Privacy-Preserving Content-Based Image Retrieval and Sharing in the Cloud

Mr. K. Gopi[1], P. Gayathri[2], S. Maheswari[3], P. Bala Praveena[4], N. Harini[5]
[1]Assoc. Prof, Dept of CSE, Tirumala Engineering College, Narasaraopet, Guntur, A.P., India
[2,3,4,5]B. Tech Students, Dept of CSE, Tirumala Engineering College, Narasaraopet, Guntur, A.P., India

ABSTRACT - Storage needs for visual data have risen in recent years, as a result of the proliferation of modern increasingly immersive digital services and software for both personal and corporate use. This has become a major motivator for the use of cloud-based data outsourcing solutions. Outsourcing data management to the Cloud, on the other hand, introduces new problems that must be carefully handled, especially in terms of privacy. We suggest a reliable mechanism for outsourced privacy-preserving storage and retrieval in broad image repositories in this article. Our proposal is built on a new Image Encryption Scheme with Content-Based Image Retrieval capabilities. Our solution allows for secure storage as well as browsing using CBIR queries while maintaining privacy. We created a prototype of the proposed architecture, formalized and validated its security properties, and experimentally assessed its performance and precision. Our findings show that is provably stable, makes for more effective operations in terms of both time and space complexity, and facilitates more accurate realistic implementation scenarios.

Keywords: Image retrieval, image sharing, multimedia, privacy-preserving

I. INTRODUCTION

Visual evidence now accounts for a sizable portion of global Internet traffic in both business and personal contexts [1]. The number of photographs, graphics, and photos created and posted every day is the at an alarming pace. The need for vast volumes of data storage has been a guiding force for data outsourcing services such as those that use Cloud Storage and Computing solutions. Such networks (for example, Instagram and Flickr) are said to be among the fastest growing internet services [2]. Furthermore, the existence of vast volumes of photographs in public and private libraries necessitates the use of content-based search and retrieval (CBIR) technologies [3].

While data outsourcing seems to be a natural option for supporting large-scale image storage and retrieval schemes, it actually introduces new problems in terms of data control and privacy. This is a result of outsourcing info, which normally entails relinquishing control over it [4]. Recent events have shown unequivocally that Cloud vendors cannot be trusted to protect their customers' data.
Furthermore, malicious server managers operating with the vendors have complete access to data on the cloud machines running them. Finally, remote hackers may take advantage of programme flaws to obtain unauthorized access to servers. The latest event involving the iCloud image management provider and celebrity photo leaks highlights the significance of these risks for cloud-based visual data stores.

The traditional way to addressing privacy in this case is to encrypt confidential data before outsourcing it and to do all computations on the client side. However, this introduces an excessive amount of client overhead because data must be regularly copied, decrypted, stored, and safely re-uploaded. Many applications, especially online and mobile applications that operate on very large datasets, such as image repositories with CBIR services, are unable to cope with this overhead. Outsourcing computations and doing procedures over encrypted data on the server side will be a more feasible method. Existing proposals in this domain, including those involving completely homomorphic encryption, are also computationally prohibitively costly.

II. RELATED WORK

[6] Previous ideas for promoting outsourced image storage, discovery, and retrieval in the encrypted domain can be narrowly classified into two types: Searchable Symmetric Encryption (SSE)-based approaches and Public-Key Partially-Homomorphic approaches (PKHE). SSE has been extensively used in the scientific community in the past for both text and image retrieval. Clients use SSE-based tools to process and encrypt their data before sending it to the Cloud. This processing results in the development, encryption, and storage of an index in the outsourced infrastructure, allowing clients to search their data quickly and securely. Usually, data is encrypted using a probabilistic symmetric-key encryption scheme, whereas the index is secured using a hybrid of probabilistic and deterministic encryption.

[7] The literature-available alternatives to SSE are focused on public-key partially-homomorphic encryption (PKHE). Clients encrypt images pixel by pixel using a PKHE scheme with these methods, enabling the cloud to store and

index their encrypted images on their behalf while eliminating many of the realistic problems associated with SSE-based solutions. Unfortunately, PKHE works are even more time and space consuming.

[10] Formalized paraphrase Aside from the SSE and PKHE research directions, other studies have taken similar approaches to what we suggest in this article, but for different reasons. However, the work does not support large-scale repositories since it only allows linear searching, requires the template being matched to be re-encrypted for comparison for each different image in a repository, and relies on the availability of public images as noise for encryption, which can easily be found by an attacker using common high-availability repositories for dictionary attacks or by tracking a repository.

[11] which proposes a series of algorithms for the encryption of various data structures, including matrix-based datatypes like photos, thus allowing queries to be performed over the ciphertext Their key motivation, however, is to retrieve partial knowledge over a single encrypted data item, while we concentrate on allowing an untrusted third party to generate indexes over large collections of encrypted images and resolve user queries about these large collections.

III. PROPOSED ARCHITECTURE

We will now go into an example device model and design that we visualise using our framework and CBIR. We consider two major entities in this model: the cloud and consumers. Images are outsourced to cloud-managed servers. Each archive is used by different Users, who can also add their own images and search for images using a query image. Users may also insist that their creators/owners grant them access to stored images. Our goal is to protect users' privacy, so all data sent to the cloud is encrypted.

A single account creates repositories. When a repository is created, the user generates a new repository key, which is then exchanged with other trustworthy users, allowing them to search the repository and store new photos. A user would also require an image key created for that image in order to add/update pictures. Camera keys are kept confidential from their users, which means that even users who may browse a registry must query the owners of unique photos for access to them. It should be noted that in our environment, using separate keys per-file is optional; that is, if registry users want to eliminate additional key management work and are able to lose fine-grained access control, they may use the same image key for all images or in groups of images.

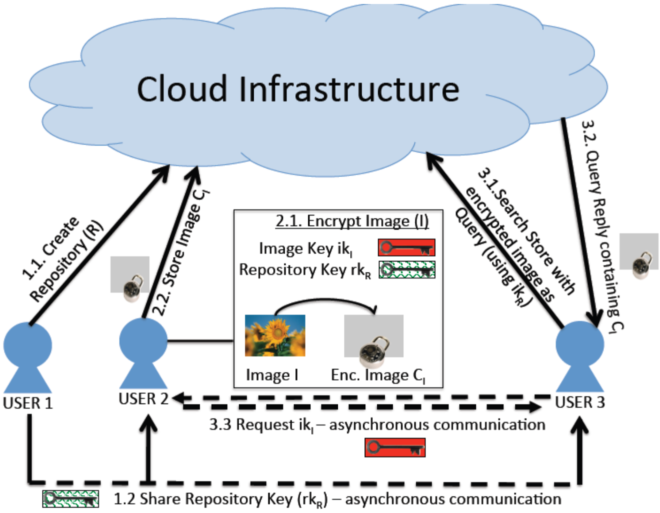
Cloud Infrastructure
1.1. Create Repository (R)
2.2. Store Image C_I
2.1. Encrypt Image (I)
Image Key ik_I
Repository Key rk_R
Image I
Enc. Image C_I
3.1.Search Store with encrypted image as Query (using ik_I)
3.2. Query Reply containing C_I
USER 1
USER 2
USER 3
3.3 Request ik_I – asynchronous communication
1.2 Share Repository Key (rk_R) – asynchronous communication

Figure 1.Proposed Architecture

IV. RESULTS AND OBSERVATION

When compared to the remaining competitive alternatives, the findings show that IES-CBIR with image compression provides overall improved efficiency. This is due to IES-extremely CBIR's high cryptographic throughput, coupled with the fact that users just need to encrypt photos. Other alternatives, on the other hand, either have very poor cryptographic throughput (PKHE) or enable users to perform indexing operations (SSE). More specifically: IES-CBIR without compression has somewhat higher cryptographic throughput, however the performance gained is lost as the user uploads larger decompressed images; PKHE has prohibitive overheads due to both the low cryptographic throughput of the public-key Paillier cryptosystem and its high ciphertext expansion; and SSE needs costly initial training performed by the user.

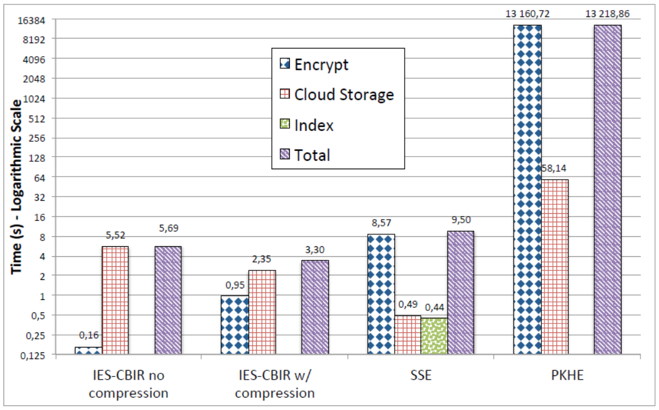

Figure 2. Comparison Results

V. CONCLUSION

In this paper, we suggested a new stable architecture for the privacy-preserving outsourced collection, discovery, and retrieval of large-scale, dynamically modified image libraries, with a focus on minimizing client overheads. The IES-CBIR cryptographic system, which is specially developed for photos, serves as the foundation of our framework. The discovery that color information in images can be distinguished from texture information was key to its creation, allowing the use of different encryption methods with different properties for each one and allowing privacy-preserving Content-Based Image Retrieval to be done by third-party, untrusted cloud servers. We formalized our proposals' security, and additional experimental evaluation of applied prototypes demonstrates that our approach achieves a fascinating trade-off between precision and recall in CBIR, while demonstrating high efficiency and scalability as compared to alternative solutions.

VI. REFERENCES

[1]. M. Meeker and L. Wu, “Internet Trends,” in D11 Conf., 2013.

[2]. Global Web Index, “Instagram tops the list of social network growth,” http://blog.globalwebindex.net/instagram-tops-list-of-growth, 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, pp. 91–98.

[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]. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, “Depot: Cloud Storage with Minimal Trust,” ACM Trans. Comput. Syst., vol. 29, no. 4, pp. 1–38, Dec. 2011.

[12]. C. Gentry, S. Halevi, and N. P. Smart, “Homomorphic evaluation of the AES circuit,” in CRYPTO’12. Springer, 2012, pp. 850–867.

[13]. P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in EUROCRYPT’99, 1999, pp. 223–238.

[14]. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” in Adv. Cryptol. Springer, 1985, pp. 10–18.

[15]. C.-Y. Hsu, C.-S. Lu, and S.-c. Pei, “Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT,” IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593–4607, 2012.