International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-2, December 2012

Providing Authorization by Using Face Recognization for Private Cloud Computing

Janita S. Patel, G.B.Jethava

Abstract—Cloud computing technology is a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. The main concern is security privacy and trust.This paper include authorization based security for cloud server.In this paper we introduce face recognization to provide authorization for cloud security.

I.INTRODUCTION

Cloud computing is a new concept of computing technology that uses the internet and remote servers in order to maintain data and applications. It provides dramatically scalable and virtualised resources, bandwidth, software and hardware on demand to consumers. This allows the consumers to safe cost of hardware deployment,software licenses and system maintenance. The consumers are able to use applications or services on the clouds using the internet. Users can typically connect to clouds via web browsers or web services. When customer develops their own applications and run their own internal infrastructure then is called private cloud Although cloud computing offers many advantages to the consumers, it also has several security issues.In this paper, we focus on how to solve the security issues of cloud computing. Authentication based on facial biomatrics will be applied to the cloud computing security. This paper illustrates authentication based security by using facial biomatrics.Face recognition system consists of face verification, and face recognition tasks. In verification task, the system knows a priori the identity of the user, and has to verify this identity, that is, the system has to decide whether the a priori user is an impostor or not. In face recognition, the a priori identity is not known: the system has to decide which of the images stored in a database resembles the most to the image to recognize.

II.WHAT IS CLOUD COMPUTING?

Cloud computing is latest trend in IT world. It is Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on-demand, like the electric grid. This technology has the capacity to admittance a common collection of resources on request.It uses the internet and remote servers in order to maintain data and applications. It provides dramatically scalable and virtualised resources, bandwidth, software and hardware on demand to consumers. This

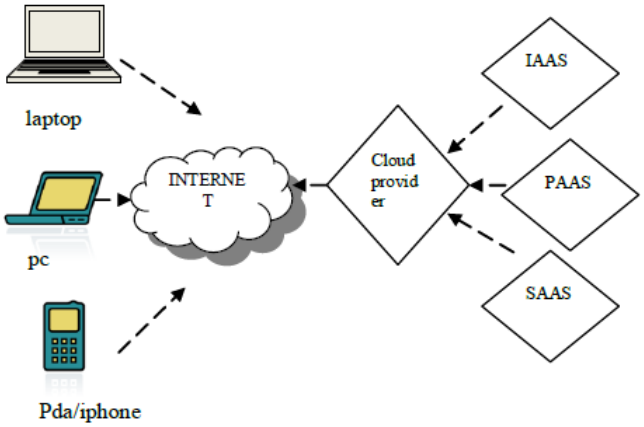

Figure 1

Allows the consumers to safe cost of hardware deployment, software licenses and system maintenance. The consumers are able to use applications or services on the clouds using the internet. Users can typically connect to clouds via web browsers or web service.

A. Types of Cloud

There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services.

a) Public Cloud

A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

b) *Private Cloud*

A private cloud is established for a specific group or organization and limits access to just that group.

c) Community Cloud

A community cloud is shared among two or more organizations that have similar cloud requirements.

d) Hybrid Cloud

A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

B. Security Issues On Cloud Computing

a) Privacy Issue

It is the human right to secure his private and sensitive information. In cloud context privacy occur according to the cloud deployment model.

Manuscript published on 30 December 2012.
* Correspondence Author (s)
Janita S. Patel, M.E.I.T., 3rd sem, Parul Institute if eng. And tech., Gujarat Technical univercity, Vadodara ,India.
G.B.Jethava, H.O.D. of I.T. Dept., Parul Institute if eng. And tech., Gujarat Technical univercity, Vadodara, India.

In Public cloud is one of the dominant architecture when cost reduction is concerned, but relying on a CSP to manage and hold customer information raises many privacy concerns.

b) Lack of user control

In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor. In this new paradigm user sensitive information and data is processed in 'the cloud' on systems having no any, therefore they have danger of misuse, theft or illegal resale. Adding more, this is not patent that it will be possible for a CSP to guarantee that a data subject can get access to all his/her PII, or to comply with a request for deletion of all his/her data. This can be difficult to get data back from the cloud, and avoid vendor lock-in.

c) Unauthorized Secondary Usage

One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized secondary uses of users' data, mostly the targeting of commercials. Now a days there are no technological barriers for secondary uses. In addition, it has the connected issue of financial flexibility of the CSPs: for example, possibility of vendor termination, and if cloud computing provider is bankrupted or another company get data then what would happen.

III. WHAT IS FACE RECOGNIZATION?

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from avideo source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image and produces a score that measures how similar the images are to each other.

A. Face Recognition Techniques (FERET)

a) Eigenfaces

Eigenface is one of the most thoroughly investigated approaches to face recognition. It is also known as Karhunen-Loève expansion, eigenpicture, eigenvector, and principal component.[5,6,] used principal component analysis to efficiently represent pictures of faces. They argued that any face images could be approximately reconstructed by a small collection of weights for each face and a standard face picture. The weights describing each face are obtained by projecting the face image onto the eigenpicture.In mathematical terms, eigenfaces are the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images. The eigenvectors are ordered to represent different amounts of the variation, respectively, among the faces. Each face can be represented exactly by a linear combination of the eigenfaces. It can also be approximated using only the "best" eigenvectors with the largest eigenvalues. The best M eigenfaces construct an M dimensional space, i.e., the "face space".As the images include a large quantity of background area,the above results are influenced by background. The authors explained the robust performance of the system under different lighting conditions by significant correlation between images with changes in illumination the correlation between images of the whole faces is not efficient for satisfactory recognition performance. Illumination normalization is usually necessary for the eigenfaces approach. In summary, eigenface appears as a fast, simple, and practical method. However, in general, it does not provide invariance over changes in scale and lighting conditions.

b) Neural Networks

The attractiveness of using neural networks could be due toits non linearity in the network. Hence, the feature extraction step may be more efficient than the linear Karhunen-Loève methods.contains a separate network for each stored individual . The way in constructing a neural network structure is crucial for successful recognition.It is very much dependent on the intended application. For face detection, multilayer perceptron and convolutional neural network have been applied. For face verification, is a multi-resolution pyramid structure. [8] proposed a hybrid neural network which combines local image sampling, a self-organizing map (SOM) neural network, and a convolutional neural network. The SOM provides a quantization of the image samples into a topological space where inputs that are nearby in the original space are also nearby in the output space, thereby providing dimension reduction and invariance to minor changes in the image sample. The convolutional network extracts successively larger features in a hierarchical set of layers and provides partial invariance to translation, rotation, scale, and deformation. The authors reported 96.2% correct recognition on ORL database of 400 images of 40 individuals. In general, neural network approaches encounter problems when the number of classes (i.e., individuals) increases. Moreover, they are not suitablefor a single model image recognition test because multiple model images per person are necessary in order for training the systems to "optimal" parameter setting.

c) Graph Matching

Graph matching is another approach to face recognition. [9] presented a dynamic link structure for distortion invariant object recognition which employed elastic graph matching to find the closest stored graph. Dynamic link architecture is an extension to classical artificial neural networks. Memorized objects are represented by sparse graphs, whose vertices are labeled with a multiresolution description in terms of a local power spectrum and whose edges are labeled with geometrical distance vectors. Object recognition can be formulated as elastic graph matching which s performed by stochastic optimization of a matching cost function. They reported good results on a database of 87 people and a small set of office items comprising different expressions with a rotation of 15 degrees.

The matching process is computationally expensive,taking about 25 seconds to compare with 87 stored objects on a parallel machine with 23 transputers. [10] Extended the technique and matched human faces against a gallery of 112 neutral frontal view faces.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Probe images were distorted due to rotation in depth and changing facial expression.Encouraging results on faces with large rotation angles were obtained. They reported recognition rates of 86.5% and 66.4% for the matching tests of 111 faces of 15 degree rotation and 110 faces of 30 degree rotation to a gallery of 112 neutral frontal views. In general, dynamic link architecture is superior to other face recognition techniques in terms of rotation invariance; however, the matching process is computationally expensive.

d) Geometrical Feature Matching

Geometrical feature matching techniques are based on the computation of a set of geometrical features from the picture of a face. The fact that face recognition is possible even at coarse resolution as low as 8x6 pixels when the single facial features are hardly revealed in detail, implies that the overall geometrical configuration of the face features is sufficient for recognition. The overall configuration can be described by a vector representing the position and size of the main facial features, such as eyes and eyebrows, nose, mouth, and the shape of face outline.face recognition program provided with features extracted manually could perform recognition apparently with satisfactory results [7] automatically extracted a set of geometrical features from the picture of a face, such as nose width and length, mouth position, and chin shape. There were 35 features extracted form a 35 dimensional vector. The recognition was then performed with a Bayes classifier. They reported a recognition rate of 90% on a database of 47 people. In summary, geometrical feature matching based on precisely measured distances between features may be most useful for finding possible matches in a large database such as a Mug shot album. However, it will be dependent on the accuracy of the feature location algorithms. Current automated face feature location algorithms do not provide a high degree of accuracy and require considerable computational time.

e) Template Matching

A simple version of template matching is that a test image represented as a two-dimensional array of intensity values is compared using a suitable metric, such as the Euclidean distance, with a single template representing the whole face. There are several other more sophisticated versions of template matching on face recognition. One can use more than one face template from different viewpoints to represent an individual's face.

One drawback of template matching is its computational complexity. Another problem lies in the description of these templates. Since the recognition system has to be tolerant to certain discrepancies between the template and the test image, this tolerance might average out the differences that make individual faces unique.

In general, template-based approaches compared to feature matching are a more logical approach. In summary, no existing technique is free from limitations. Further efforts are required to improve the performances of face recognition techniques, especially in the wide range of environments encountered in real world.

f) 3D Morphable Model

The morphable face model is based on a vector space representation of faces [8] that is constructed such that any convex combination of shape and texture vectors of a set of examples describes a realistic human face. More recently, [9] combines deformable 3 D models with a computer graphics simulation of projection and illumination. Given a single image of a person, the algorithm automatically estimates 3D shape, texture, and all relevant 3D scene parameters.

In this framework, rotations in depth or changes of illumination are very simple operations, and all poses and illuminations are covered by a single model. Illumination is not restricted to Lambertian reflection, but takes into account specular reflections and cast shadows, which have considerable influence on the appearance of human skin.

The percentage of correct identification based on side-view gallery, was 95% and the corresponding percentage on the FERET set, based on frontalview gallery images, along with the estimated head poses obtained from fitting, was 95.9%.

g) Line Edge Map (LEM)

Edge information is a useful object representation feature that is insensitive to illumination changes to certain extent. Though the edge map is widely used in various pattern recognition fields, it has been neglected in face recognition. Edge images of objects could be used for object recognition and to achieve similar accuracy as gray-level pictures. [10] made use of edge maps to measure the similarity of face images. A 92% accuracy was achieved. Takács argued that process of face recognition might start at a much earlier stage and edge images can be used for the recognition of faces without the involvement of high-level cognitive functions.

A Line Edge Map approach, proposed by [11], extracts lines from a face edge map as features. This approach can be considered as a combination of template matching and geometrical feature matching. The LEM approach not only possesses the advantages of feature-based approaches, such as invariance to illumination and low memory requirement, but also has the advantage of high recognition performance of template matching.

h) Support Vector Machine (SVM)

SVM is a learning technique that is considered an effective method for general purpose pattern recognition because of its high generalization performance without the need to add other knowledge. Intuitively, given a set of points belonging to two classes, a SVM finds the hyperplane that separates the largest possible fraction of points of the same class on the same side, while maximizing the distance from either class to the hyperplane. According to [12], this hyperplane is called Optimal Separating Hyperplane (OSH) which minimizes the risk of misclassifying not only the examples in the training set but also the unseen example of the test set.

The main characteristics of SVMs are: (1) that they minimize a formally proven upper bound on the generalization error; (2) that they work on high-dimensional feature spaces by means of a dual formulation in terms of kernels; (3) that the prediction is based on hyperplanes in these feature spaces, which may correspond to quite involved classification criteria on the input data; and (4) that outliers in the training data set can be handled by means of soft margins.

IV.HOW FERET USED AS AUTHURAIZATION?

Face recognition technology, As with any other computing system, it is imperative that cloud computers ensure that the individual attempting to access the system is authorized to do so.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A new methodology of authorizing access to the cloud currently being used is face recognition. Face recognition technology consists of the following aspects, user initialization, computer initialization, and the private matching identification part of cloud. Figure displays the user initialization process. In the user part of the identification process, the computer takes a picture of the individual attempting to access the system. It then identifies the part of the image that is the person‟s face, adjusts the lighting of the image, and greys the image out, converting each pixel‟s RGB color value to gray scale data. The grey scale data is transformed from the two-dimensional face image to a one-dimensional vector. This vector is then encrypted by means of Paillier encryption algorithm to protect the user‟s identity. In essence, Paillier encryption is a type of homomorphic encryption scheme, but is not fully homomorphic as there are limitations in the functions used to encrypt the data.

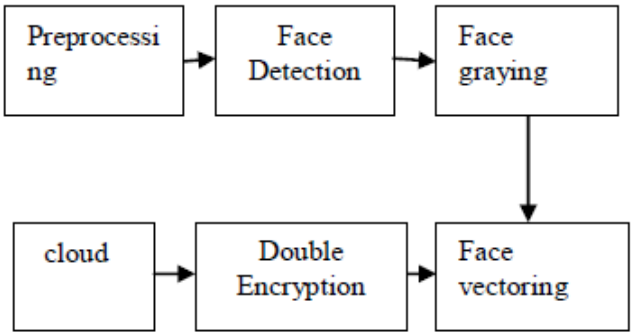

Figure 2

In the cloud initialization and private matching identification aspects of authentication, the computer then compares an individual‟s image to a database of predetermined authorized users. In order to do so, it maps the image of the face and compares it to the one‟s found in the database. In order for access to be approved, the key aspects of the taken picture must match the image that is stored in the date base within a predetermined deviation from the original [8]. If it does not, the individual is denied access and the system has effectively prevented unauthorized access to the cloud.

V.FUTURE WORK

We can use algorithm having higher recognition rate and has less computation complexity. And use that algoritham for authentication of cloud user which provide higher security to cloud.

VI.CONCLUSION

The utilization of Face Recognition technology would greatly compliment any security features already in place of the cloud. It is more reliable than biometrics or iris scanning means of authorization, as these two identification forms rely too heavily on hardware accuracy and consistency [8]. Face recognition technology is another means of identity verification in addition to an encrypted password that has the potential to be cracked or stolen. Implementing face recognition technology would help security considerably as those attempting to gain access to the cloud must have permission to do so. In effect, companies can track how long a user was using/accessing the cloud and validate their identity simultaneously. A real world application for this technology is large companies using it to ensure that lower level employees are not trying to obtain proprietary secrets to sell for profit. Face recognition technology is also applicable for the government‟s use. Using a private cloud, different branches of government can set specific levels of authorization for sensitive materials, only to viewed by authorized agents. The result of implementing this technology in the real world is a securer cloud environment[8]

REFERENCES

[1] Wang, H. Yan. (2010, December 12) “Study of Cloud Computing Security Based on Private Face Recognition” Beijing Institute of Technology.

[2] Mr. Ravindra Kumar Gupta, Ram Sagar Mishra. (2012,January) “SECURITY ON THE CLOUD”- A ReviewAvailable: http://www.ijater.com/Files/IJATER_02_09.pdf

[3] Danish jamil, hassan zaki(2011,apr) Security issues in cloud computing and countermeasures Available: http://www.ijest.info/docs/ijest11-03-04-235.pdf

[4] S. Tolba, A.H. El-Baz, and A.A. El-Harby (2006 february) Face Recognition: A Literature Review Available: https://www.waset.org/journals/ijice/v2/v2-2-14.pdf

[5] L. Sirovich and M. Kirby, “Low-Dimensional procedure for the characterisation of human faces,” J. Optical Soc. of Am., vol. 4, pp.519-524, 1987.

[6] M. Kirby and L. Sirovich, “Application of the Karhunen- Loève procedure for the characterisation of human faces,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 12, pp. 831-835, Dec.1990.

[7] P. Verlinde, G. Matre, and E. Mayoraz, “Decision fusion using a multilinear classifier,” Proc. Int’l Conf. Multisource-Multisensor Information Fusion, vol. 1, pp. 47-53, July 1998.

[8] T.J. Stonham, “Practical face recognition and verification with WISARD,” Aspects of Face Processing, pp. 426-441, 1984.

[9] K.K. Sung and T. Poggio, “Learning human face detection in cluttered scenes,” Computer Analysis of Image and patterns, pp. 432-439, 1995.

[10] S. Lawrence, C.L. Giles, A.C. Tsoi, and A.D. Back, “Face recognition: A convolutional neural-network approach,” IEEE Trans. Neural Networks, vol. 8, pp. 98-113, 1997.

[11] Takács, “Comparing face images using the modified hausdorff distance,” Pattern Recognition, vol. 31, pp. 1873-1881, 1998.

[12] Y. Gao and K.H. Leung, “Face recognition using line edge map,” IEEE [54] T. Vetter and T. Poggio, "Linear object classes and image synthesis from a single example image," IEEE Trans. Pattern Analysis and Machin Intelligence, Vol. 19, no. 7, pp. 733-742, July 1997.

[13] L. Wiskott and C. von der Malsburg, “Recognizing faces by dynamic link matching,” Neuroimage, vol. 4, pp. 514-518, 1996. Transactions on Pattern Analysis and Machine Intelligence, vol. 24,no. 6, June 2002.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)