3-Step User Authentication in Cloud Environment

Aprajita Srivastava[1,1], Somya Goel[1], Aayushi Tyagi[1] and Rachna Jain[1]

Abstract-Cloud computing technology is growing rapidly in the market. It allows users to access their files and data from any place using internet. However, the privacy and the security of user's information is progressively challenged. The user must be authenticated before every access to data or services; his/her identity must be authorized. So, in this paper, we propose layering of security settings, i.e. providing more than one level of authentication to ensure the security. We will discuss about three layers of security which will be password protection, voice recognition and then face recognition. Only after passing through these security layers, the user will be allowed to access the data or services from cloud server. We will use the concept of session key for password protection i.e. a specific session key will be allocated to the user upon each login cycle and after a prescribed time user is logged of by the system itself. Then we will use voice recognition in which the audio signal will be converted into digital form and then sent to the neural network which will identify the voice. Third will be face recognition in which we have used principal component analysis (PCA) algorithm.

Keywords-cloud computing, face recognition, password protection, speech recognition

1.Introduction

Cloud computing is emerging at a fast rate nowadays. Cloud computing is a technology in which we deliver information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server. Instead of keeping files on a hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. [14]. Many companies have opted for it since it is flexible and helps in reducing the cost. But it has some major disadvantages too. The biggest problem with which we are dealing in this sector is its security. Many steps have been taken by cloud service providers in order to secure the data but in some cases these steps are not enough. [9]

So, in order to make it more secured we have worked on providing more layers of protection so that the access becomes difficult for the people who are not authorized to access the particular data. The layers are in a way in which the user has to go through all the layers of security and when he/she will be authorized by all the layers of security only then he/she will get the access to data/services. We have worked on 3 layers of security which are:

- **Password Protection**: This is our first layer of security which is the most common and effective method. In this step we will assign a specific session key to the user upon each login cycle and after a prescribed time user is logged off by the system itself.
- **Voice Recognition**: This is our second layer of security. In this step we will represent the voice in spectral density form using sampling. Then we will send this signal to neural network that learns and predicts the features of each word.
- **Face Recognition**: This is our final layer of protection. In this step we will use principal component analysis (PCA) algorithm which is a statistical procedure that converts set of related variables into a set of unrelated variables called the principal components.

[1] Please note that the LNCS Editorial assumes that all authors have used the western naming convention, with given names preceding surnames. This determines the structure of the names in the running heads and the author index.

All the three mentioned layers of security are used to provide additional protection of data in cloud computing. These layers are further explained in detail.

2.Literature Survey

In the field of cloud computing and machine learning a lot of research has been done. The research takes upon various fields like security in the field of cloud, it leads to the important area of authentication of a user. Various authors have looked upon these fields, many of whom have been successful in their findings.

Alex Graves et al in 2006 [1] talked about speech recognition using recurrent neural networks. It deals with variable length audio and uses the same for better recognition. Collobert et al in 2008 [2] describes neural network architecture which at the end uses voice recognition, it uses a small part of the speech or a few phrases and then making sure the sentence makes sense is important in this architecture framework. It also uses multitasking and sharing of tasks into account. Marqu´es et al in 2010 [3] emphasized on the different face recognition algorithms that are useful for the detection of the user's face and utilized for authentication like PCA, LDA etc. Wang et al in 2010 [4] proposed a model that looks in to the user's face initialization and matched it with the one specified in the cloud. This method ensured cloud didn't store the faces and even while matching the data remained private. It dealt with private face recognition. Choudhury et al in 2011 [5] told all about session key management and a strong authentication framework was proposed. Password security was looked in closely and the various remedies were suggested. El-Sayad et al in 2013 [6] was designed for a specific system i.e. essentially electronic voting system. It looked in to the faces in the database and put into force an algorithm to match the faces of the user with the ones entered into the database. It was highly successful and is hence a good option to use in this field. Hashizume et al in 2013 [7] lay out the various security concerns in cloud like privacy, accessibility, accountability and worked upon correcting them. Pawle et al in 2013 [8] elaborated about the traditional and biometric techniques that are used in cloud computing. It talks about iris recognition, facial recognition, fingerprint recognition, password protection etc. Geitgey et al was interested in machine learning and dig deep into the concept of speech recognition. Ng et al linked neural networks to Google's project and voice recognition was researched in deep contemplation by him.

The authentication in cloud is an active procedure which requires a lot of thought and as many the stages better is the result so we suggest our own model based on all the research undergone by us.

3.Authentication Procedure

The authentication in cloud is a very important concept and needs to take a few risks and factors in mind when performing the same. Security is obviously the biggest issue in the field of cloud.

Authentication in cloud is based on the following traits:

A) Knowledge possessed by the user.
B) Biometric factors influencing the security like voice, face, fingerprint recognition etc. [7]

The three stages we propose for our model is using Password Protection and Biometric techniques like – i) Voice recognition and ii) Face recognition.

3.1 Password Protection

Password protection is the most traditional way to access any account and can be used as a layer of security for cloud computing. Password change method is flexible and user can change it in case they forget it or the account gets hacked. It is a method which has a no. of risks associated with it. [8] However, there are ways in which we can handle these attacks efficiently. One prominent way is to use a **session key**. [5]

*The concept of **session key** is the primary basis we define while performing password protecting schemes. A specific session key is assigned to a user upon each Login cycle and eventually after a prescribed time the user is logged off by the system itself. This is a very useful and good technique to go about when dealing with attacks on the account.[5]* The various attacks are as follows and they can be tackled using the given ways -

a) ***Password guessing attack*** **-** Guessing password is the most common attack that can happen on a system. Hence, we use a complex term with a hash function as the basis, it helps in curbing this attack and gives the account better protection.

b) ***Phishing attack*** – Phishing uses user details like username, password and security questions to get into the account and hack the same. However only a genuine user can verify all 3 steps.

c) ***User privacy*** – Privacy of the data of a user is of extreme importance so we use encryption techniques and do not send the data in raw form, we transmit it as codes.

d) ***Replay attack*** – A user's data is fraudulently repeated and hence we need to tackle this. The password is protected by the concept of session key so we can rest assured that this attack will never arise as the session key will expire after a stipulated amount of time.

e) ***Man in the middle attack*** – Again in this type of attack the hacker knows some of the schemes required to work through but he doesn't know the hash function and encryption data sent by the session key for that session. Hence this attack is highly unlikely to occur.

f) ***Impersonation attack*** – This attack occurs if some person steals our details like our credit card credentials. It can be compared to an example like some person stealing our mobile phone and using all our personal data in a malicious way. It can be protected by hashing the data appropriately.

These are some of the attacks and ways to reduce them. The basis we advocate in the first stage of our authentication is to assign a session key, use it with encryption and hash functions to the best of our abilities. Still relying only on password protection is not advisable.

That's why we use biometric techniques which are difficult to surpass. Voice and Face recognition techniques are the second and third stages discussed in our model.

3.2 Speech Recognition

Speech recognition is the capacity of a machine or program to identify words and phrases in spoken language and transform them to a machine-readable format. It can be viewed as a pattern recognition problem where we desire each unique sound to be distinguishable from all other sounds. Speech recognition is a powerful way to provide security for the data placed on the cloud. Andrew Yan-Tak Ng [10] while working on the Google Brain [11] project using very large scale artificial neural networks, predicated that the speech recognition shall become incredibly useful when it attains the accuracy of 99%. Thankfully we are now reaching that target resulting in Voice recognition, a form of biometric software, that is more secure form of cloud data protection because our voices are unique. The speech recognition uses a neural network that is shown in Fig. 1.

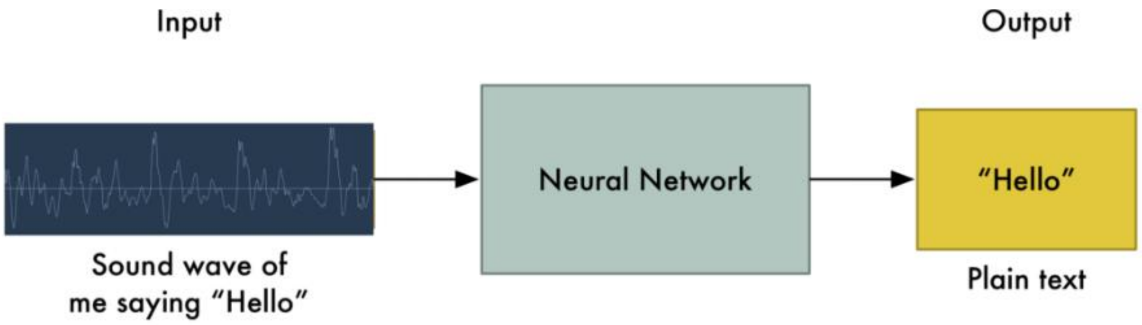


Fig.1. Block diagram for speech recognition using neural network

Theory of Speech recognition

The speech produces the audio wave which is sampled to convert to digital form. “CD Quality” audio is sampled at 44.1khz. But for speech identification, a sampling rate of 16khz (16,000 samples per second) is sufficient to cover the frequency range of human speech.

The sampled data needs pre-processing before feeding to the neural network. To make this data easier for a neural network to process, the complex sound wave is broken into its component parts, namely. low-pitched parts, the next-lowest-pitched-parts, and so on. Then by adding up how much energy is in each of those frequency bands (from low to high), a fingerprint of sorts for this audio snippet is created which is fed to the neural network. A recurrent neural network (RNN)ends up with a mapping of each audio chunk to the letters most likely spoken during that chunk [9]. Neural network has a memory that influences future predictions. Memory of previous predictions helps the neural network make more accurate predictions going forward.

Algorithm

The algorithm used above to deal with variable-length audio is called Connectionist Temporal Classification or CTC [1][12]. It obviates the need for pre-segmented data, and allows the network to be trained directly for sequence labelling.

Neural Network (NN) architecture

A NN automatically learns features for the desired task in the deep layers of its architecture. The deepest layer (consisting of lookup-tables) implicitly learns relevant features for each word in the dictionary. While training NNs on associated tasks, dividing deep layers in these NNs enhances features created by these deep layers, and thus enhance generalization performance. The last layers of the network are specific to the task [2]. Fig. 2 shows the architecture of working of RNN. Fig 3 shows deep multi-tasking with NN. Task 1 and Task 2 are two tasks trained by the architecture. One lookup-table (in black) is shared. The other lookup-tables and layers are task specific.

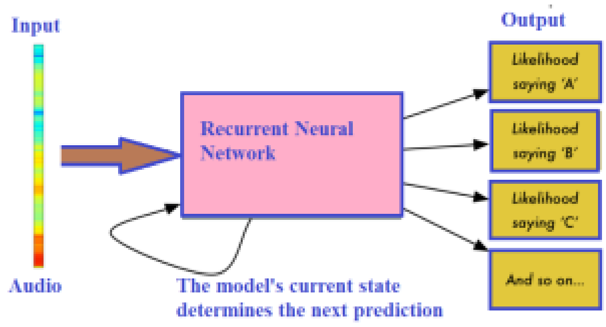
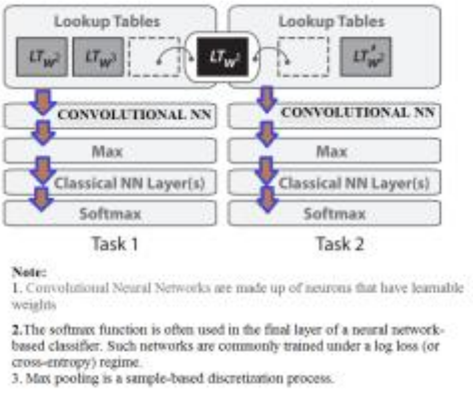


Fig. 2 Prediction by RNN for the speech recognition



Note:
1. Convolutional Neural Networks are made up of neurons that have learnable weights
2.The softmax function is often used in the final layer of a neural network-based classifier. Such networks are commonly trained under a log loss (or cross-entropy) regime.
3. Max pooling is a sample-based discretization process.

Fig. 3 Deep multi-tasking with NN

3.3 Facial Recognition

The human face plays an important role in how we interact with the world. It is one of the preferred way of biometrics because of its ease of implementation. This method does not come with many drawbacks as it is non-intrusive and also does not require a complex hardware system. The users can easily click a photo with their phone’s camera or a webcam while registering for an account. [4] While logging in, the camera will detect the users face and match it with the existing database of the system. The user will be allowed access only once their face will match with the one in the database. This layer provides an added security in a cloud system where user anomaly is the biggest security issue. [3][6]

The two most important components for facial recognition would be: -

1. Facial verification,
2. Facial identification

The difference between the two can be understood from the diagram given below.

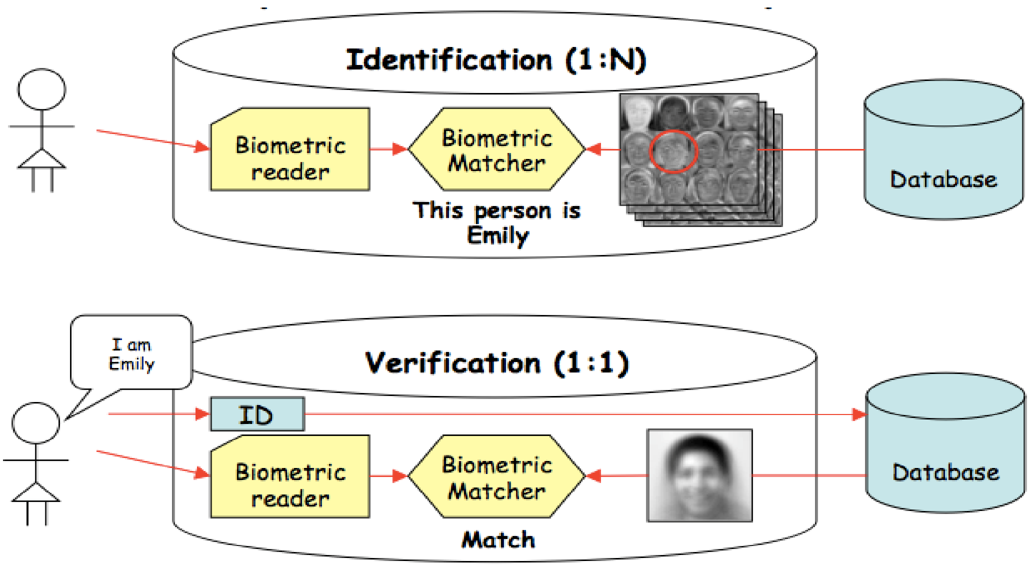


Fig 4 Difference between facial identification and facial verification

There are various number of algorithms that can be used for the purpose of facial recognition. These include PCA(Principal Component Analysis) algorithm, LDA(Linear Discriminant Analysis),Fisherfaces, LPB(Local Binary Patterns) and FTC (Facial Trait code). [3]

After thorough analysis of all these techniques, we made the following comparison: -

	FACTORS->	Good Performance	Ease of implementation	Less time consuming
ALGORITHMS				
1.	PCA	Yes	Yes	Yes
2.	LDA	yes	Yes	Yes
3.	Fisherfaces	No	No	No
4.	LBP	Yes	Yes	No
5.	FTC	Yes	Yes	No

Table 1 Comparison among different algorithms used in facial recognition

So, after thorough comparison, we were left with PCA and LDA to work in our application. But PCA, which is an “unsupervised” learning algorithm tends to outperform LDA when it comes to smaller databases. So, we have chosen PCA as our algorithm for facial recognition in our proposal.

PCA algorithm

It is a mathematical procedure that performs dimensionality reduction by extracting the principal components of multidimensional data. [13]

Our task of recognizing the user’s face and then matching it with images in the database to give him access to account contains some modules.

Modules are basically small parts of the system we are trying to build.

Different modules -

1. Adding image (while registration)
   ->Includes capturing image from a web camera and then storing it in our system.

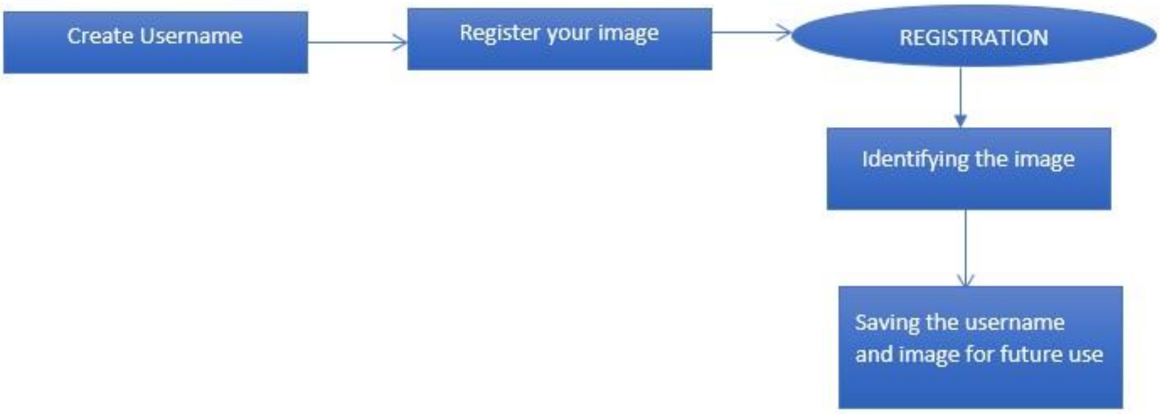


Fig 5 Addition of Image

2. Login
   ->Compares captured image with stored images in the system.

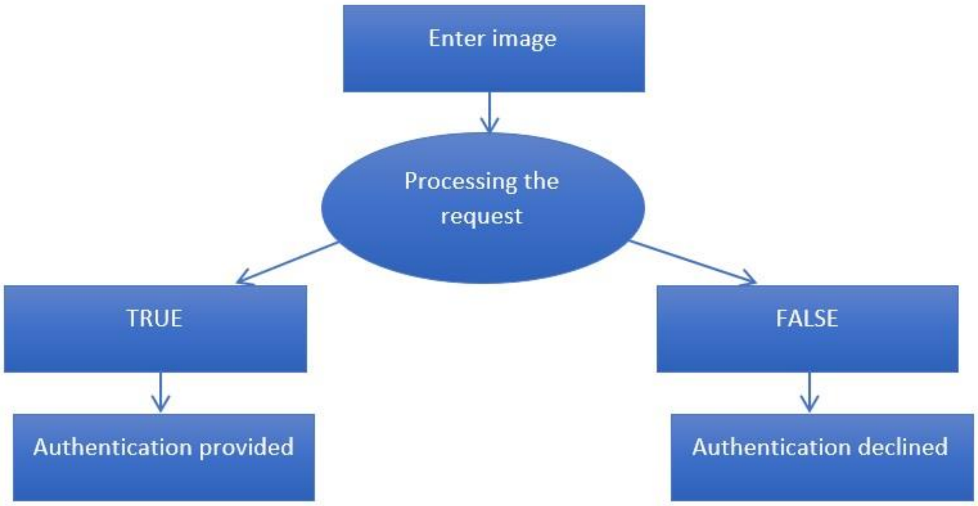


Fig 6 Comparison of captured images

3. Eigenface Computation

   ->used to compute face space used for face recognition.

   -> Steps involved:

   a) Computing an average face matrix.

   b) Building a covariance matrix.

   c) Computing eigenvalues and eigenvector.

   d) Computing faces using eigenvectors.

e.) Computing eigenspace for our given images.

4. Identification

->takes image and compares it with existing images in the database. If the image is matched, success message is shown to the user.

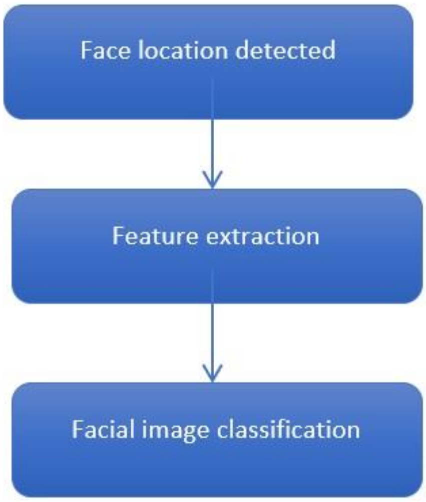


Fig.7 Stages of face recognition

4.Conclusion

The services of cloud are majorly dependent on data sharing so security is a major concern to identify authorized user, secure authentication is necessary in cloud computing. To ensure that the data security is maintained, we have added 3 layers in our process for user login. Step-1 is entering your textual password after which a session key will be generated which will be active for a stipulated period of time after which the session expires. Step-2 is voice recognition. We will enter a sample of our voice by saying a phrase or a word, which will then be matched with the voices in our database system. Step-3 in our process, added as an extra security layer is face recognition. The user, while registering for an account will capture his image using a camera and it will be stored in the system. When he tries logging in, he will have to use his camera to capture his image again and once matched with the one in the system, will provide him access to his cloud account. The security level of cloud provider in terms of secure authentication is much improved by using face recognition system.

References

[1] Alex Graves et al, "Connectionist Temporal Classification: Labelling Unsegmented Sequence Data with Recurrent Neural Networks", http://www.cs.toronto.edu/~graves/icml_2006.pdf

[2] Collobert, R. and Weston, J., 2008, July. A unified architecture for natural language processing: Deep neural networks with multitask learning. In *Proceedings of the 25th international conference on Machine learning* (pp. 160-167). ACM.

[3] Face Recognition Algorithms - Proyecto Fin de Carrera June 16, 2010 Ion Marqu´es

[4] Wang, C. and Yan, H., 2010, December. Study of cloud computing security based on private face recognition. In *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on* (pp. 1-5). IEEE.

[5] Choudhury, A.J., Kumar, P., Sain, M., Lim, H. and Jae-Lee, H., 2011, December. A strong user authentication framework for cloud computing. In *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific* (pp. 110-115). IEEE.

[6] El-Sayad, N.E., Abdel-Kader, R.F. and Marie, M.I., 2013. Face Recognition as an Authentication Technique in Electronic Voting. *Editorial Preface*, *4*(6).

[7] Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B., 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), p.5.

[8] Pawle, A.A. and Pawar, V.P., 2013. Face recognition system (FRS) on cloud computing for user authentication. *International Journal of Soft Computing and Engineering (IJSCE)*, *3*(4).

[9] Adam Geitgey, “Machine learning is Fun!”, https://medium.com/@ageitgey/machine-learning-is-fun-80ea3ec3c471

[10] Andrew Yan-Tak Ng, Wikipedia, https://www.wikiwand.com/en/Andrew_Ng

[11] Google Brain, Wikipedia, https://www.wikiwand.com/en/Google_Brain

[12] Adam Coates, https://www.youtube.com/watch?v=9dXiAecyJrY&feature=youtu.be&t=13874

[13] https://www.slideshare.net/LaxmanaRao436/face-recognition-and-detection-by-pca-algorithm

[14] http://www.investopedia.com/terms/c/cloud-computing.asp