International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 8146-8150
© Research India Publications. http://www.ripublication.com

Secure Storage of Images in cloud using Dual Public Key Cryptography and Blocker Protocol

S.Libi Farrell[1,*], Dr. J.Arokia Renjith[2]

[1]Student, M.E.Computer Science and Engineering, Jeppiaar Engineering College, Chennai, India.

[2]Professor/HOD, Computer Science and Engineering, Jeppiaar Engineering College, Chennai, India.

Abstract

In the medical cloud computing, the hospital administrator encrypt the images before outsourcing it in to the cloud server. In this case, only authorized doctors are allowed to access the images since the medical images are highly confidential. Encrypting the images before outsourcing is a commonly used approach, where the patient only needs to send the corresponding encryption key to the authorized doctors. This, however, significantly limits the confidentiality of the images. In this paper, we propose two Secure and Efficient Encryption schemes over medical images. Firstly, we leverage the Elgamal and Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) encryption techniques to propose a double encryption, which can achieve secure storage of images in the cloud. Secondly, we propose an enhanced scheme to provide security by providing Schnorr Protocol in order to achieve Proof of Knowledge. Compared with existing proposals, our schemes are better in terms of security. Then, we propose an enhanced scheme to provide Blocker Protocol, to know who is retrieving the image from the cloud server.

Keywords: Elgamal Encryption, Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) Encryption, Schnorr Protocol, Blocker Protocol.

INTRODUCTION

Health Care is the maintenance of the condition to act in anticipation of ailments, the recognition of the nature of an illness by examination of the symptoms and other medical ailments. Health Care is achieved by health practitioners. Health Care can vary across countries, communities and individuals which are identified by many conditions. It is a computing technique that enables security, confidentiality and Integrity. Radiologists can remotely store images on the cloud server and then open the images by the Doctor with the help of Patient's Id. The medical images are sensitive Images, it is necessary to encrypt the medical Images before it is updated to the cloud. Since, the encrypted Images take large time to retrieve; we use Elgamal Encryption to achieve easy retrieval of Images and to provide Confidentiality. Since, the cloud is not an trusted authority, we use Rivest-Shamir-Adleman (RSA) Encryption in the cloud.In our scheme, we propose Schnorr Protocol to enjoin static and dynamic question; in order to achieve security, confidentiality and Integrity. Static Question made up of standard questions. Dynamic question made up of questions which often get changed. In our scheme, we propose Blocker Protocol in order to know who (Doctor) is retrieving the images which are updated by the Radiologists. Further, the Performance is analyzed. Recently, searchable symmetric encryption and Attribute-Based Hybrid Encryption has been proposed to search over encrypted images. However, in such schemes, it takes heavy arithmetic operations to retrieve the Images. On the other hand, there is a chance of adaptive attackers (Brute Force attack) to retrieve the Images by guessing. However, these approaches significantly increase the complexity in storage, search and updating processes. To address the above issues, in this paper, We propose the Elgamal Encryption and Rivest-Shamir-Adleman (RSA) Encryption scheme over medical cloud Images. This work extends and improves our previous investigation. The original contributions of the paper are:Firstly, we deploy the Elgamal Encryption, it depends on two factors: Firstly, Security depends on the large Integers. Secondly, Security depends on the discrete logs. Each time at the time of encryption, the plaintext gives a different ciphertext.

SCOPE OF THE PAPER

Cloud Computing is the process of computing and storing images as a service to a community of. The name comes from the use of storing of large amount of images in the cloud. Cloud computing entrusts services with a user's images, software and computation over a network. Public clouds are made available to the public by a provider who hosts the own cloud. Private cloud is provided to a particular organization. Hybrid clouds are the composition of two or more clouds that remains unique, With this process, the suggestion is that it specifics how the end purposes of a system are associated with security, confidentiality and integrity. Cloud computing provides images from processing to give measure to the organization. Moreover, computing performs autonomic processing, enabling organizations to provide and to perform security.

LITERATURE SURVEY

HeleiCui[1] proposed deals with exploiting and uniquely bringing together techniques from data encryption, searchable encryption, Image Processing are used in the proposed scheme has salient properties of user access privilege confidentiality and user secret key accountability.

RongMaoChen[2] the issues for the encryption of data using Keyword Guesssing attack (KGA) which is an inherent vulnerability of the traditional PEKS framework.

JieXu [3] proposed the design of a circuit cipher text policy attribute based hybrid encryption with verifiable delegation scheme in order to secure the system using attributes.

Sheren A.EL Booz[4] proposed a new Scheme for the authentication level of security by using two authentication techniques Time Based One Time password(TOTP) for cloud user's verification and Automatic Blocker Protocol(ABP) to fully protect the system from unauthorized cloud users the experimental results demonstrate the effectiveness and efficiency of the proposed system when auditing shared data integrity.

Joseph K.Liu [5] proposed a 2FA access control system, especially for web–based cloud services in addition attribute–based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy.

Zhirong Shen[6] proposed a design to enhance the privacy KSAC also plants noises in the query to hide user access privilege intensive evaluations on real-world dataset are conducted to validate the applicability of the protection for user's privilege.

Zhijie Wang [7] proposed CCP-CABE achieves the efficiency because it generates constant-size keys and cipher text regardless of the number of involved attributes and it also keeps the computation cost constant on lightweight devices.

Taeho Jung[8] proposed semi anonymous privilege control scheme access control to address not only the data privacy ,but also the user identity privacy in existing access control schemes access control decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity Subsequently we present the access control which fully prevents the identity leakage and achieve the Full anonymity.

Shaohua Tang [9] proposed the hierarchical Key assignment Scheme based on linear –geometry as the solution of flexible and fine-grained hierarchical access control in cloud computing the simulation shows that our scheme has an optimized trade-off between computation consumption and storage space.

Yifeng Zheng[10] proposed encrypted cloud media center hosting encrypted images we have provided thorough security analysis to show the security strengths of our system design our implementations have adopted a format-compliant SVC encryption strategy and optimized the storage of encrypted images for efficient design.

PROPOSED SYSTEM

Present system achieves goal by exploiting and uniquely combining techniques of Dual Public Key Encryption (DPKE) and Automatic Blocker Protocol (ABP). Present System shows secure cloud storage architecture that allows an organization to store image securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud.In DPKE, enables a user to search encrypted image in the asymmetric encryption setting, associated with pixels for each of which a public key component is defined. The encrypted associates the set of attributes to the message by encrypting it with the corresponding public key components.Based on the proposed DPKE scheme, the owner encrypts the images and features with public key encryption, which will be appropriately selected with regard to functionality and efficiency. To avoid the interaction with the owner for content access while still enforcing access control, we apply Proxy re-encryption (PRE) to allow for the access control managed by the cloud but without granting the decryptions rights to the cloud. ABP ensures the information about the cloud user to the image owner by sending one time password (OTP).The technology used in this system is DPKE (Dual Public Key Encryption). In the proposed system, the image owner first LSH keys (Locality Sensitive Hashing) 'v' for each feature for each LSH key it generates two secure digests h1 and h2, where h1 is used to generate the key and the h2 is used for encryption. The Images together with features are encrypted with the PKE Scheme by using the cloud key. At last the encrypted image is uploaded to cloud for secure services. This system assures the secrecy of the image and preserves the privacy of users from the cloud server while entrusting most of the access control enforcement to the cloud servers.

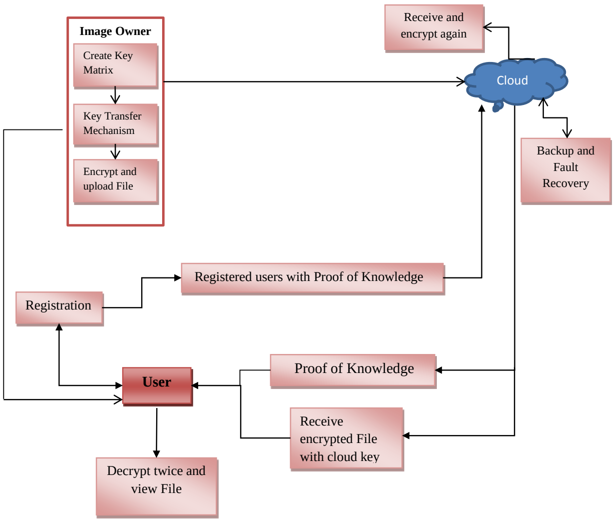
Image Owner
Create Key Matrix
Key Transfer Mechanism
Encrypt and upload File
Receive and encrypt again
Cloud
Backup and Fault Recovery
Registered users with Proof of Knowledge
Registration
User
Proof of Knowledge
Receive encrypted File with cloud key
Decrypt twice and view File

Figure 1. Basic structure of the system

SCHNORR PROTOCOL

The protocol is defined for a cyclic group S_p of order p with generator s.In order to prove Proof of Knowledge, $y = \log_m z$, the sender interacts with the verifier as follows:

1. The first round the sender commits himself to randomness r; therefore the first message $r = s^t$ power r is also called commitment.

2. The verifier replies with a challenge e chosen at random.
3. After generating e , the sender sends the third and last message(the response) $s = t + ey$.
4. The verifier accepts, if $s^8 = ry^e$.

BLOCKER PROTOCOL

The Time-Based One-Time Password Algorithm(TOTP) is an algorithm that computes a one-time password from a shared secret Key at the current time.User enters Username and Password into a website, it generates a one –time password to the user using TOTP running locally on a smartphones.If the OTP is matched, then the server will send the message to the owner whether to accept or reject, if the owner accepts, then the image will be viewed by the cloud users. If the owner rejects, then the image cannot be viewed by the cloud users. The theorem can be proved by using the formula,

$$B^1 = B$$

$$B^1 = aC \bmod pq$$

$$C = \prod_{K=1}^{C} P_e Q_{f_g} \bmod h$$

$$= \prod_{k=1}^{c} (Q_g M \bmod h)$$

$$= \sum_{k=1}^{c} Q_g h_{f_g} \bmod h$$

DUAL PUBLIC KEY CRYPTOGRAPHY

$E1()$ and $E2()$ be the two encryption functions , and $"M"$ be the key, If A encrypts it using $E1()$ and sends $E1(M)$ to B. B encrypts the image as $E2(E1(M))$ and sends it to A. A decrypts $E2(E1(M))$ using $E1()$.A receives $E2(M)$, meaning when she sends to B, he will be able to decrypt the image using $E2()$ and receives $"M"$.

Elgamal Encryption :

Elgamal encryption algorithm depends on large integers and discrete logs. Each time at the time of encryption, the plaintext gives a different cipher text. A reckons (i) A large prime M_A. (ii) A element $\gamma_A \bmod M_A$. (iii) A integer $I_A, I_A \le M_A$. (iv) $\alpha_A = \gamma_A{}^{I_A} (\bmod M_A)$. Alice's Public key is $(M_A, \gamma_A, \alpha_A)$. Her private Key is I_A. B encrypts a image $E(E \le M_A)$ and sends it to Alice. B receives a random integer r. B reckons $\eta = \gamma_A{}^r (\bmod M_A)$ and $s = \alpha_A{}^r E(\bmod M_A)$, and then get rid of r then sends the encrypted Image (n,s) to B. When B receives the encrypted image (n,s), B decrypts (using private Key I_A) by calculating $s_n{}^{-I_A}$.

$$S_n{}^{-I_A} = \alpha_A{}^r E(\gamma_A{}^r)^{-I_A}$$

$$= (\gamma_A{}^{I_A})^r E(\gamma_A{}^r)^{-I_A}$$

$$= E$$

RSA Encryption:

The Keys of the RSA Algorithm are generated as: (i) Choose two different prime numbers r and s . (ii) Compute $\omega = rs$.(iii) Compute $\omega(n) = lcm(\omega(r), \omega(l)) = lcm(r-1, s-1)$. r and s: the primes from the key generation, $p_r = p(\bmod r-1), p_s = p(\bmod s-1)$ and s_{inv} can be taken as $s_{inv} = s^{-1}(\bmod r)$. These values compute the exponentiation of $n = i^j (\bmod rs), n_1 = i^{j_r} (\bmod r), n_2 = i^{j_s} (\bmod s)$. Compute $K = s_{inv}(n_1 - n_2)(\bmod r)$. If $n_1 \le n_2$ then, it can be taken as $s_{inv}[(n_1 + [\frac{s}{r}]r) - n_2]$ $(\bmod r)$, then the value of n can be written as $n = n_2 + ks.$

Modules

Image Owner: The module consists of storing of images in to the cloud server by encryption technique setup with the proposed system(Dual Public Key Encryption(DPKE)) by generating Key matrix m Key Transfer Mechanism is generated after the Image owner creates the Key Matrix by DPKE, and then the key k is given to the Image Owner.

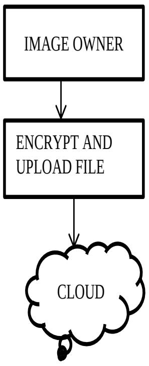

Figure 2. Image Owner

Cloud Server: The cloud server again encrypts the image using Proxy Re-encryption which compresses the image and the actual image gets stored in the cloud server.

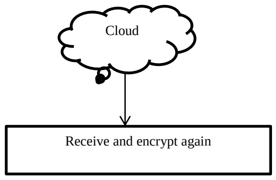

Figure 3. Cloud Server

Cloud Administrator: If there is any Issue in the Key generation between the cloud server and cloud users, the cloud Administrator will perform the Back up and Fault Recovery in order to generate the key.

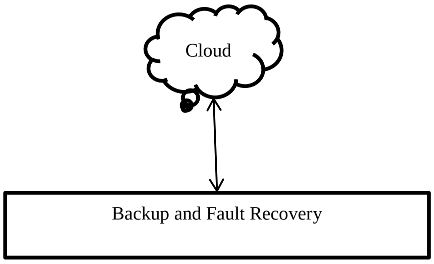

Figure 4. Cloud Administrator

Cloud User: In this module, the Cloud users will retrieve the Image from the cloud user by receiving encrypted file and decrypt twice and view the file.

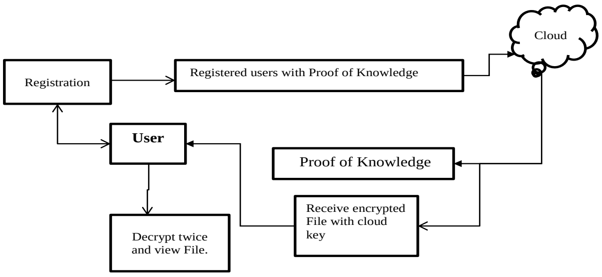
Cloud
Registration
Registered users with Proof of Knowledge
User
Proof of Knowledge
Receive encrypted File with cloud key
Decrypt twice and view File.

Figure 5. Cloud User

RESULT ANALYSIS

CloudSim is a structure for displaying and reproduction of registering frameworks and administrations. Initially, CloudSim constructed basically at the Cloud Computing and Distributed Systems (CLOUDS) Laboratory in the University of Melbourne Australia. CloudSim has turned out to be a standout amongst the most prevalent open source cloud test systems in the exploration and the scholarly world. CloudSim is totally composed in Java. At first created as a solitary cloud test system, CloudSim has additionally been reached out by free scientists. CloudSim is demonstrated by a case study involving dynamic provisioning of application services in the hybrid federated clouds environment. The result of this case study proves that the federated Cloud computing model significantly improves the application QOS requirements under fluctuating resource and service demand patterns. The CloudSim simulation layer provides support for modeling and simulation of virtualized Cloud-based data center environments including dedicated management interfaces for VMs, memory, storage, and bandwidth. The fundamental issues, such as provisioning of hosts to VMs, managing application execution, and monitoring dynamic system state, are handled by this layer. A Cloud provider, who wants to study the efficiency of different policies in allocating its hosts to VMs (VM provisioning), would need to implement his strategies at this layer. Such implementation can be done by programmatically extending the core VM provisioning functionality. There is a clear distinction at this layer related to provisioning of hosts to VMs. A Cloud host can be concurrently allocated to a set of VMs that execute applications based on SAAS provider's defined QOS levels. This layer also exposes the functionalities that a Cloud application developer can extend to perform complex workload profiling and application performance study. The top-most layer in the CloudSim stack is the User Code that exposes basic entities for hosts (number of machines, their specification, and so on), applications (number of tasks and their requirements), VMs, number of users and their application types and broker scheduling policies. By extending the basic entities given at this layer, a Cloud application developer can perform the following activities:1) Generate a mix of workload request distributions and application configurations.2) Cloud availability scenarios and perform robust tests based on the custom configurations.3)Implement custom application provisioning techniques for clouds and their federation.

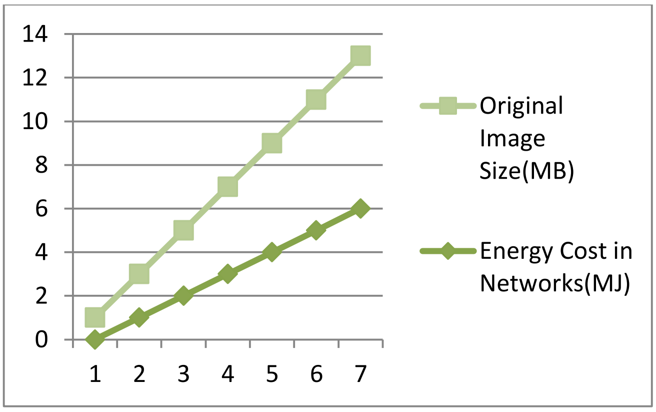

Figure 6. Performance Graph

In the above graph, Energy Cost in Networks is taken in 'Y' axis, and Original Image Size is taken along 'X' axis. In the above graph, uploading a small size image digest t (e.g., 97.7 KB) saves energy from 1.5 times to over 5 times in term of Joule than uploading the original big size image. Even though we introduce additional computations at the network, e.g., generating secure digest and estimating H, the overall energy cost still has an advantage. We know that the Correlation estimation may be processed multiple times, depending on the number of clients. However, even running 10 times over a small group of clients, the energy cost is still much lower than original data transmission. There are two keys p and q, By using the formula n=p q, we can show that energy cost has become low.

CONCLUSION

The proposed system present system achieves goal by exploiting and uniquely combining techniques of Dual Public Key Encryption (DPKE) and Blocker Protocol. Present System shows secure Dual Public Key Encryption storage Architecture that allows an organization to store Image securely in a cloud, while maintaining the sensitive information related to the organization. In DPKE, images are associated with pixels for each of which a key is defined. In the proposed system, the image owner first LSH keys (Locality Sensitive Hashing). For each feature LSH key it generates two secure keys h1 and h2, where h1 is used to generate the key and the h2 is used for encryption. The Images together with features are encrypted with the PKE Scheme by using the cloud key. At last the encrypted image is uploaded to cloud for secure services. This system assures the secrecy of the image and preserves the privacy of users from the cloud server while entrusting most of the access control enforcement to the cloud servers. The system ensures the Performance improvement in the energy cost. The energy cost has become lower.

REFERENCES

[1] Helen Cui. , Xingliang Yuan, Cong Wang, ”Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing, ”IEEE TRANSACTIONS ON MOBILE COMPUTING., January 2016.

[2] Rongmao Chen, Yi Mu, Guomin Yang, Funchun Guo and Xiaofen Wang,” Dual Server public key Encryption with Keyword Search for Secure Cloud Storage,”IEEE TRANSACTIONS ON INFORMATION FORENSICS SECURITY., December 2015.

[3] Jie Xu, Qiaoyan Wen, Wenmin Li and Zhengping Jin,” Circuit Cipher text-policy Attribute-Based Encryption with verifiable Delegation in Cloud Computing, ”IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS., April 2015.

[4] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, ”A secure Cloud Storage System Combining Time-Based One Time Password and Automatic Blocker Protocol,” JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING.

[5] Joseph K. Liu,Man Ho Au,Xinyi Huang, Rongxing Lu, Jin Li, ”Fine Grained Two-factor Access Control for Web-based Cloud Computing Services, ”IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY., March 2015.

[6] Zhirong Shen, Jiwu Shu and Wei Xue, ”Keyword Search with Access Control over Encrypted Cloud Data,” IEEE SENSORS JOURNAL.,Vol.18,no.4,pp.255-258, April 2016.

[7] Zhijie Wang, Dijiang Huang, Yan Zhu, Bang Li, and Chun-Jen Chung,” Efficient Attribute –Based Comparable Data Access Control,”IEEE TRANSACTIONS ON COMPUTERS,”Vol.17,March 2015.

[8] Taeho Jung, Xiang-Yang Li, Zhiguo Wan and Meng Wan, ”Control Cloud Data Access Privilege and Anonymity with fully Anonymous Attribute-Based Encryption, ”IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, ”Vol.10,January 2015.

[9] Shaohua Tang, Xiaoyu Li, Xinyi Huang, Yang Xiang, Lingling Xu, ”Achieving Simple, Simple, Secure and Efficient Hierarchical Access Control in Cloud Computing, ”IEEE TRANSACTIONS ON COMPUTERS,”, September 2015.

[10] Yifeng Zheng, Xingliang Yuan, Jinghua Jiang, Cong Wang, and Xiaolin Gui,” Towards Encrypted Cloud Media Center with Secure Deduplication, ”IEEE TRANSACTIONS ON MULTIMEDIA, ”January 2016.

[11] Sikhar Patranabis, Yash Shrivastava and Debdeep Mukhopadhyay, ”Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on Cloud, ”IEEE TRANSACTIONS ON COMPUTERS, ”March 2016.

[12] Meng Shen, Mingwei Wei, Liehuang Zhu, Mingzhong Wang, ”Classification of Encrypted Traffic with Second-order Markov Chains and Application Attribute Bigrams, ”IEEE TRANACTIONS ON INFORMATION FORENSICS AND SECURITY, ”January 2016.

[13] Song Han, Shuai Zhao, Qinghua Li, Chun-Hua Ju and Wanlei Zhou, ”PPM-HDA:Privacy-Preserving and multifunctional health Data aggregation with Fault Tolerance, ”IEEE TRANSACTIONS ON FORENSICS AND SECURITY, ”April 2015.

[14] Kun-Lin Tsai, Fang-Yei Leu, Yi-Fung Huang, Chi Yang,Cheng-Hsin Chang, King-Shing Yip, Yuchen Xue, Guan-Chi Lai, ”Cloud Encryption Using Environmental Keys, ”International Conference on Innovative Mobile and Internet Services In Ubiquitous Computing, ”March 2016.

[15] Bhushan Sakate, Harshal Patil, Rohit Rakshe, ”Separate Reversible Encrypted Data Hiding in Encrypted Image Using AES Algorithm, ”International Journal of Advanced Research in Computer Science and Software Engineering.