



A Hierarchical framework of Cloud Computing using Heart beat as Biometric

Vinithra Babu

Prof. Khaled M. Elleithy, Ph.D.

Department of Computer Science University of Bridgeport, Bridgeport , CT

ABSTRACT :

Cloud computing is the technique which is mainly used to create a cloud space. These cloud spaces that are created by the user, can store files and also can upload and download information. So in this paper we will be mainly discussing about the security purpose that we are going to use in this project. Till now we have used the biometric security methods like face recognition, finger print and so on.. But in this project what we will be discussing about it is a combination of two or more biometrics. We fuse ECG and Palm print for achieving the multi modal system. Moreover we take the heartbeat of the human being as the main biometric. So here we will be also discussing about few algorithms and methods in this topic. The two signals that we consider are Electrocardiogram and Phonocardiogram. When these two signals combine together we will be able to run the multimodal system. The ECG purpose is to record the signal frequency of the heart and store them in the database. This is done because for the user authentication purpose. The usage of PCG is to record the sound made by the heart, that is nothing but the sound of the heartbeat. There are also few complications in this model, because it is not that easy to show as a real time model. All the templates has to be stored in the database, only then the user will be able to authenticate. Considering in all this the basic challenge is the time dependency, this is because the authentication has to be done in a timely manner.

INTRODUCTION:

Cloud computing seems to be the simplest concept, but a huge variation are present in it. So initially if we want to get registered in the cloud space we need to know some basic instructions. The first thing is if a person wants to register in the cloud domain he will be providing his details. Once he is done with that then according to his usage he will be getting the space. Then he can upload and download all kinds of files that he needs. Once he has done with this, then next thing come the security purpose. Cloud computing is the only technology that can communicate with any type of virtual or real time methods. In general, cloud computing is the distribution of network where they have the access to communicate within the network area. All these network devices are served up by the virtual hardware devices which appear to be the real one, but actually they are not. The Cloud Computing mainly concentrates on the fields like reliability, confidentiality and security. During the network, each performs a different function and used for different purposes

PROBLEM IDENTIFICATION:

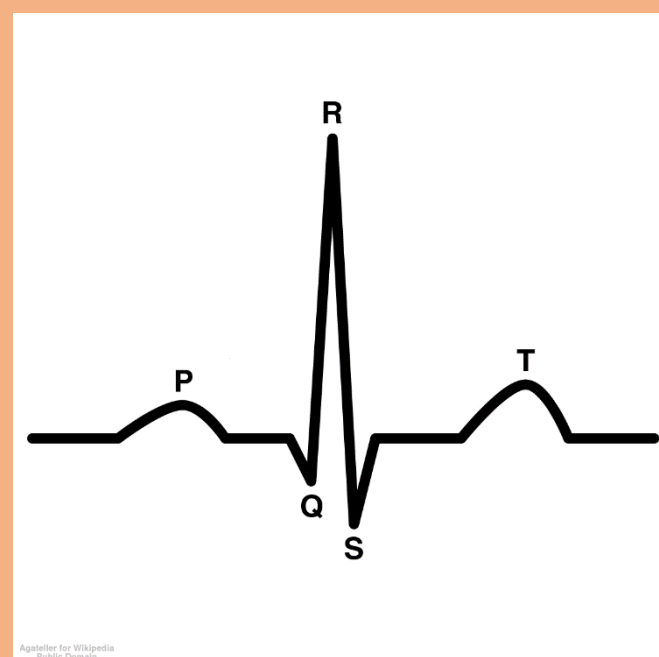
The purpose of this development is to provide secured space so that the user can store all his information in the cloud area. This project is not only regarding the storage but also about the security purpose which also been added along with it. The main consideration in developing this project is to protect the information in the cloud. For this we use the heartbeat signal as the security purpose. The signal and frequency are combined and they are sent as an input. So the reason for using the heartbeat as the biometric is to reduce the forgery and also to minimize intrusion. So as we know it is the combination of two or more biometric that we use. When we use this multimodal system specification there are possible chances that the accuracy of the system might be more difficult to enhance it.

PROPOSED SOLUTION:

The system becomes less accurate when there is only one behavioral or physiological feature to be evaluated this is one of the major drawback of using the single biometric system so in order to overcome this disadvantage a fusion of two or more biometrics techniques is needed to increase the system performance .multimodal systems also provide anti spoofing in order to avoid the situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage so it is difficult for the intruder of spoof biometrics simultaneously thus detection of heart beat is a important step in the process of designing high security system this is because a template signal has to be sufficiently descriptive of the intra class variability in order for the system to perform robust matching the discrete wavelet transform is chosen for preprocessing of the signal because it provides dual functionality using maxima lines information that is obtained from the discrete wavelet transformation coefficients thereby allowing noise reduction

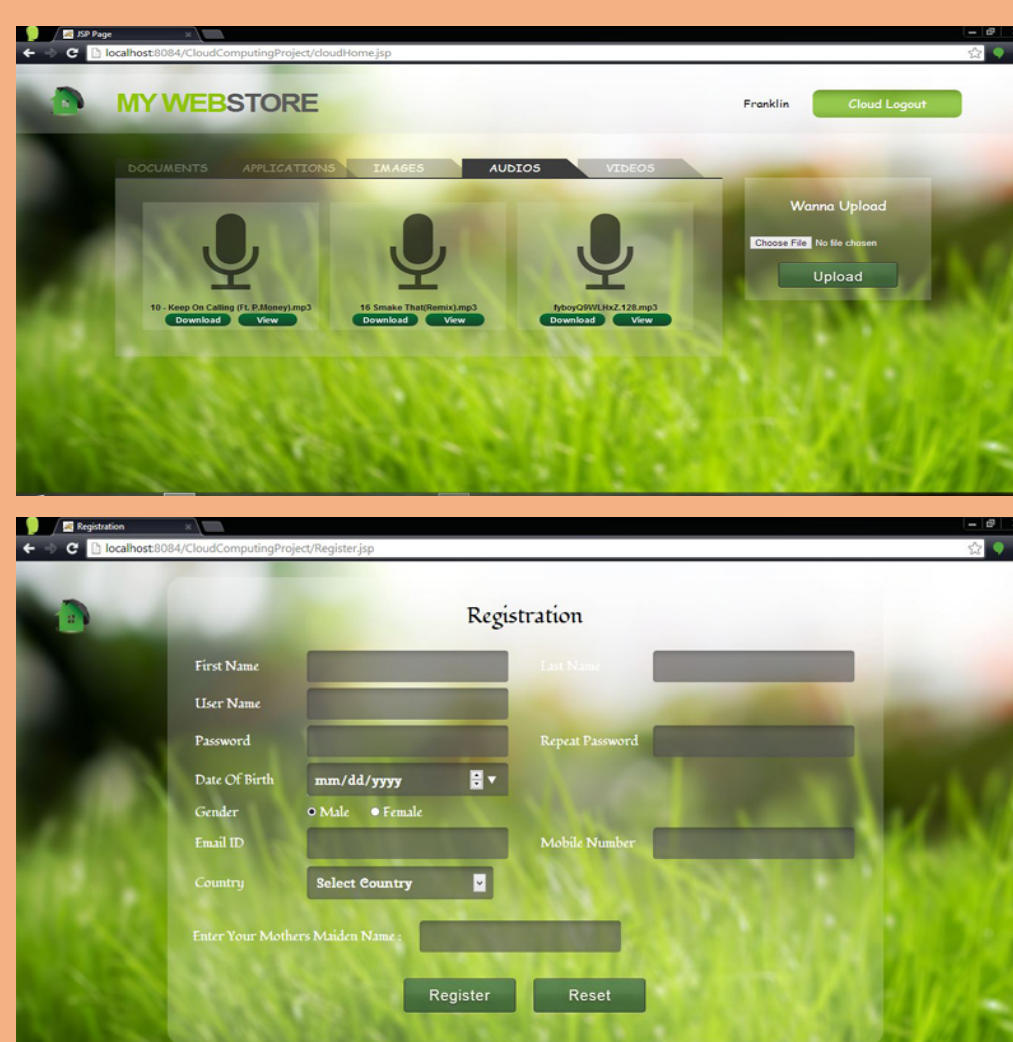
RELATED WORK:

The electrical activity of heart is captured using ECG. With each heartbeat, an electrical signal moves from the top of the heart to the bottom. An ECG machine records this electrical signal from the heart and is interpreted. A normal ECG tracings includes waveform components which indicate electrical events during one heartbeat. These waveforms are labelled P, Q, R, S, T and U. P wave is the first short upward movement of the tracing. The QRS complex, normally begins with a downward deflection, Q; a larger upwards deflection, a peak (R); and then a downwards S wave. The QRS complex represents ventricular depolarization and contraction. The PR interval indicates the transit time for the electrical signal T wave is normally a modest upwards waveform PCG is used to record the sounds and murmurs made by the heart using the machine called phonocardiograph. A wave like oscillation is said to be wavelet which begins at amplitude zero, increases then decreases back to zero. It can be used in seismograph and heart monitor. As a mathematical tool wavelet is used to extract data from different kind's majorly audio signals and images. Thus the result processed from above is stored in the database of the cloud storage. Anti-spoofing is done so that no attacker can forge the source address of a packet so that the security level is raised to the next step. Checkpoint verifies the source address of every packet relating it to the topology of network. Whenever a user tries to authenticate himself the signals are processed in the same procedure defined above and is authenticated.



SIMULATIONS:

The simulation for this project is complicated and we need special requirements for implementing in the real time. So in this project we show the outputs in the form of simulations. The first comes the registration page followed by the cloud home page. Then next comes the files like audio, video, documents and photos. The authentication part is the main point here. The heartbeat of the normal human being, which is stored in the database, backend process.



The above is the registration page, this is for the first time user. Once they have registered with the cloud, then the following simulation shows the files in the cloud. As said before as the authentication process is complicated, it is not possible to show in the real time process. But still we will be showing the process of working.

ALGORITHM AND METHODS:

In this project it doesn't include much calculation part, because we will be working on the signal and frequency. And it is stored in the database. But some algorithms and method are involved. The first one is the Mel Frequency Cepstral Coefficients, It is a representation of short power spectrum of a sound based on a linear cosine transform of frequency. They are used to recognize the sound of the heartbeat. Also used in audio similarity measures. Next method is the, Wavelet based analysis, It is a wave like oscillation with an amplitude that begins with zero, increases, and then decreases back to zero. It is just used in signal processing and signal analysis. We will just sample a particular frequencies of heart beat that is used for authentication purpose. Finally come the anti-spoofing method, is a technique for identifying and dropping packets that have a false source address. So if the user authentication is not been identified then it is not possible to get into the cloud space.

CONCLUSION:

This project completely describes about the heartbeat authentication. As it is less user friendly, the real time usage is quite complicated in this case. But in future this security method will be the more used one. The enhancement is used in the military purpose and also for the business dealers in the international level. The cloud storage provides the user for the better resource allocation. The ECG and PCG are the two methods which are used, but in the future there are possible chances of advanced methodologies.

REFERENCE:

- [1] B. Abrahao, V. Almeida, J. Almeida, A. Zhang, D. Beyer, and F. Safai, "Self-Adaptive SLA-Driven Capacity Management for Internet Services," Proc. IEEE/IFIP 10th Network Operations and Management Symp. (NOMS '06), 2006.
- [2] C. Adam and R. Stadler, "Service Middleware for Self-Managing Large-Scale Systems," IEEE Trans. Network and Service Management, vol. 4, no. 3, pp. 50-64, Dec. 2007.
- [3] B. Addis, D. Ardagna, B. Panicucci, and L. Zhang, "Autonomic Management of Cloud Service Centers with Availability Guarantees," Proc. IEEE Third Int'l Conf. Cloud Computing (CLOUD),2010.
- [4] J. Almeida, V. Almeida, D. Ardagna, I. Cunha, C. Francelanci, and M. Trubian, "Joint Admission Control and Resource Allocation in Virtualized Servers," J. Parallel and Distributed Computing, vol. 70,no. 4, pp. 344-362, 2010.
- [5] Amazon, Inc., "Amazon Elastic Cloud," <http://aws.amazon.com/ec2/>, 2013.
- [6] Amazon, Inc., "AWS Elastic Beanstalk," <http://aws.amazon.com/elasticbeanstalk/>, 2013.
- [7] D. Ardagna, S. Casolari, M. Colajanni, and B. Panicucci, "Dual Time-Scale Distributed Capacity Allocation and Load Redirect Algorithms for Cloud Systems," J. Parallel and Distributed Computing, vol. 72, no. 6, pp. 796-808, 2012.