Available Online through  
www.ijptonline.com  

FACE RECOGNITION IN CLOUD COMPUTING  
R. Prema, Dr. P. Shanmugapriya, Dr. R. VasanthKumar Mehta  
1Assistant Professor and Research Scholar, Department of Computer Science and Engineering,  
SCSVMV University, Kanchipuram, Tamilnadu, India.  
2Associate Professor, Department of Information Technology, SCSVMV University,  
Kanchipuram Tamil Nadu, India.  
3Associate Professor and Head, Department of CSE, SCSVMV University, Kanchipuram, Tamil Nadu, India.  
Email: premarajan2013@gmail.com  

Received on: 20.10.2016  
Accepted on: 25.11.2016  

Abstract  

Face recognition presents a challenging problem in the field of image processing, image analysis and computer vision,  
and as such has received a great deal of attention over the last few years because of its many applications in various  
domains. A lot of algorithms and techniques have been proposed for solving the challenge a person using face  
recognition system.  

Cloud computing is a new technology whereas user can access their files or data or information from any place using the  
internet. There are several benefits of cloud computing like increased throughput, reduced costs, and improved  
accessibility but on the other hand it has some security issues and drawbacks. User authentication is a major problem.  
Due to lack of proper security and weakness in safeguard which lead to many vulnerability in cloud computing. This  
paper focuses on the problem of security. In first phase which is known as Data classification the classification of  
data is done by client before storing it.  

Keywords: Cloud security, Data Storage, Data Security, Face Recognition, Authorized Person.  

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\(^1\). 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\(^2\).

2. Related Work

Recently, In\(^3\) proposed a homomorphic distributed verification protocol to ensure data storage. This protocol is the security in cloud computing using Pseudorandom Data. Their scheme achieves the Database providing using 3Layer security for database in cloud and Providing Biometric Solution to password management for database in cloud.

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\(^4\). From the cloud consumers’ perspective, security is the major concern that hampers the adoption of the cloud computing model Enterprises outsource security management to a third party that hosts their IT assets (loss of control)\(^5\).

- 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\(^6\). According to the Data Breach Investigations Report conducted in 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 risk⁷. 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 stakeholders⁸. 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 ring 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 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 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. The data leakage and security attacks can be caused by insufficient authentication. Cloud services are paid services so to identify authorized user is major concern in cloud computing. In this paper, we focus on the security issues of cloud computing, particularly on authentication. To solve authentication problem in cloud computing, there are different traditional as well as biometric techniques as stated below but it has some drawbacks. 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 Algorithm⁹. 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 in Figure 1 i.e ring 1 contains most confidential data, ring 2 contains those data which is protected from unauthorized modification, ring 3 contain data which is publicly available. Proposed Algorithm for classification of data:

1. For i=1 to n
   
   \[ C[i] = \text{value of confidentiality} \]
   
   \[ I[i] = \text{value on integrity} \]
   
   \[ A[i] = \text{value of availability} \]

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 */

![Figure 1. Protection rings.](image)

For authentication of face we have applied the method as suggested in. Here Canny Edge Detection algorithm has been used as mentioned in 12.

Canny’s edge detection algorithm 13:

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 of the image.
2. **Finding gradients:** The edges should be marked where the gradients of the image have large magnitudes.
3. **Non-maximum suppression:** Only local maximum 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.

![Figure 2. Original Image](image)

The detailed steps are as follows:

**Step1:**

![Figure 3. Smoothened Image.](image)

The first step is to filter out any noise in the original image Figure 2 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. The Matlab code for the following: I, J, r, g, b, K Variables to store results.
I = imread ('hawk.png');
J = imnoise (I,'salt & pepper',0.2);

% filter each channel separately
r = medfilt2 (J (:,:, 1), [3 3]);
g = medfilt2 (J (:,:, 2), [3 3]);
b = medfilt2 (J (:,:, 3), [3 3]);

% reconstruct the image from r, g, b channels
K = cat (3, r, g, b);

subplot (121);imshow (J);
subplot (122);imshow (K);

Step 2:

After smoothing the image and eliminating the noise Figure3, 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).

[Gmag, Gdir] = imgradient(I,'prewitt');

Figure, imshow(Gmag, []), title('Gradient magnitude')

Figure, imshow(Gdir, []), title('Gradient direction')

Step 3:

Figure 4. 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\textsuperscript{14}, the edge direction will equal 0 degrees. Otherwise the edge direction will equal 90 degrees. The formula for finding the edge direction is just: \[ \text{Theta} = \text{inverse tan} \left( \frac{\text{GY}}{\text{Gx}} \right) \] Figure 4.

Step 4:

![Figure-5. 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) Figure 5.

Step 5:

![Figure-6. 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 Figure 6. 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 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 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 Figure 7. 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 T1.

![Image](image.jpg)

**Figure-7. Final Image.**

4. **Security Analysis**

In this proposed system, there are several advantages as stated below,

1) Non-intrusive

2) Unique

3) Cheap Technology

4) Fast Identification

5) Contactless Authentication

5. **Conclusion**

The services of cloud computing is based on the sharing. Cloud computing provides variety of services like IaaS, SaaS.
To provide cloud services only to the authorized user, secure authentication is necessary in cloud computing. There are so many authentication techniques like password, OTP, Voice recognition, finger recognition, palm recognition etc. but still it has some drawbacks like at times password techniques are not feasible, password can be easily stolen by hacker or if user uses complex password, user may forget that password etc\textsuperscript{15}.

This paper deals with providing security to the user on cloud which is a very major issue. 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. To improve the quality of face recognition more advanced algorithms can be used which may include different facial expression recognition, 3D face recognition expressions etc.

References:


15. Recent Advances in Image, Audio and Signal Processing.