International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 588 - 592

Secured Uploading and Retrieval of Data Using Visual Cryptography Scheme

Priyanka.K
Computer Science & Engineering
Easwari Engineering College
Chennai, India
priyanka.sharlinn@gmail.com

Mrs.V.Mercy Rajaselvi M.E(Ph.D)
Asst Professor - Selection Grade
Easwari Engineering College
Chennai, India
mercyeec@gmail.com

Abstract-Cloud storage provides a convenient, massive, and scalable storage at low cost, but data security is a major issue that prevents users from storing files on the cloud. This paper focuses on security for the documents that are uploaded and stored on the cloud. However, it poses risks to end users unless the data is encrypted for security. This study addresses these issues by proposing Visual Cryptography Scheme (VCS) for securing the files. In order to prevent issues like breaches and malware attacks on cloud, this innovative scheme helps in high level security to safeguard the files that are stored on the cloud.

Keywords: *Visual Cryptography Scheme, Order Preserving Encryption, Advanced Encryption Standard.*

*****

I. Introduction

Cloud computing and storage provide consumers and enterprises with various capabilities to store and process their data. Organizations use Cloud in a variety of different service models (SaaS , PaaS , and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are privacy concerns associated with cloud computing. These issues are classified into two categories: security issues faced by cloud providers and security issues faced by their customers. The provider must ensure that their infrastructure is secure and that their clients' information and applications are secure while the end user must take way to reinforce their relevance and use strong passwords and authentication system are taken.

When an organization elects to store data or host applications on the public cloud, it loses its potential to have physical access to the servers hosting its information. As a result, confidential data is at risk from insider attacks. Therefore, cloud providers must guarantee that thorough background checks are conducted for employees who have physical access to the servers in the data centre.

In order to safeguard resources, cut costs and maintain good organization, service providers often store more than one customer's data on the same server. As a result, there is a possibility that one user's private data can be viewed by other users (possibly even competitors). To handle such receptive situations, service providers should make

proper data isolation and logical storage segregation.

The wide-ranging use of virtualization in implementing cloud infrastructure brings exceptional refuge concerns for users or tenants of a public cloud service. This introduces an additional layer - virtualization that itself must be properly configured, managed and secured. Specific concerns include the latent to conciliation the virtualization software or "hypervisor". While these concerns are largely theoretical, they do exist.

II. Previous work

Mingyuan Xia et al (2015) [1] enhances data storage in the cloud infrastructure which is rapidly gaining popularity throughout the world. However, it poses risks to consumers unless the data is encrypted for security. Encrypted data should be effectively searchable and retrievable without any privacy leaks, particularly for the mobile client. Although recent research has solved many security issues, the architecture cannot be applied on mobile devices directly under the mobile cloud environment. This is due to the challenges imposed by wireless networks, such as latency sensitivity, poor connectivity, and low transmission rates. This leads to a long search time and extra network traffic costs when using traditional search schemes. This study addresses these issues by proposing an efficient Encrypted data Search (EnDAS) scheme as a mobile cloud service. This innovative scheme uses a lightweight trapdoor (encrypted keyword) compression method, which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency. In this study, we also propose two optimization methods for document search, called the Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) algorithm, to speed the search time. Results show that EnDAS reduces search time by 34% to 47% as well as network traffic by 17% to 41%.

H. Guan et al (2015) [2] enhances privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging. In this paper, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied. Our experiments show that TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55%

per file retrieval, meanwhile the network traffics during the file retrievals are also significantly reduced.

Farrukh Shahzad et al (2015) [3] proposed an evolution of cloud computing which has revolutionized the computing is abstracted and utilized on remote third party infrastructure. It is now feasible to try out novel ideas over the cloud with no or very low initial cost. There are challenges in adopting cloud computing; but with obstacles, we have opportunities for research in several aspects of cloud computing. One of the main issue is the data security and privacy of information stored and processed at cloud provider's systems. In this work, a practical system (called SAFE) is designed and implemented to securely store/retrieve user's files on the third party cloud storage systems using well established cryptographic techniques. It utilizes the client-side, multilevel, symmetric/asymmetric encryption and decryption operations to provide policy-based access control and assured deletion of remotely hosted client's files. The SAFE is a generic application which can be extended to support any cloud storage provider as long as there is an API which support basic file upload and download operations.

Xing Sun et al (2013) [4] proposed an approach in cloud computing that enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data has to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is inherently demanded by large number of users and huge amount of data files in cloud. In this paper, we define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e. relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy. Thorough analysis shows that our proposed solution enjoys "as-strong-as possible" security guarantee compared to previous searchable encryption schemes, while correctly realizing the goal of ranked keyword search.

Haibing Guan et al (2012) [5] enhanced cloud computing that prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, for the first time we define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE).

Cengiz Örencik et al (2012) [6] developed Information search and document retrieval from a remote database (e.g. cloud server) requires submitting the search terms to the database holder. However, the search terms may contain sensitive information that must be kept secret from the database holder. Moreover, the privacy concerns apply to the relevant documents retrieved by the user in the later stage since they may also contain sensitive data and reveal information about sensitive search terms. A related protocol, Private Information Retrieval (PIR), provides useful cryptographic tools to hide the queried search terms and the data retrieved from the database while returning most relevant documents to the user. In this paper, we propose a practical privacy-preserving ranked keyword search scheme based on PIR that allows multi-keyword queries with ranking capability. The proposed scheme increases the security of the keyword search scheme while still satisfying efficient computation and communication requirements. To the best of our knowledge the majority of previous works are not efficient for assumed scenario where documents are large files. Our scheme outperforms the most efficient proposals in literature in terms of time complexity by several orders of magnitude.

Cong Wang et al (2012) [7] enables so much advantage of cloud computing, more and more data owners centralize their sensitive data into the cloud. With a mass of data files stored in the cloud server, it is important to provide keyword based search service to data user. However, in order to protect the data privacy, sensitive data is usually encrypted before outsourced to the cloud server, which makes the search technologies on plaintext unusable. In this paper, we propose a semantic multi-keyword ranked search scheme over the encrypted cloud data, which simultaneously meets a set of strict privacy requirements. Firstly, we utilize the "Latent Semantic Analysis" to reveal relationship between terms and documents. The latent semantic analysis takes advantage of implicit higher-order structure in the association of terms with documents ("semantic structure") and adopts a reduced-dimension vector space to represent words and documents. Thus, the relationship between terms is automatically captured. Secondly, our scheme employ secure "k-nearest neighbour (k-NN)" to achieve secure search functionality. The proposed scheme could return not only the exact matching files, but also

the files including the terms latent semantically associated to the query keyword. Finally, the experimental result demonstrates that our method is better than the original MRSE scheme.

Bing Wang et al (2014) [8] proposes Enabling keyword search directly over encrypted data is a desirable technique for effective utilization of encrypted data outsourced to the cloud. Existing solutions provide multi keyword exact search that does not tolerate keyword spelling error, or single keyword fuzzy search that tolerates typos to certain extent. The current fuzzy search schemes rely on building an expanded index that covers possible keyword misspelling, which lead to significantly larger index file size and higher search complexity. In this paper, we propose a novel multi keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. Our proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionary and effectively supports multiple keyword fuzzy search without increasing the index or search complexity. Extensive analysis and experiments on real-world data show that our proposed scheme is secure, efficient and accurate. To the best of our knowledge, this is the first work that achieves multi-keyword fuzzy search over encrypted cloud data.

III. Proposed System

This paper deals with security for the documents that are uploaded and stored on the cloud. This study is by proposing Visual Cryptography Scheme (VCS) technique for securing the files. In order to prevent issues like breaches and malware attacks on cloud, this innovative scheme helps in high level security to safeguard the files that are stored on the cloud.

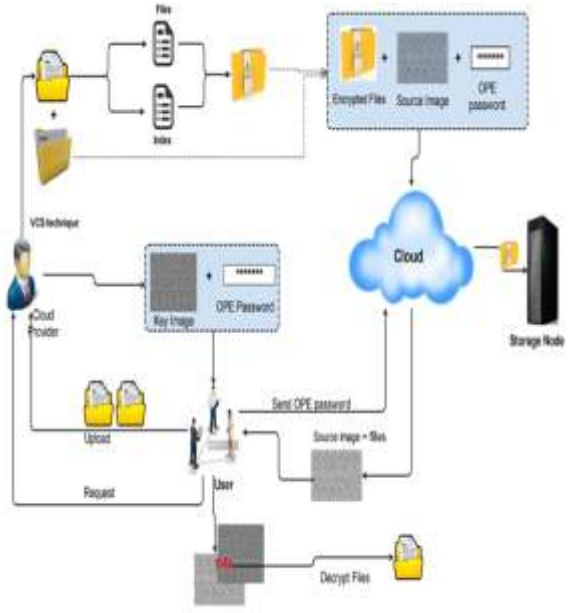


Fig a. System Architecture

In fig a. refers to System Architecture in which the VCS scheme is implemented by sending an image file (source image) along with the document file. When both the source image and key image overlays each other, a key is generated for encrypting the document file. This architecture consist of two phases: uploading phase and retrieval phase. In the uploading phase after the process of visual cryptography scheme, the document file is encrypted using Advanced Encryption Standard (AES). When a document file is uploaded to cloud, an OPE (Order Preserving Encryption) key will be generated by the cloud provider. Then along with the encrypted file, the OPE password and source image is sent to the cloud.

Next part is the retrieval phase in which the user sends the OPE password to the cloud for retrieving files. The cloud verifies by checking the OPE password with the password sent by the user and send the files and the source image if it matches. The source image and the key image overlays with each other, generating the same key used for encryption. Using the key, user can decrypt and download the desired files.

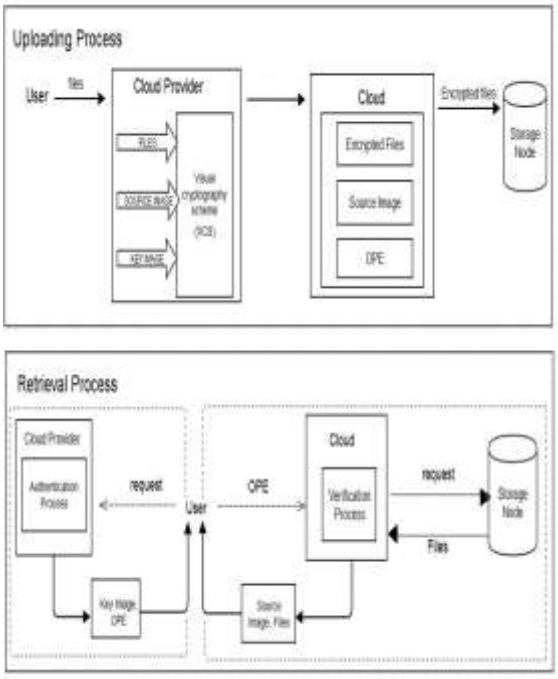


Fig b. Functional Architecture

The functional architecture of the proposed system is given in Fig b. It describes the model that identifies the functions and their interactions for the corresponding system needs. It serves as a bridge between the software engineers and architects and shows the clear view of overall part of the uploading phase and the retrieval phase and the input and output for every model of the project.

Key Generation using VCS

Visual cryptography is a cryptographic technique which allows visual information, pictures, text, etc. to be encrypted in such a way that decryption becomes an automatic operation if the correct key image is used. Visual Cryptography uses two images. One image contains random pixels and the other image contains the secret key. It is impractical to retrieve the secret key from one of the images. Both the images are mandatory to reveal the information. It works when both the images overlays each other

Working of Visual Cryptography

Each pixel of the images is separated into smaller blocks. There are constantly the same number white and black blocks.

If a pixel is separated into two parts, there are one white and one black blocks. If the pixel is separated into four equal parts, there are two white and two black blocks.

One image contains pixels which all have a random state, image 2 is identical to image 1, except for the pixels that should be black (contain key) when overlayed. These pixels have a state that is contrary to the same pixel in image 1. If both images are overlayed, the areas with indistinguishable states will look gray, and the areas with contrary states will be black.

The system of pixel can be applied in different ways.. However, you can also use pixels, separated into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is separated horizontally or vertically. There are many different pixel systems, with better contrast, higher resolution and even with colour pixels.

If the pixel states of image 1 are actually (crypto secure) random, both empty and information pixels of image 2 will also have completely random states. One cannot know if a pixel in image 2 is used to create a grey or black pixel, as the position of that pixel in image 1 (which is random) to know the overlay result. If all requests for exact uncertainty are fulfilled, Visual Cryptography provides accurate secrecy by the Information Theory.

If Visual Cryptography is used for protected interactions, the sender will allocate one random image 1 in progress to the receiver. If the sender has a message, and creates an image 2 for a particular disseminated image 1 and sends it to the receiver. The receiver aligns the two images and the secret key is revealed, without the necessity for an encryption device, The system is indestructible, as long as both images move to unauthorized user. When one of both image is intercepted it's impossible to retrieve the encrypted key.

File Upload with Security

This part deals with the uploading phase on security for the documents that are uploaded and stored on cloud. This is proposed by Visual Cryptography Scheme (VCS) for securing the document files. Files are encrypted using Advanced Encryption Standard (AES). When a document file is uploaded to cloud, an OPE (Order Preserving Encryption) key will be generated by the cloud provider. Then along with the encrypted files, the OPE password and source image is sent to the cloud.

Retrieval of files

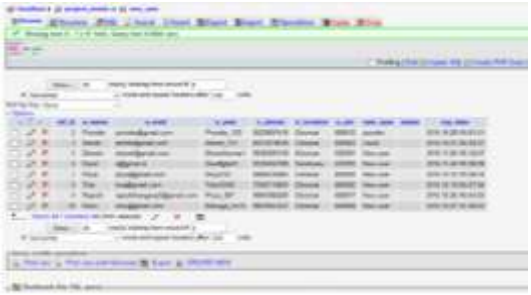
The process of retrieval part is done by the user. The user sends the OPE password to the cloud for retrieving files. The cloud verifies by checking the OPE password with the password sent by the user and sends the files and the source image if it matches. The source image and the key image overlays with each other, generating the same key used for encryption. Using the key, user can decrypt and download the files.

IV. Experimental Result

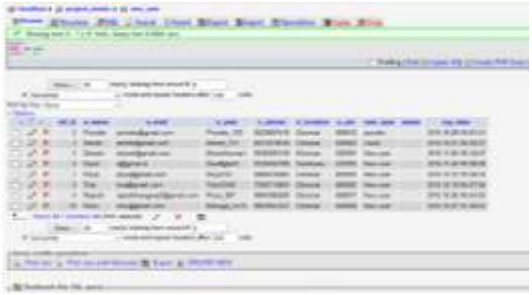
This result analysis involves gathering formal and informal data to facilitate the system define and accomplish their goals. It uncovers numerous perspectives on an issue or prospect determining any drives towards or barriers to successful recital and proposing a resolution system based on what it is revealed.

Data Set

Users:



Files:



Performance and Evaluation:

Characteristics	DES	RC5	3DES	AES with VCS
Block Size(bits)	64	32,64, 128	64	128,192, 256
Attacks: 1.Side channel 2.Brute force	Not solved	Not solved	Not solved	Solved
Security	Proven Inadequate	Considered secure	Considered secure	Considered secure
Speed	Very slow	Slow	Slow	Very Fast

V. Conclusion and Future Work

This paper focuses on security for the documents that are uploaded and stored on cloud. However, it poses risks to consumers unless the data is encrypted for security. This study addresses these issues by proposing Visual Cryptography Scheme (VCS) technique for securing the files. Then the files are encrypted using Advanced Encryption Standard (AES). Then the encrypted files are securely sent to the cloud.

This paper is done for security of files in cloud database. This project can be enhanced with more features in future. But multi security approaching methods can be used in the uploading phase. In future we can implement more advanced encryption techniques for encrypting a particular file.

References

[1] Cao. N, C. Wang, M. Li, K. Ren, and W. Lou, (2011) "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. Int. Conf. Comput. Commun. (INFOCOM), pp. 829–837.

[2] Gentry.C and S. Halevi, (2011) "Implementing gentrys fully- homomorphic encryption scheme," in Advances in Cryptology– EUROCRYPT 2011, pp. 129–148.

[3] Gartner, (2012) "Worldwide traditional pc, tablet, ultramobile and mo- bile phone shipments on pace to grow 7.6 percent in 2014,"

[4] Nyberg .K, (2010)"Fast accumulated hashing," in Proc. Int. Workshop Fast Softw. Encryption (FSE), Feb. 1996, pp. 83–87.

[5] Orencik.C and E. Savas,,(2011)"Efficient and secure ranked multi- keyword search on encrypted cloud data," in Proc. Joint EDBT/ICDT Workshops, pp. 186–195.

[6] L. Vaquero L. Rodero-Merino, J. Caceres, and M. Lindner,(2008) "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55.

[7] Wang, N. Cao, K. Ren, and W. Lou,(2011)"Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Systems, vol. 23, no. 8, pp. 1467–1479

[8] Wang.C , N. Cao, J. Li, K. Ren, and W. Lou,(2011)"Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS),pp. 253–262.

[9] C. Gentry, (2009) "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University,

[10] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan,(2010) "Fully homomorphic encryption over the integers," in Advances in Cryptology-EUROCRYPT, pp. 24–43.

[11] D. Stehl´e and R. Steinfeld, (2010), "Faster fully homomorphic encryp- tion," in Advances in Cryptology-ASIACRYPT, pp. 377– 394.

[12] R. Chen, A. Reznichenko, P. Francis, and J. Gehrke, (2012) "Towards statistical queries over distributed private user data," in USENIX Symp. Netw. Syst. Des. Implementation (NSDI), vol. 12, pp. 13–13.

[13] D. X. Song, D. Wagner, and A. Perrig, May (2000) "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Priv. (SSP), , pp. 44–55.

[14] E.-J. Goh et al., "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[15] Y.-C. Chang and M. Mitzenmacher, Jun. (2005) "Privacy preserving keyword searches on remote encrypted data," in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS), pp. 442–455.

[16] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, Oct. (2006) "Searchable symmetric encryption: improved definitions and efficient con- structions," in Proc. ACM Conf. Comput. Commun. Secur. (CCS) pp. 79–88.

[17] S. Zerr, E. Demidova, D. Olmedilla, W. Nejdl, M. Winslett, and S. Mitra, Mar. (2008) "Zerber: r-confidential indexing for distributed docu- ments," in Proc. Int. Conf. Extending Database Technol. (EDBT), pp. 287–298.

[18] K. D. Bowers, A. Juels, and A. Oprea, Dec. (2009) "Hail: a high-availability and integrity layer for cloud storage," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), pp. 187–198.

[19] J. Li, R. Ma, and H. Guan, Feb. (2015) "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Trans. Cloud Comput.

[20] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Jan. (2014). "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Systems, vol. 25, no. 1, pp. 222–233.