International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 7, Issue 7, July2018, pp.701-704, ISSN 2278 -1412

Security Enhancement in Cloud Environment Using Identity Based Encryption and Hyper Chaotic Searchable Image Encryption

Shruti Kirti Dixit [1], Dr. Tripti Arjariya[2]
[1]*M.Tech Scholar, Department of Computer Science Engineering, Bhabha Engineering Research Institute Bhopal shaludixit4@gmail.com, India;*
[2,] *HOD, Department of Computer Science Engineering, Bhabha Engineering Research Institute Bhopal, tripti.beri@gmail.com, India;*

Abstract *– In our scheme, as with the suggestion, we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. Furthermore, we consider realizing revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model.*

Keywords*: IBE, HCIE, Cloud computing, PKG, KU-CSP*

I. Introduction

With the advancement of information and computing technology, large-scale datasets are being exponentially generated today. Examples under various application contexts include medical images, remote sensing images, satellite image databases, etc. Along with such data explosion is the fast-growing trend to outsource the image management systems to cloud and leverage its economic yet abundant computing resources too efficiently and effectively acquire, store, and share images from data owners to a large number of data users. Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys.

Cloud computing is an emerging computing paradigm in which IT resources and capacities are provided as services over the Internet while hiding platform and implementation details. Promising as it is, this paradigm also brings forth new challenges for data security and privacy when users outsource sensitive data for sharing on cloud servers, which are likely outside of the same trusted domain of data owners.

Many people are confused about what cloud computing is, especially as the term is overused. Roughly, it describes highly scalable resources provided as an external service via the Internet on a pay per use basis. Cloud computing can be defined as a specialized distributed computing model, which is dynamically configured and delivered on demand. This new massively scalable paradigm is different from traditional networks. It is highly abstract to deliver three levels of services.

II. Hyper Chaotic Searchable Image Encryption (HCIE)

In the proposed scheme, an image owner having a low computational power (e.g., mobile devices) connects to the cloud. The user desires to use the storage capacity and cloud computational power. She/he stores the images securely and wants to retrieve or access them afterwards. The image owner has a collection of his sensitive images. However, the image owner wants that his collection must be secure enough before outsourcing to the cloud for further processing. Figure 1 shows the System framework of proposed algorithm. In this figure only encryption algorithm has been explored. User authentication using image captcha is explored in section while reusing the system framework of Figure 1. The security enhancing process which performs in image owner's machine uses images obtained from social media

sites such as flicker to create masks for the original image with a lightweight encryption algorithm to further enhance the security of the image. The identity of the masks called flk_ID and the keys which are used for encryption process are kept secret. The image owner creates the key matrix of the keys used for encryption and ID of the masks. Then the key matrix encryption is performed by the image owner. In key encryption λ-values and λ-vector are created with a secret index of the image. More about λ-values and λ-vector is explained in section. Here in this section λ-values and λ-vector are created. After encrypting the image and keys, image owner sends the encrypted image to the cloud for storage with the λ-values and secret index and λ-vectors are sent to the authorized cloud user. When a cloud user wants to retrieve the image, it sends the request to the cloud. For sending the request he/she extracts the keys and creates the index for searching the remotely stored image collection, and then sends the index to the cloud server. The cloud performs the requested computation on the encrypted images and returns the results in the encoded forms to the image owner. The image owner decodes the received results to get the images on which the requested computations are done by the cloud.

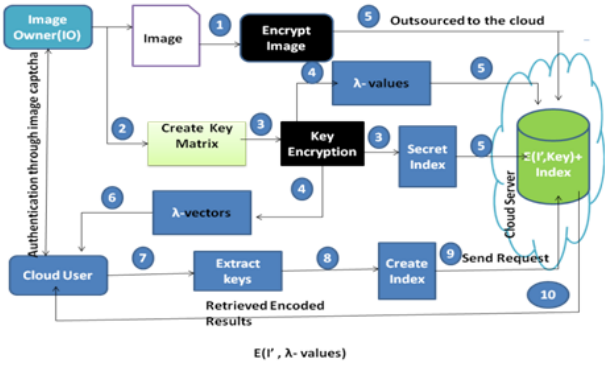

Fig.1 System framework

III. Proposed Methodology

In this proposed work, introduce outsourcing computation into IBE (Identity Based Encryption) revocation, and formalize the security definition of outsourced revocable IBE (Identity Based Encryption) for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of simple operations for PKG and eligible users to perform locally.

In our scheme, as with the suggestion, we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component.

At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decrypt ability, unrevoked users needs to periodically request on key update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).

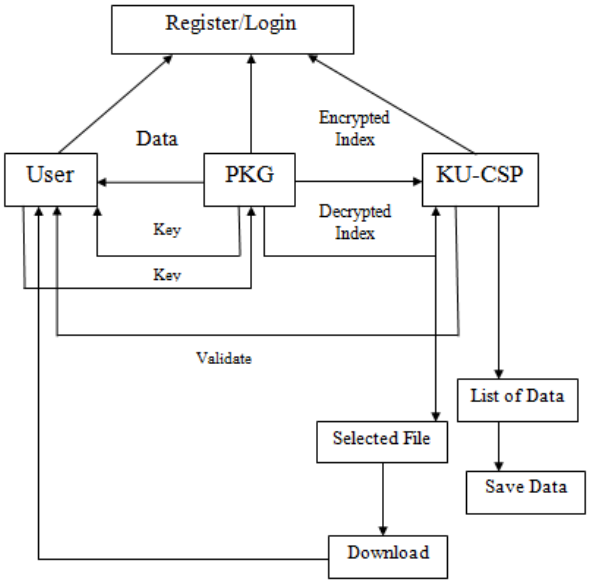

Fig.2 Flow diagram of proposed system

IV. Simulation Results

In this proposed work realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires re-issuing the whole private key for unrevoked users.

Fig.3 user login page

Fig.3 shows the User login page. In this panel enter the username and password. Here user can login with registered username and password. Only registered users can login inside panel.

Fig.4 user home page

Fig.4 shows the user home page. After enter the login details then opens the user home. In this panel three menu are shows upload, file view and logout.

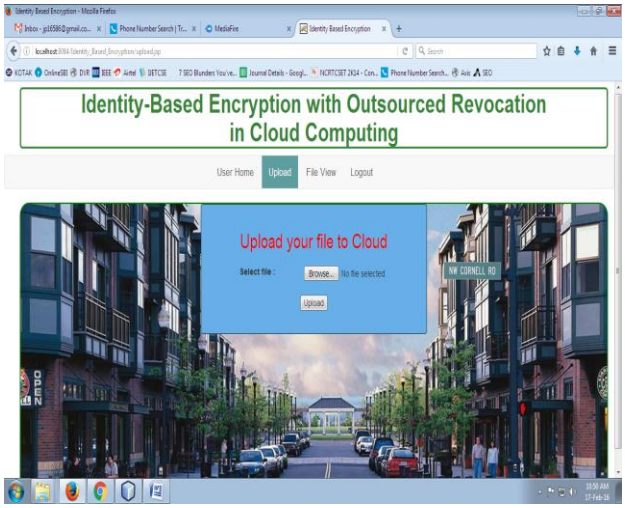

Fig.5 uploads data in cloud server

Fig.5 shows the upload data in cloud server. In this we upload the any data file upload in cloud server.

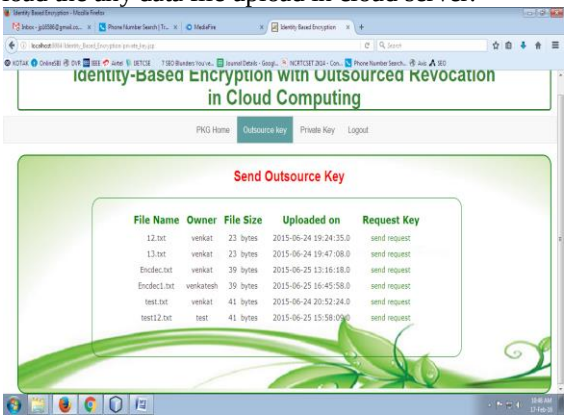

Fig.6 Send outsource key panel

Fig.6 shows send outsource key panel. PKG will send the outsourced key to CSP.

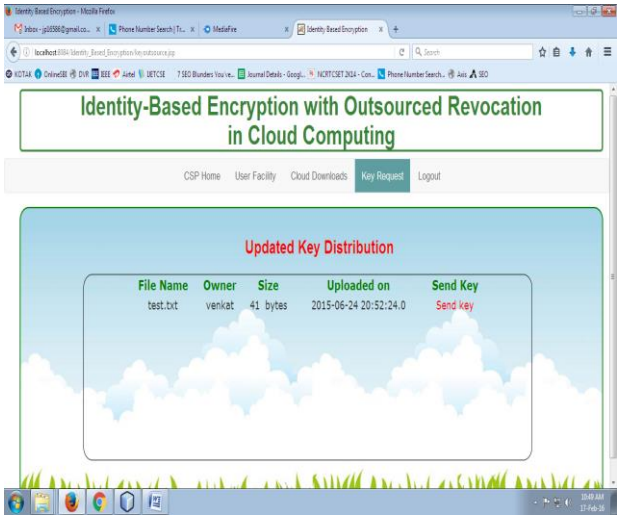

Fig.7 Update key Distribution

Fig.7 based on the trigger the CSP will receive the outsourced key from PKG then CSP sends the updated key to the users' registered mail id.

Fig.8 Cloud download panel

Fig.8 shows download data in cloud server. After enter the provide key then shows the download view in the cloud server.

V. Conclusion

It In this research work, propose a revocable scheme in which the revocation operations are delegated to Cloud Service Provider. With the aid of key update Cloud Service Provider, the proposed scheme is full-featured: It achieves constant efficiency for both computation at private key generate and private key size at user; User needs not to contact with private key generate during key update, in other words, private key generate is allowed to be offline after sending the revocation list to key update Cloud Service Provider; No secure channel or user authentication is required during key-update between

user and key update Cloud Service Provider. Cloud servers cannot learn anything about the customer image because only the encoded images are stored on the server. It allows searching to take place within the cloud servers where they learn nothing more than the searching result about the image information..

References

[1] Li, Jin, et al. "Identity-based encryption with outsourced revocation in cloud computing." Ieee Transactions on computers 64.2 (2015): 425-437.

[2] Wang, Cong, et al. "Privacy-assured outsourcing of image reconstruction service in cloud." IEEE Transactions on Emerging Topics in Computing 1.1 (2013): 166-177.

[3] Li, Jin, et al. "Fine-grained access control system based on outsourced attribute-based encryption." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2013.

[4] Li, Jingwei, et al. "Outsourcing encryption of attribute-based encryption with mapreduce." International Conference on Information and Communications Security. Springer, Berlin, Heidelberg, 2012.

[5] Benjamin, David, and Mikhail J. Atallah. "Private and cheating-free outsourcing of algebraic computations." Privacy, Security and Trust, 2008. PST'08. Sixth Annual Conference on. IEEE, 2008.

[6] Wang, Cong, Kui Ren, and Jia Wang. "Secure and practical outsourcing of linear programming in cloud computing." INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[7] Zhou, Zhibin, and Dijiang Huang. "Efficient and secure data storage operations for mobile cloud computing." Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, 2012.

[8] Green, Matthew, Susan Hohenberger, and Brent Waters. "Outsourcing the decryption of abe ciphertexts." USENIX Security Symposium. Vol. 2011. No. 3. 2011.

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography TCC'05), 2005, pp. 264–282.

[10] Thilakanathan, Danan, et al. "Secure data sharing in the Cloud." Security, Privacy and Trust in Cloud Systems. Springer, Berlin, Heidelberg, 2014. 45-72..