IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

A Secure Framework for Content Based Image Retrieval in Cloud Repositories

Rahul Hariharan D, Sarran J T, Vishal P K, R. Chitra

U.G Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

U.G Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

U.G Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Associate Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: Storage requirements for visual data have been increasing in recent years, following the emergence of many highly interactive multimedia services and applications for mobile devices in both personal and corporate scenarios. This has been a key driving factor for the adoption of cloud-based data outsourcing solutions. However, outsourcing data storage to the Cloud also leads to new security challenges that must be carefully addressed, especially regarding privacy. In this paper we propose a secure framework for outsourced privacy-preserving storage and retrieval in large shared image repositories. 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 while preserving privacy against honest-but-curious cloud administrators. We have built a prototype of the proposed framework, formally analysed and proven its security properties, and experimentally evaluated its performance and retrieval precision. Our results show that IES-CBIR is provably secure, allows more efficient operations than existing proposals, both in terms of time and space complexity, and paves the way for new practical application scenarios.

KEYWORDS: Cloud Computing, Privacy, Image.

I. INTRODUCTION

To propose a secure framework for outsourced privacy-preserving storage and retrieval in large shared image repositories. Cloud computing is a new form of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is the delivery of hosted services over the internet. Cloud computing services can be public, private or hybrid. The growing industry of cloud has provided a service paradigm of storage/computation outsourcing helps to reduce users' burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users. The three main benefits of cloud computing are self-service provisioning, elasticity, pay per use. The three broad categories of cloud computing are Infrastructure as a Service, Platform as a Service and Software as a Service.

II. LITERATURE SURVEY

Project Title : Bootstrapping for Approximate Homomorphic Encryption
Author Name : Jung HeeCheon,Kyoohyung Han, Andrey Kim.
Year of Publish : 2017
Abstract : This paper extends the leveled homomorphic encryption scheme for an approximate arithmetic of Cheon et al. (ASIACRYPT 2017) to a fully homomorphic encryption, i.e., we propose a new technique to refresh low-level ciphertexts based on Gentry's bootstrapping procedure.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

The modular reduction operation is the main bottleneck in the homomorphic evaluation of the decryption circuit. We exploit a scaled sine function as an approximation of the modular reduction operation and present an efficient evaluation strategy. Our method requires only one homomorphic multiplication for each of iterations and so the total computation cost grows linearly with the depth of the decryption circuit.

Project Title : Privacy-Preserving Content-Based Image Retrieval in the Cloud
Author Name : Bernardo Ferreira, Joao Rodrigues, Joao Leitao, Henrique Domingos
Year of Publish : **2014**
Abstract : Storage requirements for visual data has been increasing in recent years, following the emergence of many new services and applications for both personal and corporate use. This has been a key driving factor for the adoption of cloud-based data outsourcing solutions. However, outsourcing data storage to the Cloud also leads to new challenges that must be carefully addressed, especiallyregarding privacy. In this paper we propose a novel secure framework for outsourced and distributed privacy- preserving storage and retrieval in large image repositories. Our proposal is based on a novel cryptographic scheme, named IES-CBIR, specifically designed for media image data. Our solution enables both encrypted storage and querying using Content Based Image Retrieval (CBIR) while preserving privacy. We have built a prototype of the proposed framework, analyzed its security properties, and experimentally evaluated its performance and precision. Our results show that IES-CBIR allows more efficient operations than existing proposals, both in terms of time and space complexity, while enabling less restrictive use cases and application scenarios.

Project Title : An ID-Based Public Key Cryptosystem based onInteger Factoring and Double Discrete Logarithm Problem.
Author Name : Chandrashekhar Meshram, Shyam Sundar Agrawal.
Year of Publish : 2014
Abstract : In 1984, Shamir [1] introduced the concept of anidentity-based cryptosystem. In this system, each user needs to visit a key authentication center (KAC) and identify himself before joining a communication network. Once a user isaccepted, the KAC will provide him with a secret key. In this way, if a user wants to communicate with others, he only needs to know the "identity" of his communication partner and the public key of the KAC. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. In this paper, we propose an id-based cryptosystem based on the integer factoring and double discrete logarithm problem and we consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.

Project Title : Enabling Privacy-preserving Image-centric Social Discovery
Author Name :Xingliang Yuan, Xinyu Wang, Cong Wang, Anna Squicciarini, andKui Ren
Year of Publish : **2014**
Abstract : The increasing popularity of images at social media sites is posing new opportunities for social discovery applications, i.e., suggesting new friends and discovering new social group with similar interests via exploring images. To effectively handle the explosive growth of images involved in social discovery, one common trend for many emerging social media sites is to leverage the commercial public cloud as their robust backend datacenter. While extremely convenient, directly exposing content-rich images and the related social discovery results to the public cloud also raises new acute privacy concerns. In light of the observation, in this paper we propose a privacy-preserving social discovery service architecture based on encrypted images. As the core of such social discovery is to compare and quantify similar images, we first adopt the effective Bag-of-Words model to extract the "visual similarity content" of users' images into image profile vectors, and then model the problem as similarity retrieval of encrypted high-dimensional image profiles. To support fast and scalable similarity search over hundreds of thousands ofencrypted images, we propose a secure and efficient indexing structure.

Project Title : Privacy Preserving Processing Over Encrypted Images
Author Name : M.Tarek Ibn Ziad, Amr Alanwar, MoustafaAlzantot, Mani Srivasta.
Year of Publish : 2016
Abstract : Cloud computing services provide a scalable solution for the storage and processing of images and multimedia files. However, concerns about privacy risks prevent users from sharing their personal images with third-party services. In thispaper, we describe the design and implementation of CryptoImg, a library of modular privacy preserving image processing operations over encrypted images. By using homomorphic encryption, CryptoImg allows

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

the users to delegate their image processingoperations to remote servers without any privacy concerns. Currently, CryptoImg supports a subset of the most frequently used image processing operations such as image adjustment, spatial filtering, edge sharpening, histogram equalization and others. We implemented our library as an extension to the popular computer vision library OpenCV. CryptoImg can be used from either mobile or desktop clients. Our experimental results demonstrate that CryptoImg is efficient while performing operations over encrypted images with negligible error and reasonable time overheads on the supported platforms

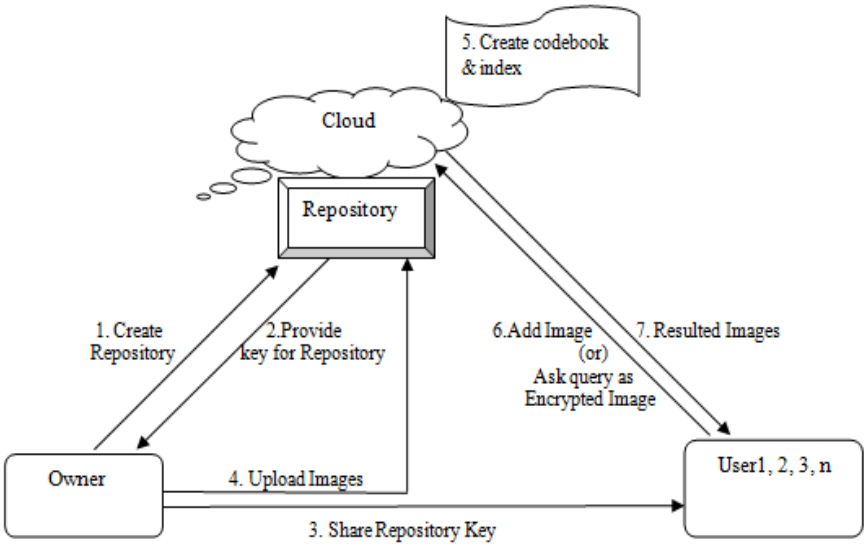
III. PROPOSED METHOLODOGY AND DISCUSSION

Existing System:

Storage requirements for visual data have been increasing in recent years, following the emergence of many highly interactive multimedia services and applications for mobile devices in both personal and corporate scenarios. Existing proposals in this domain remain largely unpractical, 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.

Proposed System:

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 multiples 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-Visual-Words (BOVW) 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.



| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

Create Repository & Upload Images:

Repository is storage space of collection of data. Each repository is created by single user. He is the owner of that repository. Then, he generates a key for that repository by using RSA algorithm and shared with the users who are all have an account to access it. Now, Repository can be accessed by multiple users with the permission of an owner. Then, owner upload huge amount of image datasets as zip file into the cloud.

Codebook & Index generation:

The admin of cloud has responsibility to create documents based on images which is useful for searching of images by users. So, he extracts zip file and applying CBIR Encryption technique. It encrypts images based on color values and texture features and also shuffling the pixels in column-wise as well as row-wise. Then, he creates codebook, index and image key for those encrypted images. These files are used to improve the searching efficiency of cloud and also manage the time properly while retrieving answer.

Add Image/Query to cloud:

Now, Users can access the cloud to add their own images into the repository. So, if that cloud has 'n' number of users, then repository has chance to increase rapidly. Now, the repository has collection of 'n' number of images in different domains. All the images are stored in encrypted format for security. Then, user has to ask query to cloud. Its take query is in the format of encrypted image using CBIR encryption technique.

Content Based Searching & Retrieval:

After receiving encrypted image query, the cloud extracts the features of an original image. Now applying content-based searching on the codebook and image index by using that extracted features. Obviously, now searching results will be an encrypted image. This resulted answer will send to that corresponding user. Now, user can apply CBIR decryption technique to decrypt the retrieved images. So, the answer will be very fine and delicious due to huge dataset.

AES Algorithm:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

RSA Algorithm:

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.RSA involves a public key and private key.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

IV. RESULTS

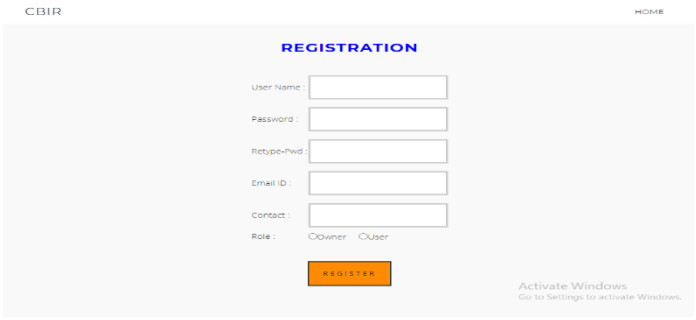


Fig. 2: Registration Form

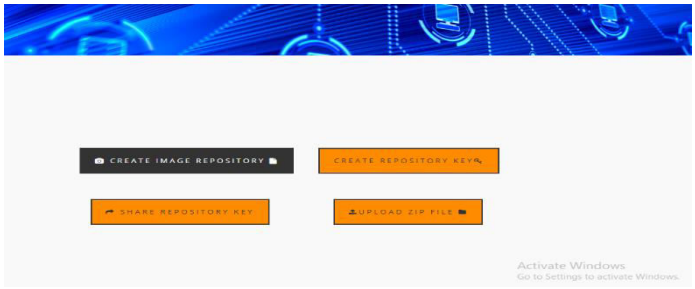


Fig. 4: Owner Page

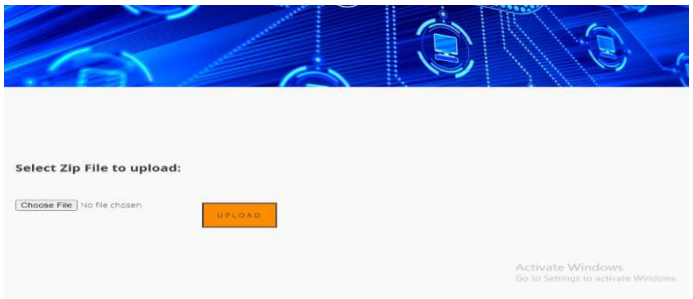


Fig. 5: Zip upload page

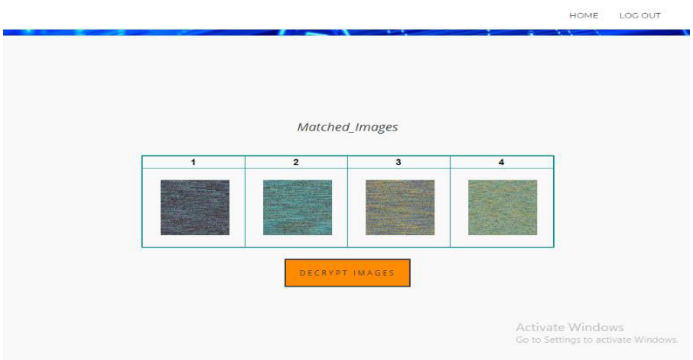


Fig. 6: Encrypted Search Results

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

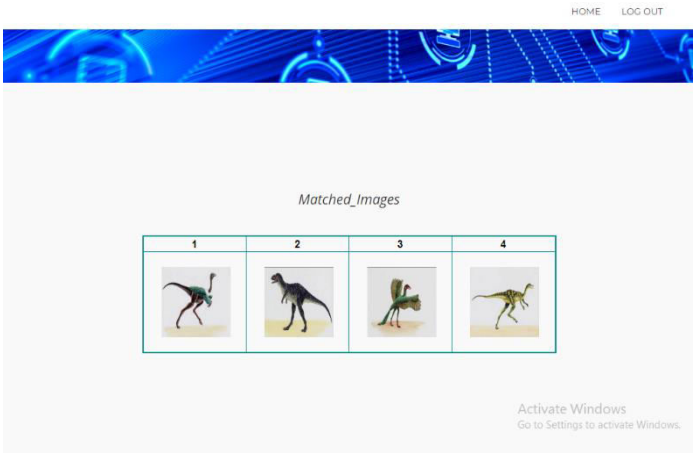


Fig 7: Decrypted Search Results

V. CONCLUSION

In this paper we have proposed a novel cryptographic scheme, named IES-CBIR, to support privacy-preserving out sourcing of storage and search/retrieval of images in the encrypted domain, implemented with readily-available storage clouds. Key to the design of IES-CBIR is the observation that in images, color information can be separated from texture information, enabling the use of different encryption techniques with different properties for each one. Leveraging IES-CBIR, we designed a secure framework focused on dynamic, multitenant image outsourcing, focused on retrieval scenarios, where the reduction of network traffic and client's computational overhead were central aspects of the design. To validate our proposal in terms of security, efficiency, and precision, we presented a formal analysis and experimental evaluation of a prototype system leveraging IES-CBIR, comparing the results with relevant alternatives from the literature. Obtained results show that our approach is secure and doesn't leak private information of involved parties while having good retrieval precision, and better performance with lower computational overhead imposed on clients. This work's main focus is on privacy issues.

VI. FUTURE WORK

One has to consider issues related to reliability and availability as complementary dependability criteria. While we don't address these explicitly in this paper, we plan to focus on them in future work, by combining different cloud infrastructures with independent administration and independent failures, exploring diversity to improve dependability criteria, fault-tolerance and intrusion-resilience.

REFERENCES

[1] M. Meeker, "Internet Trends 2015," in Code Conf., 2015.
[2] Global Web Index, "Instagram tops the list of social network growth," http://tinyurl.com/hnwwlzm, 2013.
[3] C. D. Manning, P. Raghavan, and H. Sch ¨ utze, An Introduction to Information Retrieval. Cambridge University Press, 2009, vol. 1.
[4] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in CCSW'09, 2009.
[5] D. Rushe, "Google: don't expect privacy when sending to Gmail," http://tinyurl.com/kjga34x, 2013.
[6] G. Greenwald and E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," http://tinyurl.com/oea3g8t, 2013.
[7] A. Chen, "GCreep: Google Engineer Stalked Teens, Spied on Chats," http://gawker.com/5637234, 2010.
[8] J. Halderman and S. Schoen, "Lest we remember: cold-boot attacks on encryption keys," in Commun. ACM, vol. 52, no. 5, 2009.
[9] National Vulnerability Database, "CVE Statistics," http://web.nvd.nist.gov/view/vuln/statistics, 2014.
[10] D. Lewis, "iCloud Data Breach: Hacking And Celebrity Photos," https://tinyurl.com/nohznmr, 2014.
[11] A. W. M. Smeulders, M. Worring, S. Santini, A. Gupta and R. Jain, "Content-based image retrieval at the end of the early years", IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 12, pp. 1349-1380, Dec. 2000.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003190

[12] Y. Rui, T. S. Huang and S.-F. Chang, "Image retrieval: Current techniques promising directions and open issues", J. Vis. Commun. Image Representation, vol. 10, no. 1, pp. 39-62, 1999.
[13] R. Datta, J. Li and J. Z. Wang, "Content-based image retrieval: Approaches and trends of the new age", Proc. 7th ACM SIGMM Int. Workshop Multimedia Inf. Retrieval, pp. 253-262, 2005.
[14] W. Lu, A. Swaminathan, A. L. Varna and M. Wu, "Enabling search over encrypted multimedia databases" in SPIE, San Jose, CA, USA, vol. 7254, 2009.
[15] W. Lu, A. L. Varna, A. Swaminathan and M. Wu, "Secure image retrieval through feature protection", Proc. IEEE Int. Conf. Acoust. Speech Signal Process., pp. 1533-1536, 2009.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details