3-Layer Security Using Face Recognition in Cloud

[1]Yogeshwari Chaudhari, [2]Tanaya Dave,[3]Sarita Barade,[4]SupriyaMane,
[5]Prof.S.M.Sangve,[6]Prof.A.S.Devare

1,2,3,4 UG Student, Department of Computer, Dnyanganga College of Engineering and Research;
Pune,Maharashtra,India
5,6Assistant Professor, Department of Computer, Dnyanganga College of Engineering and Research;
Pune,Maharashtra,India

Abstract

In cloud computing databases are the centralized large data centers, where the management of the data and services may not be fully trust worthy which is provided by large amount of computing and storage to customers provisioned as a service over the internet. Due lack of proper security and weakness in safeguard which lead to many vulnerability in cloud computing. This paper has been written to focus on the problem of data leakage. In first phase which is known as Data classification the classification of data is done by client before storing it. During this phase the data is to be categorized on the basis of CIA (Confidentiality, Integrity, and Availability). The client who wants to send the data for storage needs to give the value of C (confidentiality), I (integrity), A(Availability). The value of C is based on level of secrecy of data processing and prevents unauthorized disclosure, value of I based on how much assurance of accuracy is provided, reliability of information and value of A is based on how frequently it is accessible. Second phase, known as Data Access uses 3-layer technique for accessing the data. The user wanting to access the data needs to be registered and before every access to data, his/her identity is authenticated for authorization. For the authentication purpose we use face recognition.

Keywords: *Cloud security, Data protection, Data Storage, Confidentiality, Integrity, Availability, Face Recognition.*

1. INTRODUCTION

Cloud computing is a comprehensive solution that delivers IT as a service. It is an Internet-based computing solution where shared resources are provided like electricity distributed on the electrical grid. Computers in the cloud are configured to work together and the various applications use the collective computing power as if they are running on a single system. Services are classified into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud computing is deployed as three models such as Public, Private, and Hybrid clouds [3].Data storage in cloud offers so many benefits to users: It provides unlimited data storage space for storing user's data. Users can access the data from the cloud provider via internet anywhere in the world not on a single machine. We do not buy any storage device for storing our data and have no responsibility for local machines to maintain data. There are different issues and challenges with each cloud computing technology. In this paper a solution to the security problem of Database providing using 3 Layer security for database in cloud and Providing Biometric Solution to password management for database in cloud.

2. LITERATURE SURVEY

Recently, Wang et al. [4] proposed a homomorpic distributed verification protocol to ensure data storage. This protocol is the security in cloud computing using Pseudorandom Data. Their scheme achieves the storage correctness as well as identifies misbehaving servers. However, this scheme was not providing full protection for user storage data in cloud computing, because Pseudorandom Data does not cover the entire data while verifying the cloud servers for data storage correctness i.e. some data corruptions may be missing.

From the cloud consumers' perspective, security is the major concern that hampers the adoption of the cloud computing model [4]Enterprises outsource security management to a third party that hosts their IT assets (loss of control).

- Co-existence of assets of different tenants in the same location and using the same instance of the service while being unaware of the strength of security controls used.

- The lack of security guarantees in the SLAs between the cloud consumers and the cloud providers.

- Hosting this set of valuable assets on publicly available infrastructure increases the probability of attacks.

From the cloud providers' perspective, security requires a lot of expenditures (security solutions' licenses), resources (security is a resource consuming task), and is a difficult problem to master (as we discuss later). But skipping security from the cloud computing model roadmap will violate the expected revenues as explained above. So cloud providers have to understand consumers' concerns and seek out new security solutions that resolve such concerns. Encryption is the traditional way of security measure for protecting files, but it introduces computational overhead as the data has to be encrypted to store it and decrypted for processing.

According to the 2009 Data Breach Investigations Report conducted by Verizon Business Risk Team, 64% of data breaches resulted from hacking and intrusions. Dedicated resources are expected to be more secure than shared resources. The attack surface in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are neither being tampered with nor compromised, particularly when residing on shared physical infrastructure. Security management needs to include security requirements and policies specifications; security controls configurations according to the policies specified, and feedback from the environment and security controls to the security management and the cloud stakeholders.

[1] Proposes an algorithm for data leakage. The first job of the user is to categories it on the basis of confidentiality, integrity and availability. Here D [] represents data, now the user have to give the value of C–confidentiality I–integrity and A–availability. After Appling proposed formula the value of criticality raring is calculated. Now allocation of data on the basis of Cr is done in protection ring. This suggests that internal protection ring is very critical and it require more security technique to ensure confidentiality.

In the algorithm proposed in [1] the term I has not been used anywhere in the formula. Also for the value 7 of S[k] no ring has been assigned.

3. PROPOSED METHOD

In existing system [1] when user sends request along with username to access the data to cloud provider, the cloud provider first check in which ring requested data belong. If authentication is required, it first checks the username in its own directory for existence, if the username does not exist it ask the user to register itself. If the username matches it redirect the request to company for authentication.

To avoid user efforts when password does not match and user has to go back to company and register again this system give solution to this problem by providing face authentication rather than password. In this first user fills registration form and provides all details(UID), at that time he also provides his face. This face image is cropped and face feature vector is generated using Canny Edge Detection Algorithm. This feature vector is stored in encrypted format along with the ring no to which the user belongs. When the user wants to access the data stored he simply has to give his UID and face. Again face feature vector is calculated, matched with the existing feature vector(if the user is already registered). If the match is within the threshold value the user gets authenticated to access the data. If the user is not registered he first needs to register to access the data.

The data to be stored is classified according to CIA value. After that the data is encrypted and send to cloud for storage according to ring i.e ring1 contains most confidential data,ring2 contains those data which is protected from unauthorized modification,ring3 contain data which is publicly available

.

Proposed Algorithm for classification of data:

```
1. For i=1 to n
        3.1 C[i] =value of confidentiality
        3.2 I[i] =value on integrity
        3.3 A[i] =value of availability

2. For i=1 to n
        S[i] =C[i] +I[i] +A[i];
        If S[i] ==7 then
        R[i]=1              /*ring 1*/
        If S[i] ==6 then
        R[i] =2              /*ring 2*/
        If S[i]==5 then
        R[i] =3              /*ring 3*/
```

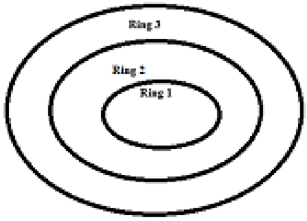


Fig. 1 Protection rings

For authentication of face we have applied the method as suggested in [2].Here Canny Edge Detection algorithm has been used as mentioned in [7].

Canny's edge detection algorithm:
The Canny edge detection algorithm is known to many as the optimal edge detector. Gray scaled image should be given as input to Canny Edge Detection Algorithm.
The algorithm runs in 5 separate steps:

1. Smoothing: Blurring of the image to remove noise
.
2. Finding gradients: The edges should be marked where the gradients of the image has large magnitudes.

3. Non-maximum suppression: Only local maxima should be marked as edges.

4. Double thresholding: Potential edges are determined by thresholding.

5. Edge tracking by hysteresis: Final edges are determined by suppressing all edges that are not connected to a very certain (strong) edge.

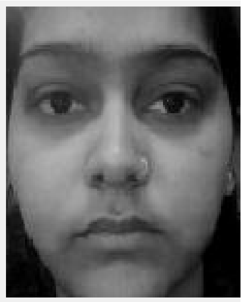


Fig. 2 Original Image

The detailed steps are as follows:

Step1:

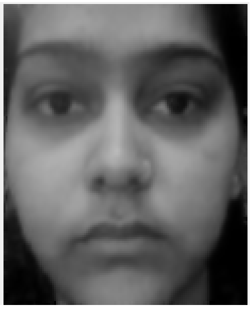
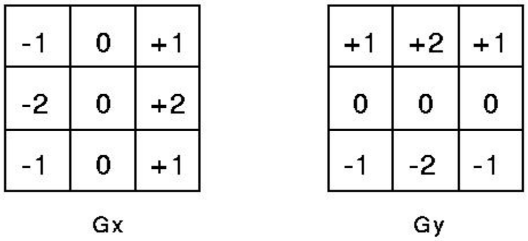


Fig. 3 Smoothened Image

The first step is to filter out any noise in the original image before trying to locate and detect any edges. And because the Gaussian filter can be computed using a simple mask, it is used exclusively in the Canny algorithm. Once a suitable mask has been calculated, the Gaussian smoothing can be performed using standard convolution methods. A convolution mask is usually much smaller than the actual image. As a result, the mask is slid over the image, manipulating a square of pixels at a time. The larger the width of the Gaussian mask, the lower is the detector's sensitivity to noise. The localization error in the detected edges also increases slightly as the Gaussian width is increased. The Gaussian mask used in my implementation is shown below.

Step 2:

After smoothing the image and eliminating the noise, the next step is to find the edge strength by taking the gradient of the image. The Sobel operator performs a 2-D spatial gradient measurement on an image. Then, the approximate absolute gradient magnitude (edge strength) at each point can be found. The Sobel operator uses a pair of 3x3 convolution masks, one estimating the gradient in the x-direction (columns) and the other estimating the gradient in the y-direction (rows). They are shown below:



-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Fig 4. Sobel operators

The magnitude, or edge strength, of the gradient is then approximated using the formula:
$|G| = |Gx| + |Gy|$

Step 3:

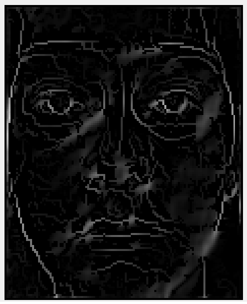


Fig. 5 Edges after non-maximum suppression

The direction of the edge is computed using the gradient in the x and y directions. However, an error will be generated when sumX is equal to zero. So in the code there has to be a restriction set whenever this takes place. Whenever the gradient in the x direction is equal to zero, the edge direction has to be equal to 90 degrees or 0 degrees, depending on what the value of the gradient in the y-direction is equal to. If GY has a value of zero, the edge direction will equal 0 degrees. Otherwise the edge direction will equal 90 degrees. The formula for finding the edge direction is just:

Theta = inverse tan (Gy / Gx)

Step 4:

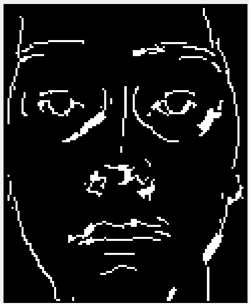


Fig. 6 Strong Edges

Once the edge direction is known, the next step is to relate the edge direction to a direction that can be traced in an image. There are only four possible directions when describing the surrounding pixels - 0 degrees (in the horizontal direction), 45 degrees (along the positive diagonal), 90 degrees (in the vertical direction), or 135 degrees (along the negative diagonal). So now the edge orientation has to be resolved into one of these four directions depending on which direction it is closest to (e.g. if the orientation angle is found to be 3 degrees, make it zero degrees). Think of this as taking a semicircle and dividing it into 5 regions.

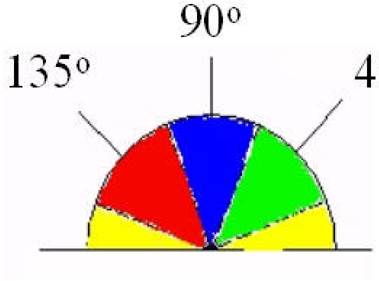


Fig 7. Canny Edge Detector

Therefore, any edge direction falling within the yellow range (0 to 22.5 & 157.5 to 180 degrees) is set to 0 degrees. Any edge direction falling in the green range (22.5 to 67.5 degrees) is set to 45 degrees. Any edge direction falling in the blue range (67.5 to 112.5 degrees) is set to 90 degrees. And finally, any edge direction falling within the red range (112.5 to 157.5 degrees) is set to 135 degrees.

Step 5:

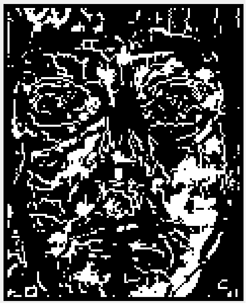


Fig. 8 Weak Edges

After the edge directions are known, non maximum suppression now has to be applied. Non maximum suppression is used to trace along the edge in the edge direction and suppress any pixel value (sets it equal to 0) that is not considered to be an edge. This will give a thin line in the output image.

Finally, hysteresis is used as a means of eliminating streaking. Streaking is the breaking up of an edge contour caused by the operator output fluctuating above and below the threshold. If a single threshold, T1 is applied to an image, and an edge has an average strength equal to T1, then due to noise, there will be instances where the edge dips below the threshold. Equally it will also extend above the threshold making an edge look like a dashed line. To avoid this, hysteresis uses 2 thresholds, a high and a low. Any pixel in the image that has a value greater than T1 is presumed to be an edge pixel, and is marked as such immediately. Then, any pixels that are connected to this edge pixel and that have a value greater than T2 are also selected as edge pixels. If you think of following an edge, you need a gradient of T2 to start but you don't stop till you hit a gradient below T1.

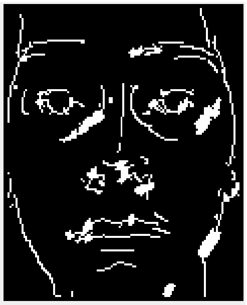


Fig. 9Final Image

4. CONCLUSION

This paper deals with providing security to the data on cloud which is a very major issue currently. The data to be stored on cloud is classified on the values on Confidentiality, Integrity, and Availability and stored into the 3 different rings (virtual rings). To access data priority on rings is checked. For authentication purpose while accessing data we are using face recognition as it is more efficient compared to the password management.

During face recognition the environmental conditions such as lighting, position of face etc. matter. To improve the quality of face recognition more advanced algorithms can be used which may include facial expression recognition, 3D face recognition etc.

References

[1] Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal“3 Dimensional Security in Cloud Computing”, IEEE 2011.

[2] Chenguang Wang and et al,”Study of Cloud Computing Security Based on Private Face Recognition”, IEEE 2010

[3] Cloud Computing FOR DUMMIES by Judith Hurwitz, RobinBloor, Marcia Kaufman, and Fern Halper. WILEY INDIAEDITION.

[4] Cong Wang,Qian wang and Kui Ren and Wenjing Lou,“Ensuring Data Storage Security in Cloud Computing ,Quality of Service, 2009, IWQoS IEEE 17th Internationalworkshop ,pp 1-9,2009.

[5] Paul S. Wooley,Network Analyst, Tyco Electronics “Identifying Cloud Computing SecurityRisks” February 2011

[6] Turk, M.A., Pentland, A.P., “Face recognition using eigenfaces.”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 586–591(1991)

[7] John Canny. A computational approach to edge detection. Pattern Analysis
Intelligence, IEEE Transactions on, PAMI-8(6):679–698, Nov. 1986.