ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 6, June 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Analysis of Cloud Computing Security Using Pixel Key Pattern with AES

V. N. M. Padmavathy[1]
Research Scholar
H.H.The Rajah's College (Autonomous),
Pudukkottai – India

Dr. S. Ravichandran[2]
Research Guide, Head of The Department of CA
H.H.The Rajah's College (Autonomous),
Pudukkottai – India

Abstract: ***Cloud computing is not an innovation, but a means for the use of advanced computing power and storage capacity of the building improved IT services. Cloud computing has a lot of comment. Attempts to describe the general cloud computing, however, has a problem because cloud computing is not a single type of system, but the basic technology deployment spectrum covered, configuration possibilities, service models and modes. Internet for those who use the media as a means to allow a significant impact on the delivery of content-related industries to the end users. For this to work, the use of technical advice is well known Rijndael encryption algorithm (REA) with the help of the algorithm can be encrypted under a public cloud storage of user data, but also to decipher it. This article describes the hybrid cloud, allowing organizations to provide secure data storage in the public cloud, private cloud and remain in the organization's information security storage related architectures. In this architecture, data access or want to share only with the user's public cloud interaction, they did not enter the public user access to the private cloud. And we moved here discussed security and data security of the rest of the data.***

Keywords: Cloud, Encryption Algorithm, Pixel Key Pattern, Rijndael Algorithm, Security.

I. INTRODUCTION

Cloud computing is an on demand computing in which dynamically scalable and often virtualized resources are provided as a service. It is a methodology that takes the help of the internet to provide services like storage for the end users, computations, database driven services for different sectors of industries.

Security is the key for the Cloud success, security in the cloud is now the main challenge of cloud computing.

The Cloud Security Alliance (CSA) defines areas of concern for cloud computing divided into two broad categories: governance and operations. All of these areas are critical and should be taking in consideration when evaluating the security of a cloud environment.

With multi-tenancy resources are shared by multiple users. For example, two or more tenants could have their OSs running on the same server or two or running an instance of the same application with different data.

Data security is a critical issue for open systems based on cloud applications or World Wide.

In recent ages, transmission through communication medium requires more data security. Attacks on data may decrease its worth. There are lots of ways available to overcome this issue. One of them is secure data transfer through image.

II. LITERATURE SURVEY

Randeep Kaur et al Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution.

R. Kalaichelvi et al in this paper, visual cryptography is proposed to maintain data confidentiality. Additionally, a range of visual cryptography schemes are explored in terms of their unique properties. Cloud Computing is a boon to store a massive amount of data.

Randeep Kaur et al This paper is focused on the security issues of cloud computing and techniques to overcome the data security issue. Before analysing the security issues, the definition of cloud computing and brief discussion to under cloud computing is presented.

R. Charanya et al It provide elastic architecture accessible through internet and also it eliminate the setting up of high cost computing infrastructure for the IT based solutions and services. Cloud computing is pay-per-use model, on-demand network access to a shared pool of configurable computing resources like Application-as a service, Platform as a services and infrastructure as a services.

III. METHODOLOGY

A. Cloud Computing

Cloud Computing is a booming era which guarantees reliable, scalable, pay-per-use, customized and dynamic computing environments for end-users. The quickly evolving technology is subsequently leading to the rise in the requirements of the clients. This new paradigm of cloud computing is appealing vendors and various associations have begun understanding the profits by putting their applications and data into the cloud. This helps in cheaper and efficient utilization of available resources and easier handling of larger computational problems.

B. Security of Data in Cloud

Security is a key barrier to the broader adoption of cloud computing. The real and perceived risks of providing, accessing and controlling services in multitenant cloud environments can slow or hinder the migration to services by IT organizations. Although cloud computing promises lower costs, rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy.

The data in the cloud may be divided into the data in IaaS environment and the data in PaaS or SaaS environment related to cloud based applications. The data stored in the cloud storages is similar with the ones stored in other places and needs to consider three aspects of information security: confidentiality, integrity and availability. The common solution for data confidentiality is data encryption. To ensure the effect of encryption, the use of both encryption algorithm and key strength are needed to be considered. As the cloud computing environment encompasses large amounts of data transmission, storage and handling so there also needs to consider processing speed and computational efficiency of encrypting large amounts of data. In such cases, symmetric encryption algorithm is more suitable than asymmetric encryption algorithm.

C. Steganography

Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganography techniques available to hide the data depending upon the carriers we use. In steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption.

D. Algorithm

1. client registers and logins with the cloud provider.
2. for all the images in the dataset, choose the random image say k.
3. the data (m) is stored in the variable named d.
4. compute the length of the m ; lets say 10.
5. find all the contours in the image using pixel key pattern,
6. if the contour's thickness > threshold_value
7. compute the matrix of that pixel
8. else
9. find the next contour
10. convert the available matrix as well as the data into the bytes format.
11. replace the redundant bits of the matrix with the bits of the data.
12. create the new image with the help of available matrics.
13. client sends the image to the available gateway.
14. find the size of the file (say 1000kb)
15. split the file using threshold value (100 bytes)
16. for i=1 to 1000
17. j =0;
18. if(j < 100)
19. read the data from the original file
20. write into the new file 21. j++;
21. else
22. create a new file
23. j = 0;
24. end if
25. end for
26. send these fragmented files to the cloud provider for storage.

E. Pixel Key Pattern

Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganography techniques available to hide the data depending upon the carriers we use. In steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption. Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. The main file formats that are used for steganography are text, images, audio, video, protocol. Images are the most popular cover objects used for steganography.

The scope of the work is to extract the useful information from large amount of data and store at cloud in secure fashion and then make inferences required by the organization. But the predictions that are generated as a result of mining should be secure from any kind of interception. In this sense, steganography is the best option for sending information secretly because it hides the existence of secret message and provides more security. The security module which is used is image steganography as images are the most popular because of their frequency on the Internet. So the prime focus is to increase the capacity to provide better security during transmission.

IV. ALGORITHM CONCEPTS

A. Rijndael Algorithm

The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys.

Rijndael is an iterated block cipher. Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). provides the details of the Rijndael round function. Rijndael also defines a method to generate a series of subkeys from the original key. The generated subkeys are used as input with the round function.

Rijndael was designed based on the following three criteria :

- Resistance against all known attacks;
- Speed and code compactness on a wide range of platforms;
- Design simplicity

B. Pixel Key pattern

Edge detection is a tool used in image processing and computer visualization. It is the process which aims at identifying and locating sharp points in an image which are due to the change in pixel intensity. The most common algorithm used for edge detection is pixel key pattern. It uses multistage algorithm to detect a wide range of edges in images. The characteristics of this algorithm are: low error rate, edge points be well localized and single response to an edge.

We can extract all pixel values only when image is given as an input. We can apply cipher algorithm having following steps.

Step -2. Start

Step -2. Import data and form image by interpreting each element.

Step -3. Extract all r, g, b component from image.

Step -4. Reshape all r, g, b component in to one dimensional array for each.

Step -5. Let, t= [y; 1; p] which is a column matrix. Step -6. Transpose ‘t’ .

Step -7. Reshape ‘t’ into one dimensional array. S

Step -8. Let, n= Total number of array.

Step -9. Let, r= (1st part of n): (1/3rd part of n) as one dimensional array.

Step -10. Let, b= (1/3rd part of n): (2/3rd part of n) as one dimensional array.

Step -11. Let, g= (2/3rd part of n): (nth) as one dimensional array.

Step -12. Transform its with its original dimensions.

Step -13. Finally all data will convert into an image. For decrypt the image from cipher text to plain text inverse of algorithm is used.

V. PROBLEM DESCRIPTION

Cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many Security problems. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. Cloud computing infrastructures use new technologies and services, most which have not been fully evaluated with respect to security. This leads to affects many customers who are sharing the infected cloud. The security issues faced by cloud computing are discussed below:

1. Data Access Control: Sometimes confidential data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Data exists for a long time in a cloud, the higher the risk of unauthorized access.
2. Data Integrity: Data integrity comprises the following cases, when some human errors occur when data is entered. Errors may occur when data is transmitted from one computer to another; otherwise error can occur from some hardware malfunctions, such as disk crashes.
3. Data Theft: Cloud computing uses external data server for cost affective and flexible for operation.
4. Data Loss: Data loss is a very serious problem in Cloud computing. If banking and business transactions, research and development ideas are all taking place online, unauthorized people will be able to access the information shared.
5. Privacy Issues: Security of the Customer Personal information is very important in case of cloud computing. Most of the servers are external, so the vendor should make sure that is well secured from other operators.
6. Security issues in provider level: A Cloud is good only when there is a good security provided by the vendor to the customers. Provider should make a good security layer for the customer and user .And should make sure that the server is well secured from all the external threats it may come across. The cloud computing service provider has.
7. User level Issues: User should make sure that because of its own action, there should not be any loss of data or tampering of data for other users who are using the same Cloud.

VI. IMPLEMENTATION

A. Implementation

The smooth ordering of patches is done and this can be used for many applications. The applications are like the image denoising, image inpainting image de-blurring etc. The method for the smooth ordering of the image is reordering the patches of the image. Thus reconstructing the original image.For implementation, we have an image with us. Now we are adding some disturbances into it for making it a corrupted image. Now this is the image on which we have to apply the smooth reordering of patches and perform image denoising and image in-painting. Y is the original image and Z the image after adding impurities. Z could be having noise or it could have missing pixels. The corrupted image then satisfies

$$z = My + v$$

B. Permutation matrix

To design a matrix P, that would produce a smooth signal when it is applied to the target image y is as follows. When the image Y is known, the solution is to reorder it as a vector, and then apply a simple sort operation on the obtained vector.

C. Image Inpainting

The problem of image inpainting is of the recovery of missing pixels in the given image. Here v = 0, and M is a diagonal matrix of size N X N which contains ones and zeroes in its main diagonal corresponding to existing and missing pixels, correspondingly. Each patch may contain missing pixels, and we denote by Si the set of indices of non-missing pixels in the patch xi . We choose the distance measure between patches xi and x j to be the average of squared differences be-tween existing pixels that share the same location in both patches. First the matrix P is calculated. when a patch does not share pixels with any of the unvisited patches, the next patch in the path is chosen to be its nearest spatial neighbour. An operator H is used, which recovers the missing values using cubic spline interpolation. We apply the matrix P 1 on the resulting vectors and obtain the estimated subimages y j

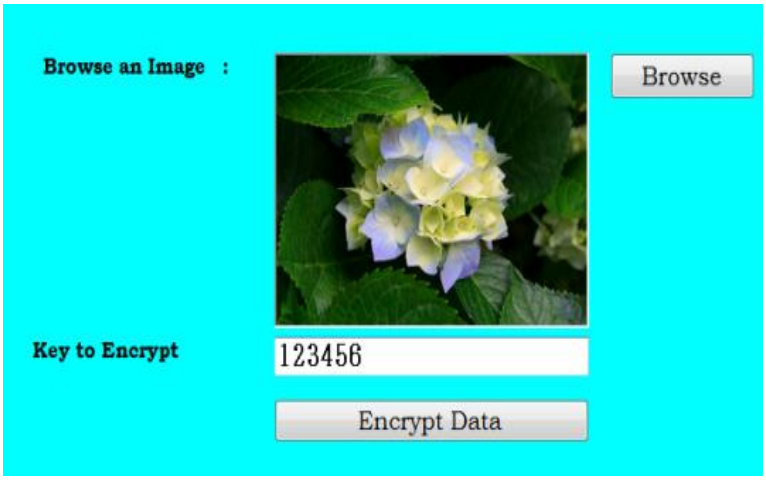
D. Image denoising

In image denoising, the recovery of an image from its noisy version is carried out. In that case M = I and the corrupted image satisfies z = y + v. The patches xi may contain noise, and we choose the distance measure between xi and x j to be the squared Euclidean distance divided by n. A 1D linear shift invariant filter, is used for this purpose. There are two filters to switch between based on the patch content. The smooth areas in the image are treated differently than areas with edges or texture. First patches are partitioned into those smooth Ss and those with edges and texture Se.

E. Encryption

An Encryption Scheme known as Pixel Key pattern Algorithm is implemented on the image after denoising and inpainting This encryption makes these images free to be used for military purposes where the secrecy of recovered image is necessary. Encryption is implemented as follows.

1. The M X M square matrix is divided into rectangles of width *vi* and number of elements M.
2. The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from right to left beginning with upper rectangles, and then lower ones.
3. Inside each rectangle, the scan begins from the bottom left corner towards upper elements.



F. Encoding Process

Step 1: The application prompts for the text and image from the sender who wants to hide the message.

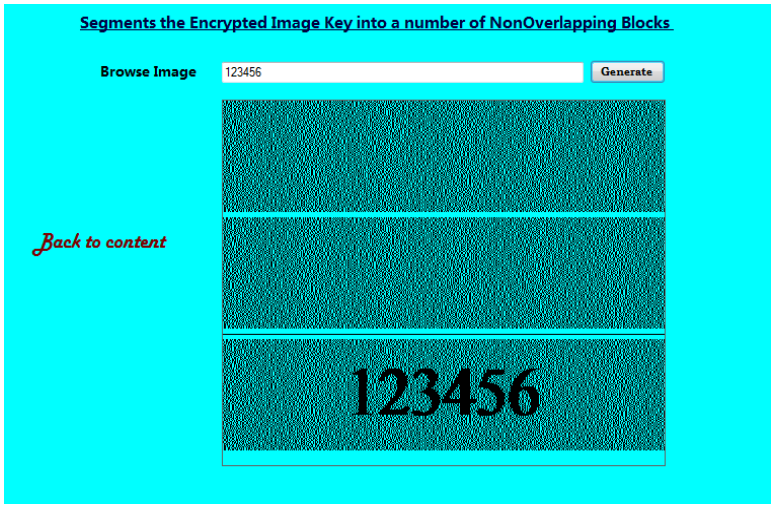
Step 2: Steganographic program encrypts the text using DES or RSA or any other encryption algorithm.

Step 3: Steganographic program analyses the image to find the pixel value of all the pixels within the image.

Step 4: Steganographic program uses the unique RGB modbit method to find out whether each letter of the message can be represented in the image and records the position to a field in the image metadata itself. For calculation of modbit the program adds the RGB values of each pixel and divides it to get the mod. If the mod value matches with that represented for the character internally, the position for that character is recorded.

Step 5: If the image does not have pixel values to represent a particular character, the steganographic program finds and changes a pixel that almost matches with the image pixel and which can represent the character of text.

Step 6: Finally when all the pixels which can be identified on the image and its position is recorded along with the image metadata, the user is informed that the encryption part is complete.



Set pixel values in image

:ncrypted image has been successfully saved.

G. Decoding Process

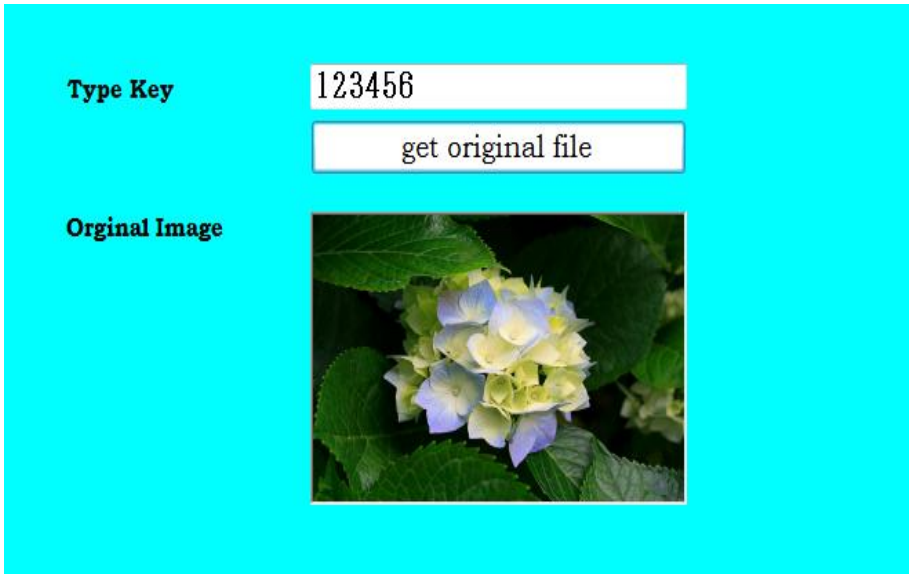
Step 1: The receiver opens the image.

Step 2: The steganographic software asks for key to decrypt the image file.

Step 3: Steganographic software decrypts the metadata first and finds the pixel positions.

Step 4: Using the pixel positions, get the RGB values and decodes by reverse modbit and finds the corresponding encrypted text.

Step 5: Decrypt this text and provide back the message to the user.



VII. Conclusion and Further Work

Cloud computing itself is in the development stage, and therefore has not completed a security risk. Obviously, even the major cloud service provider such as Amazon, Google and other faces many security challenges, remained stable. Achieve a comprehensive settlement of the legal issues is still a problem. Cloud computing in the organization may decide only on the basis of the risk benefit ratio and make the issue of cloud computing at this level, be taken.

Cloud computing should be safe from all external threats, it appears between the customer and service provider cloud securely and mutual understanding. The maximum positive value when the difference between the actual virtual machine security and cloud security. These studies should be gaps and differences and their disposal center. The main goal of cloud computing is to safely store and transfer data cloud.

The existing system contains some disadvantages so the future scope is to remove the disadvantages by adding reversible manner means, data extraction and recovery of image are free of errors. The PSNR will be improved to get original cover back. In future it may possible that memory space can be reserved before encryption which requires less amount of time for data extraction & image recovery In future, we will extend this system considering audio, or video files as the cover. In this paper only digital image is considered as cover.

References

1. Enhancing Cloud Computing Security by Using Pixel Key Pattern by Randeep Kaur, Jagroop Kaur.
2. An Innovative Solution for Cloud Security through Quantitative Analysis of Various Visual Cryptography Schemes by R. Kalaichelvi, Dr. L. Arockiam.

3. Cloud Computing Security Issues And Its Solution: A Review by Randeep Kaur , Jagroop Kaur
4. Levels of Security Issues in Cloud Computing by R. Charanya , M.Aramudhan , K. Mohan , S. Nithya.
5. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques by Rohit Bhadauria, Sugata Sanyal.
6. H. Sharma, M. Arya, D. Goyal, "Secure Image Hiding algorithm using cryptography and steganography", International Journal of Scientific Research, vol. 13 (5), pp. 01-06, Jul-Aug. 2013.
7. . Memon, M. R. Naeem, M. Tahir, M. Aamir, A. A. Wagan, "A New Cloud Computing Solution for Government Hospitals to Better Access Patients' Medical Information", American Journal of System and Software, vol. 2 (3), pp. 56-59, June 2014.
8. Ayushi, "A Symmetric Key Cryptographic Algorithm",in International Journal of Computer Applications, pp. 01-04, February. 2010.
9. R. M. Patel, D. J. Shah," Multiple LSB data hiding based on Pixel value And MSB value", in 2013 Nirma University InternationalConference ,pp. 1-5, November. 2013.
10. M. Mishra, G. Tiwari, A. K. Yadiv,"Secret Communication Using Public Key Steganography", in IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), pp. 1-5, May. 2014.
11. S. Narayana, G. Prasad,"Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions", Signal & Image Processing: An International Journal (SIPIJ), pp. 60-73, December. 2010.
12. W. Stallings, Cryptography and Network Security, (Five Editions), ISBN: 978-81-317-6166-3, 2011. [13] M. R. Naeem, W. Zhu, A. A. Memon," New approachfor UML Based modeling of relational databases", International Journal of Computer Science and Telecommunications, Vol. 5(5), pp. 18-23,May. 2014.
13. F. B. Shaikh, S. Haider," Security threats in cloud Computing", in 6th International Conference on Internet Technology and Secured Transactions, p. 214-219, December. 2011.
14. H. Matbouli, Q. Gao, "An Overview on Web Security Threats and Impact to E-Commerce Success", in 2012 International Conference on Information Technology and e-Services, pp. 1- 6, March. 2012.
15. M. Jouini, L. B. A. Rabai, A. B. Aissa," Classification of security threats in information systems", 5th international conference on Ambient Systems, pp. 489-496, December.2014.

