrambled words (BOEW) model. The picture is scrambled by shading esteem substitution, square stage, and intra-square pixel change. At that point, the nearby histograms are determined from the scrambled picture hindered by the cloud server. All the neighborhood histograms are grouped together, also, the bunch focuses are utilized as the scrambled visual words. Thus, the pack-of- scrambled words (BOEW) model is worked to speak to each picture by an element vector, i.e., a standardized histogram of the encoded visual words. The similitude between pictures can be straightforwardly estimated by the Manhattan separation between included vectors on the cloud server side. Exploratory outcomes and security investigation on the proposed plan show its pursuit precision and security.

KEYWORDS: Cloud computing, KNN, CBIR, public key, private key, encryption

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relieson sharing of resources to achieve coherence and economies of scale, similar to a public utility. Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.

Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand. Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet). Cloud Computing provides an alternative to the on-premises data centre. With an on-premises data centre, we have to manage everything, such as purchasing and installing hardware, virtualization, installing the operating system, and any other required applications, setting up the network, configuring the firewall, and setting up storage for data. After doing all the set-up, we become responsible for maintaining it through its entire lifecycle .But if we choose Cloud Computing, a cloud vendor is responsible for the hardware purchase and maintenance. They also provide a wide variety of software and platform as a service. We can take any required services on rent. The cloud computing services will be charged based on usage.

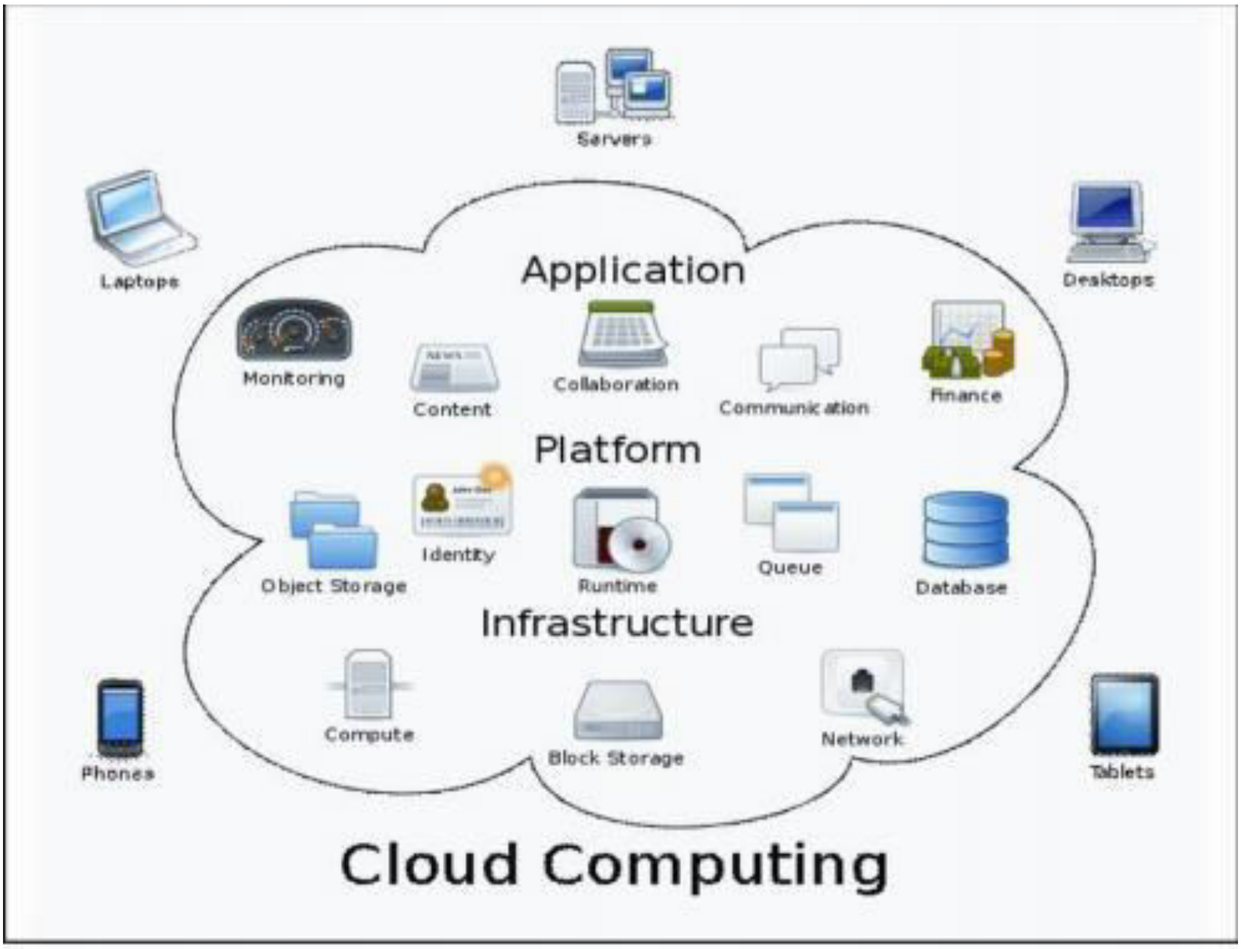


FIGURE 1: Architecture diagram

II. LITERATURE SURVEY

In the year June 2017, Lan Zhang, Taeho Jung proposed a novel system PIC: a Privacy-preserving Image search system on Cloud, which is a step towards feasible cloud services which provide secure content-based large-scale image search with fine-grained access control. Users can search on others' images if they are authorized by the image owners. Majority of the computationally intensive jobs are handled by the cloud, and a querier can now simply send the query and receive the result. Specially, to deal with massive images, we design our system suitable for distributed and parallel computation and introduce several optimizations to further expedite the search process. Our security analysis and prototype system evaluation results show that PIC successfully protects the image privacy at a low cost of computation and communication.

In the year August 2018, Tengfi Yang, Jianfeng Ma proposed a method to implement Hahn moments in the encrypted domain by usingSomewhat Homomorphic Encryption (SHE) in this paper, named Privacy-Preserving Hahn Moments (PPHM). First, a mathematical framework is proposed to implement the PPHM and image reconstruction in the encrypted domain. Then, the detailed theoretical analysis about data expansion and quantization errors shows that plaintext Hahn moments and plaintext image reconstruction can be implemented by utilizing PPHM over encrypted image. Moreover, security analysis shows that the PPHM can guarantee the image content security.

In the year 2017, Haitao Lang, Haibin Ling proposed a novel problem of classifying covert photos, whose acquisition processes are intentionally concealed from the subjects being photographed. Covert photos are often privacy invasive and, if distributed over Internet, can cause serious consequences. Automatic identification of such photos, therefore, serves as an important initial step toward further privacy protection operations.

| DOI: 10.15680/IJIRCCE.2021.0903203|

III. PROPOSED METHODOLOGY DISCUSSION

Storage requirements for visual data have been increasing in recent years, following the emergence of many highly interactive multimediaservices and applications for mobile devices in both personal and corporate scenarios. Existing proposals in this domain remain largely impractical, namely those requiring fully homomorphism encryption, which is still computationally too expensive. Since mobile clients usually have limited computational and storage resources, they tend to rely on cloud services for storing and processing bulky data such as images. In this scenario, mobile clients (users) want to delegate their private image repositories storage to a cloud provider, while coping with the limitations of their device's storage capability, computational power, and battery life. In general, Encryption techniques in image processing lead to change in the size of an encrypted image. So, retrieval cannot be achieved properly. User's privacy is affected due to the carelessness of cloud service providers. Images are leaked due to the lowest security level in the cloud.

Our proposal is based on IES-CBIR, a novel Image Encryption Scheme that exhibits Content- Based Image Retrieval properties. The framework enables both encrypted storage and searching using Content-Based Image Retrieval queries. Images are outsourced to repositories that reside in the cloud. Each repository is used by multiple Users, where they can both add their own images and/or search using a query image. Each repository is created by a single user. Upon the creation of a repository, a new repository key is generated by that user and then shared with other trusted users, allowing them to search in the repository and add/update images. In this work, we use the Bag-Of-Encrypted-Words (BOEW) representation to build a vocabulary tree and an inverted list index for each repository. We choose this approach for indexing as it shows good search performance and scalability properties. In the BOEW model, feature-vectors are hierarchically clustered into a vocabulary tree (also known as codebook), where each node denotes a representative feature-vector in the collection and leaf nodes are selected as the most representative nodes (called visual words).

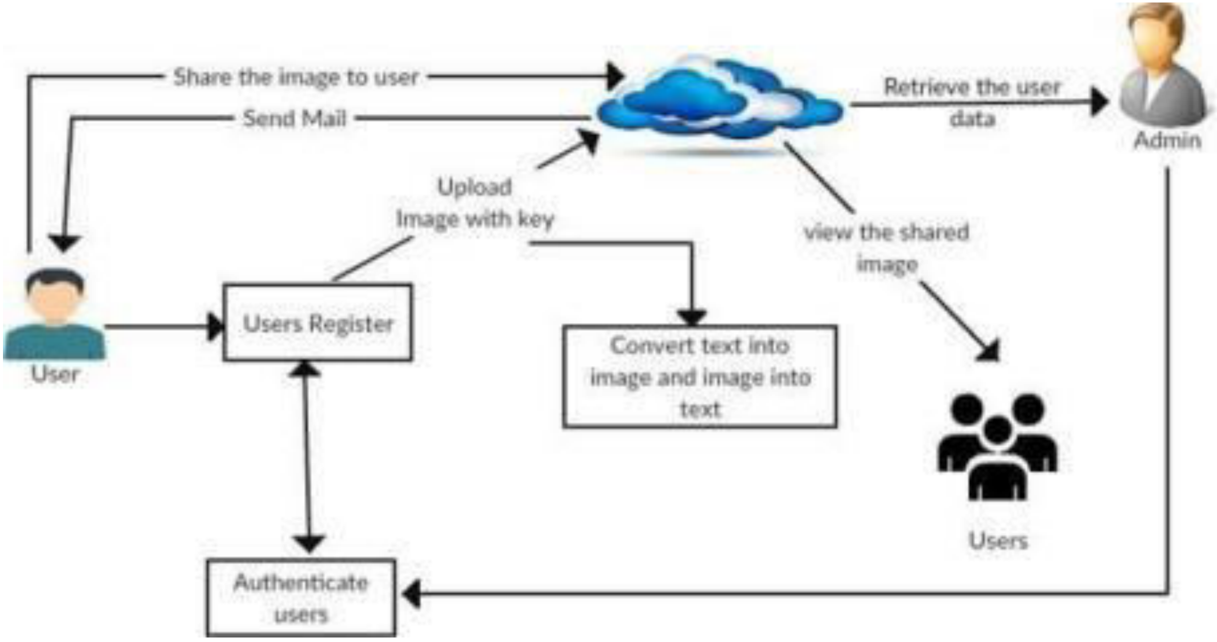


FIGURE 2:Architecture diagram

ADMIN ANALYSIS TO AUTHORIZE

In the module, the admin will be authorizing the user after the user registration. The admin can view all the authorized users and user details including uploaded images of the users. Users can log in to the page only after the admin is authorized.

USER UPLOAD IMAGE

In this module, after the user is authorized by the admin. The user can upload the image to be preserved and generate the key to the user mail and it will store in the database (Cloud Server). the images will be protected by the keys, if some unauthorized users try to extract the information only the encrypted image or text will be visible. It will be visible in the alphabet, special symbol and number (such as kdjfhjs2761@$h7#). We have used the CBIR algorithm for the encryptionof images.

RENOVATION OF TEXT AND IMAGE

In this module, after uploading the image into the database with the key if a user wants to convert the image into text they can convert it in this module. similarly, they can convert text into an image. A redistributed CBIR conspire dependent on a novel packof-scrambled words (BOEW) model is used for this conversion. The picture is scrambled by shading esteem substitution, square stage, and intra-square pixel change. At that point, the nearby histograms are determined from the scrambled picture hindered by the cloud server. All the neighborhood histograms are grouped, also the bunch focuses are utilized as the scrambled visual words

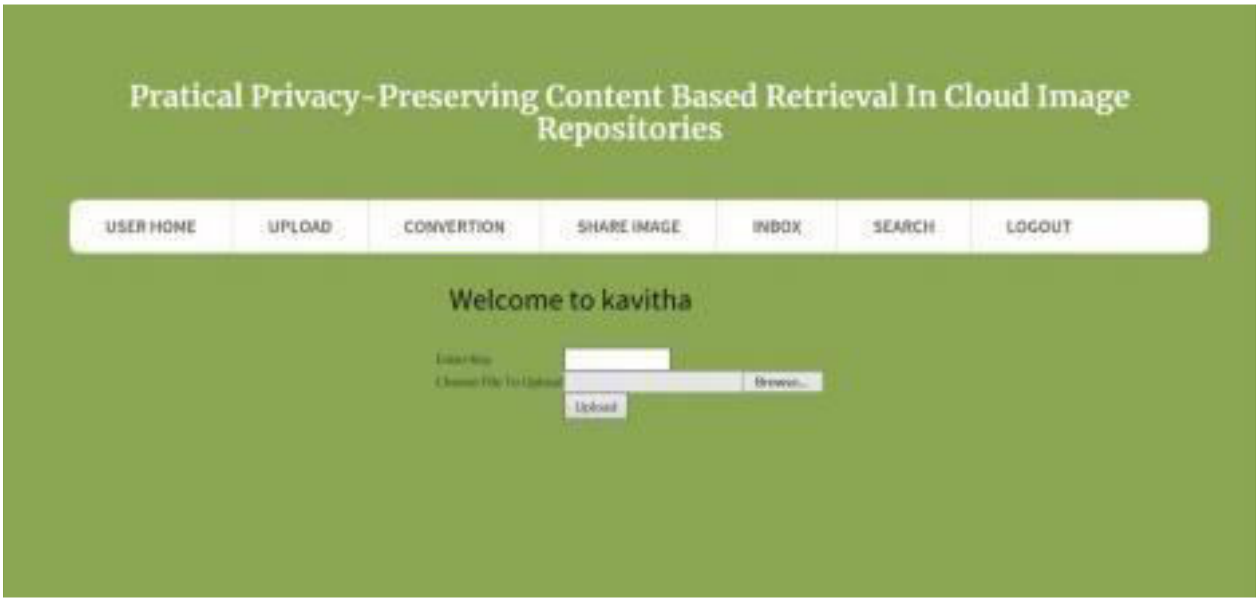
SEEK OF IMAGE

In this module, if they want any images that upload by the user. The user can share the image or document to another user if user want know about information document. Shared images will be displayed in the inbox of the user like mail they can share the imageor document shared images or document can be download from inbox. While downloading the image or document sent by another user verification key should be entered. They can search the image by using the content of an image or by using the file name of theimage document

VERIFICATION KEY AND DOWNLOAD IMAGE

The images shared can be downloaded after the verification of the key which has been sent to the user's mail while uploading the image in the cloud. KNN classifier plays an important role in maintaining the security of the keys. k-Nearest Neighbor (KNN) algorithm is proposed to protect the key from being completely leaked to untrusted image users. The KNN classifier can effectivelydetect intrusive attacks and achieve a low false-positive rate.

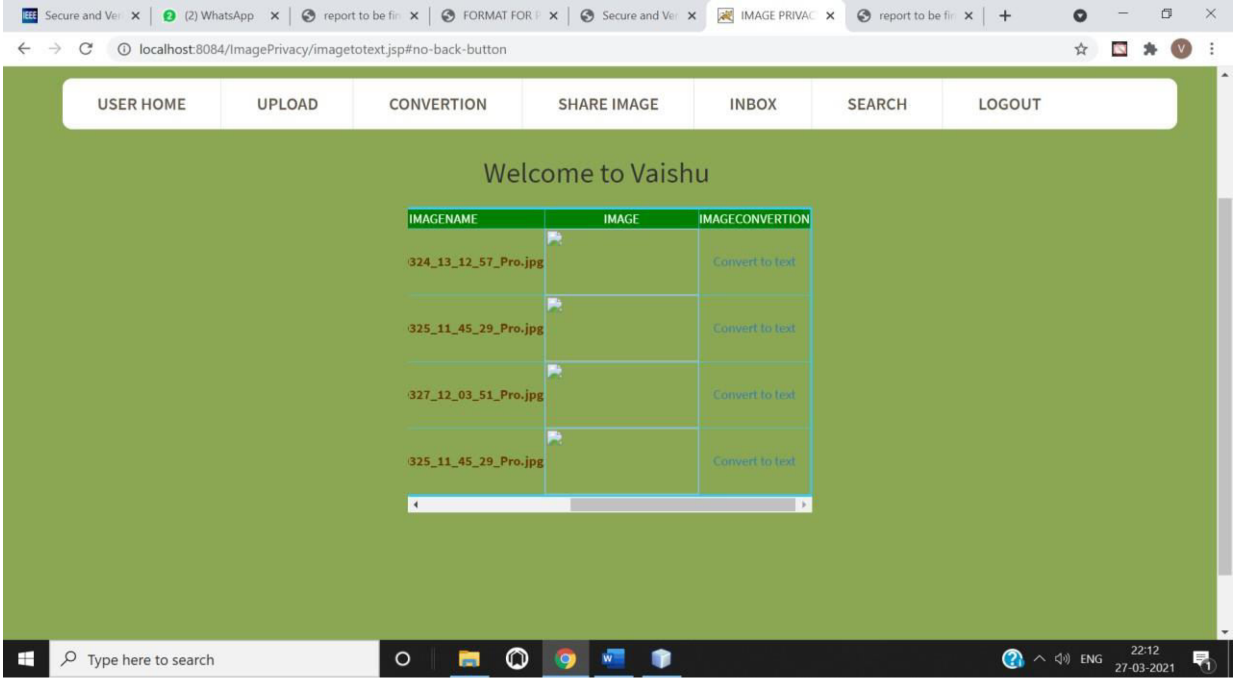
IV. EXPERIMENTAL RESULTS



Pratical Privacy-Preserving Content Based Retrieval In Cloud Image Repositories

Welcome to kavitha

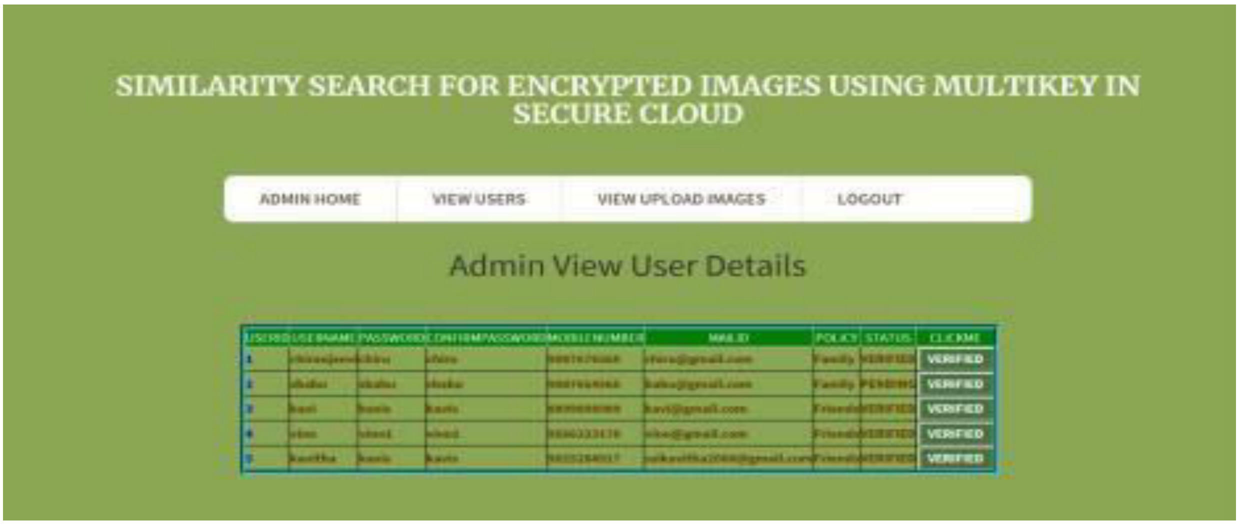
FIGURE 3: Image upload



Welcome to Vaishu

IMAGENAME	IMAGE	IMAGECONVERTION
324_13_12_57_Pro.jpg		Convert to text
325_11_45_29_Pro.jpg		Convert to text
327_12_03_51_Pro.jpg		Convert to text
325_11_45_29_Pro.jpg		Convert to text

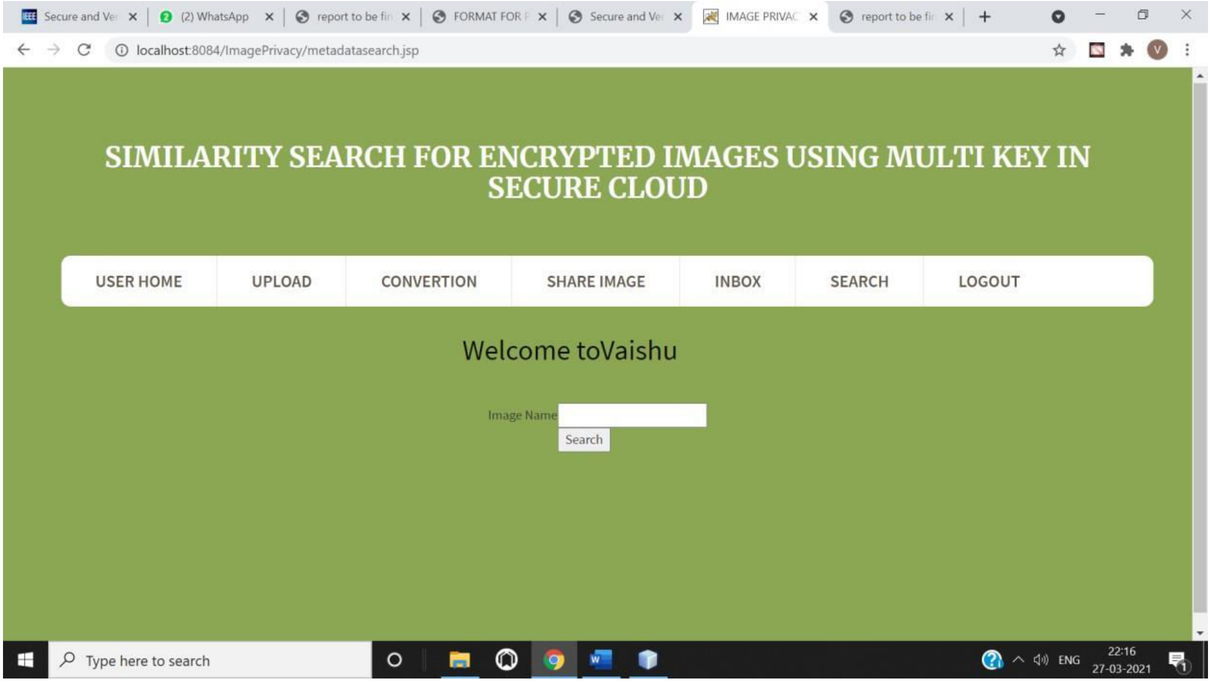
FIGURE 4: Uploaded image conversion


SIMILARITY SEARCH FOR ENCRYPTED IMAGES USING MULTIKEY IN SECURE CLOUD

Admin View User Details

USERID	USERNAME	PASSWORD	CONFIRMPASSWORD	MOBILENUMBER	MAILID	POLICY	STATUS	CLICKME
1	[illegible]	chiru	chiru	[illegible]	chiru@gmail.com	Family	VERIFIED	VERIFIED
2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Family	PENDING	VERIFIED
3	kavi	kavis	kavis	[illegible]	kavi@gmail.com	Friends	VERIFIED	VERIFIED
4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Friends	VERIFIED	VERIFIED
5	kavitha	kavis	kavis	[illegible]	[illegible]	Friends	VERIFIED	VERIFIED

FIGURE 5: Admin View



SIMILARITY SEARCH FOR ENCRYPTED IMAGES USING MULTI KEY IN SECURE CLOUD

Welcome toVaishu

Image Name

FIGURE 6: Image search

V. CONCLUSION

A novel protection saving CBIR plot is proposed. An epic sack of-scrambled words (BOEW) model is intended to accomplish a decent recovery precision. As a case study, we secure the picture content by shading esteem substitution, square change, and intra-square pixel stage. Neighborhood histograms are determined as nearby highlights. k-implies calculation is used to create encoded visual words. The histogram of the visual words is determined to speak to the picture. The comparability between pictures can be straightforwardly estimated by the Manhattan separation between highlight vectors on the cloud server side. Other than the hunt activity, the list development in our plan can be likewise redistributed to the cloud server.

VI. FURTURE ENHANCEMENT

The proposed plan can be additionally improved. Initially, it could be a significant future work to configure better nearby descriptors under our BOEW model. Furthermore, how to secure the picture content under CPA model needs further thoughtabout. At long last, it could be intriguing to apply the BOEW model to JPEG pictures.

REFERENCES

1. J.M. Lewin, R. E. Hendrick, C. J. D'Orsi, P. K. Isaacs, L. J. Moss, A. Karellas, G. A. Sisney, C. C. Kuni, and G. R. Cutter, "Comparison of full-field digital mammography with screen-film mammography for cancer detection: results of 4,945 paired exam-inations." *Radiology*, vol. 218, no. 3, pp. 873–80, 2001.
2. C. S. Lu, "Homomorphic encryption-based secure sift for privacy-preserving feature extraction," *Proceedings of SPIE TheInternational Society for Optical Engineering*, vol. 7880, no. 2, pp. 788 005–17, 2011.
3. B. Ferreira, J. Rodrigues, J. Leit˜ao, and H. Domingos, "Privacy-preserving content-based image retrieval in the cloud," in
4. *IEEE 34th Symposium on Reliable Distributed Systems*. IEEE, 2015, pp.11–20.
5. B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, "Practical privacy-preserving content-based retrieval in cloudimage reposi- tories," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, pp. 1–1, 2017.
6. Y. Rui, T. S. Huang, M. Ortega, and S. Mehrotra, "Relevance feed-back: a power tool for interactive content-based image retrieval," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 8, no. 5, pp. 644–655, 1998.
7. Y. Liu, D. Zhang, G. Lu, andW.-Y. Ma, "A survey of content-based image retrieval with high-level semantics,"
8. *Pattern Recognition*, vol. 40, no. 1, pp. 262–282, 2007.

9. C. B. Akg¨ ul, D. L. Rubin, S. Napel, C. F. Beaulieu, H. Greenspan, and B. Acar, "Content-based image retrieval in radiology: current status and future directions," *Journal of Digital Imaging*, vol. 24, no. 2, pp. 208–222, 2011.
10. X. Zhang, W. Liu, M. Dundar, S. Badve, and S. Zhang, "Towards large-scale histopathological image analysis: Hashing-based image retrieval," *IEEE Transactions on Medical Imaging*, vol. 34, no. 2, pp. 496–506, 2015.
11. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," *Journal of Computer Security*, vol. 19, no. 5, pp. 79–88, 2011.
12. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp.1–5.
13. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on parallel and distributed systems*, vol. 25, no. 1, pp. 222– 233, 2013.
14. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over
15. encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2016.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING