ImagedIt - A Secure Cloud Application

Sanket Mantri 1, Dhiraj Gupta 2, Pravin Shendkar 3, Abhishek Dubey 4
Prof. Mahendra Pawar 5 & Prof. Vinod Alone 6.
1,2,3,4B.E. Student, 5,6Assistant Professor
1,2,3,4,5,6Department of Computer Engineering.
Padmabhushan Vasantadada Patil Pratishthan’s College Of Engineering, Sion, Mumbai – 400022.

Abstract— Cloud computing has gained a lot of hype in the current world of I.T. Cloud computing is a big thing in the computing world after the internet. Cloud computing is used for the tasks performed on the computer over the internet and is visualized as the next-generation architecture of IT Enterprise. The ‘Cloud’ can be accessed through the internet. It is related to several technologies and the convergence of these various technologies has made it to be called as Cloud Computing. ImagedIt is an image storage service which enables user cloud storage, file sharing and collaborative editing. In this application, we focus on secure data storage in cloud. Quality of Service is an important aspect of Cloud Computing. To ensure the user’s data is intact i.e. checking correctness in the cloud a new simple and fast algorithm for image encryption is proposed. This scheme achieves data storage, correctness and allows the authenticated user to access his/her data.

Keywords - Cloud Computing, Security, Imagedit.

I. INTRODUCTION

The cloud is inescapable. Headlines catalogue every advance and setback in the “as a service” paradigm with equality in all aspects. Providers proclaim the model as a solution for every as well as any painful budget cut and desperate business need. And IT professionals struggle to come up with a cloud strategy that will not only help their business whip expenses and also support the form of operational agility their enterprise needs to get ahead in the marketplace.

Other security issues faced by cloud computing include sensitive data access, data segregation, privacy, authentication and policy integration, identity management, accountability, bug exploitation, recovery, visibility under virtualization, management console security, account control, and multi-tenancy issues.

We have made an online Image Editor called “Imagedit” that is deployed in a virtualized environment. The application provides universal access to an online editor that can store a huge amount of images on the cloud server after editing or even simply.

The purpose of creating such an editor lies in the fact that such an application is not currently available on any cloud setup. Using ImagedIt, users can store sensitive data that could be financial or medical documents (images) in an encrypted format online. This is users a sense of security and privacy since data is secured on the server and several measures including authentication and OTP make it tough for an intruder to access others data.

II. BACKGROUND

Cloud computing means to access the resources and services needed to perform tasks with dynamically changing needs. A cloud provides a cloud service user (CSU) that provides privilege of access to an application “as a service” provided by Cloud Security Provider (CSP). Depending upon the type of cloud and its deployment model, the CSUs are guaranteed having more or less control to the connected computing resources.

Other security issues faced by cloud computing include sensitive data segregation, data access, privacy, bug exploitation, authentication and identity management, policy integration, malicious insiders, accountability, recovery, visibility under virtualization, management console security, account control, and multi-tenancy issues.

In this paper we want to design such an editor lies in the fact that such an application is not currently available on any cloud setup. Using ImagedIt, users
III. RECENT SCENARIO

In 2011, Pradeep Tiwari et al. [2] discuss several utility and their applications. They provide a broad discussion which is useful for cloud computing research. Cloud Architecture provides services via internet (WWW) services. On demand on the basis of user requirement the application design in cloud computing environment or the applications which support cloud paradigm are on demand.

IV. PROBLEM DOMAIN

Security is an important issue in cloud environments and must be ensured to encourage more users to use cloud and the numerous benefits that come with it. Data security and storage forms one of the main aspects of security since users revert to a cloud to store large amounts of sensitive data on cloud. Our cloud application, Imagedit, provides data security by encrypting images based on an innovative algorithm.

In today’s world of social networks users have always felt a pressing need to edit and access images anytime and anywhere. There are a range of effects required by the common users for their images and these images are used in many user applications. Also, there is always a security issue related to the authentication of the users. The users must be able to access the data on the cloud only if they are authenticated. Also the database must be made secure enough so that even if an unauthorized user gains access to the data on the cloud the data is not compromised.

In 2010, Zhidong Shen et al. [3] proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. They propose a model system in which cloud computing system is combined with trusted computing platform with trusted platform module. In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

In 2011, Pritesh Jain et al. [5] survey several aspects of cloud computing security concerns. They concern on the major challenges that faces the cloud computing is how to secure and protect the data and processes the data of the user. To provide secure and reliable services in cloud computing environment is an important issue. One of the security issues is how to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in this environment.

V. PROPOSED APPROACH

To address the security issues related to cloud rose till date we have attempted to create an application on the cloud and provided additional security features to it. The application is an online image editing website that enables user to upload pictures through their own account and edit them. The users can select from a range of effects available. The effects can be applied as per the needs of the user. The user can create an altogether new and better looking picture and enhance the quality of his images. The edited pictures are then stored in the user’s account on the cloud. This stands as an advantage for the users who wish to access their images from elsewhere as the images are now on cloud and can be viewed, edited and re-edited anywhere and anytime. These pictures can be also shared by the user with his friends. Again these friends have an authentication code. Only the authorized friends can access the image. Each user has his folder on the cloud and the images are stored in it. The folder name, its contents, names and paths are also encrypted. All the user details are stored in an encrypted manner.

With the noteworthy advance in image analysis visual sensing and techniques, image data are used in many sensitive applications. Image Encryption makes full use of the scan patterns and function XOR in three standalone steps. We encrypt the images by dividing them into blocks of 8x8. These images are then shuffled by using scan patterns. The scan patterns basically access different blocks in different orders instead of the normal linear access. There are 8 scan patterns and they are applied on the image based on a key differently. A different scan pattern is there for every user so that there is enhanced encryption.

We try to create chaos in the image for better security. This image after applying chaos based encryption is then subjected to XOR by using a different image. The image obtained after XOR is then stored on the cloud. The XOR image is totally
distorted and vague such that it is difficult to make out what image it is.

When the user wants to access his image then it is decrypted in the same manner. The XOR is first performed and the chaotic same number of times as the scans for encryption. This ensures that the image is correctly decrypted. The decrypted image is made available to the user when he wishes to view it. This image is obtained without any distortions and glitches. It is exactly the same image that the user had saved on the cloud in his folder.

Apart from the encryption based security we also provide security in terms of identity management and intrusion detection. Only the authorized users are allowed to access the data on the cloud. The user is alerted whenever there are any signs of unauthorized access. The images, that is, the user data is stored in the best possible secure fashion. The data access is also simple. The user interface is also easy to understand and easy to use.

Algorithms:

1. **Triple DES**

   Triple DES is used while storing user-sensitive data in database. It is a symmetric key encryption algorithm. Same key is used for encryption and decryption. So the main thing in using symmetric key algorithm is the need to have the same key for decryption as well as for encryption. It will generate an MD5 hash based on that string input by user to make a key. Then it will use this key to encrypt and decrypt the plain text.

   The encryption and decryption algorithm is:

   $$\text{ciphertext} = E_{K_3}(D_{K_2}(E_{K_1}(\text{plaintext})))$$

   DES encrypts with $K_1$, DES decrypts with $K_2$, then DES encrypt with $K_3$.

   $$\text{plaintext} = D_{K_1}(E_{K_2}(D_{K_3}(\text{ciphertext})))$$

   DES decrypts with $K_3$, encrypts with $K_2$, and then decrypt with $K_1$.

   **In our case all three keys are identical, i.e. $K_1 = K_2 = K_3$.**

2. **MD5**

   An MD5 hash is created by taking a string of $n$ length and encoding the string into a 128-bit fingerprint. Encoding the same string using this algorithm will always result in the same 128-bit hash output. From a simple string of up to 256 characters in length, this tool provides a quick and easy way to encode an MD5 hash.

   These hashes are also used to ensure the data integrity of files. Hashing is not encryption. It is a fingerprint of the given input. It is nearly impossible to reverse engineer an MD5 hash to retrieve the original string as is a one-way transaction.

3. **Encryption and Decryption**

   So the same cryptosystem. The XOR is first performed and the chaotic
   Based Encryption wherein we shuffle the image block by using multiple scans of image. As a further improvisation to XOR, the image can be divided into smaller blocks of 4x4 or 8x8. These smaller blocks can then be individually subjected to encryption by XOR. Different images can be used for this purpose. Fixed static images can be used or the images may be randomly selected form a set of images using a key. The level of encryption depends on the level of security needed. The more secure the image requirement, the more complicated the encryption can be done.

   ![Fig.2. Chaos Based Encryption](image-url)
VI. SCREEN SHOTS

Imagedit

Create New User
Name: 
Email id: 
Mobile_Number: 

Account Information
Password: 
Re-Enter Password: 

Submit
Security Question: 
Answer: Insert Clear

Fig. 3. Registration

Fig. 4. Upload Image

Fig. 5(a). Edit Image

Fig. 5(b). Edited Image

Fig. 6. Encrypted Image

Fig. 7. Decrypted Image

VII. CONCLUSION AND FUTURE SCOPE

Considering importance of cloud technology, it is highly important to secure cloud applications from all kinds of attacks. The proposed design tries to leverage benefits of cloud computing and enhance the security of the application.

The image editing application provides the image editing features along with the benefits of cloud. The application banks on the cloud storage and provides user to store and edit the images as per his convenience. The sheer ease of accessing the image from everywhere coupled with the enhanced security features makes the website a ready tool.

The prototype discussed in this paper differs in 1. It provides a platform to the user to upload pictures anytime and anywhere.
2. Pictures can be viewed and edited anywhere according to the user requirement.

3. The pictures can be shared with the friends of the user.

4. The data of the user is stored in an encrypted manner including the images, folder paths and authentication information.

5. Images are encrypted using chaos-based encryption.

6. A new simple and fast algorithm is used for image encryption.

7. Decrypted images can be accessed whenever required by the user.

VIII. ACKNOWLEDGEMENT

We wish to acknowledge Prof. Mahendra Pawar and Prof. Vinod Alone for their throughout support and guidance in every step from conceptualization to implementation of system aiding in successful completion of this survey paper.

IX. REFERENCES


