International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-3, Issue-4, September 2013

Face Recognition System (FRS) on Cloud Computing for User Authentication

Akshay A. Pawle, Vrushsen P. Pawar

Abstract – Cloud computing is a new technology in the market. In cloud computing user can access their files or data from anyplace using internet. There are several benefits of cloud computing like increase throughput, reduce costs, improve accessibility and requires less training but on the other hand it has some security issues. In that, identifying authorized user is a major issue. The user wanting to access the data or services needs to be registered and before every access to data or services; his/her identity must be authenticated for authorization. There are several authentication techniques including traditional and biometric but has some drawbacks. In this paper, we proposed new face recognition system (FRS) which overcome all drawbacks of traditional and other biometric authentication techniques and enables only authorized users to access data or services from cloud server.

Index Terms – Authorized User, Cloud Computing, Face recognition system, Throughput

I. INTRODUCTION

Cloud computing is currently one the most hyped IT innovation [1]. Cloud computing technology is a new concept, which provides great opportunities in many areas. Cloud computing is a collection of computers and servers that are publically accessible via internet [2]. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing provides the variety of internet based on demand services like software, hardware, server, infrastructure and data storage [3].

A. Benefits of Cloud Computing

1) Increase throughput – Cloud computing get more work done in less time with less people.
2) Reduce costs – In cloud computing, user shares computer hardware, software and data so there's no need to spend money on hardware or software.
3) Improve accessibility – In cloud computing user can access data, files anytime from anywhere via internet.
4) Requires Less Training – Cloud computing takes fewer people to do more work. So there is requirement of minimum training of hardware, software problems to user.

Manuscript received September 2013.
Akshay A. Pawle, College of Computer Science and Information Technology, Latur, SRTM University, Nanded, India.
Dr. Vrushsen P. Pawar, Department of computational studies, Swami Ramanand Teerth Marathwada University, Nanded, India.

National Institute of Standard and Technology (NIST) describes cloud computing with five essential characteristics such as on-demand self-service, broad network access, rapid elasticity, measured service, and resource pooling, three service models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) and also four deployment models such as public, private, community, and hybrid [4].

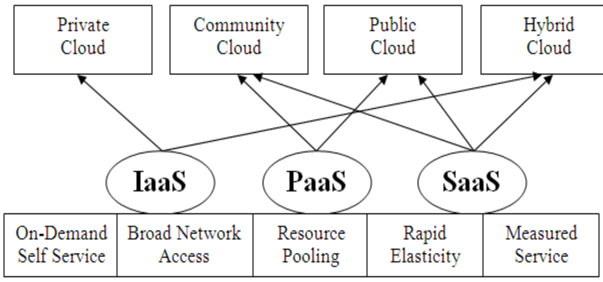


Fig. 1 Cloud Structure

B. Characteristics

1) On-demand self-service – Cloud provides all needed computing resources as per requirement to user.
2) Broad network access – User can access cloud services using desktop, laptop, mobile phone etc. over the internet.
3) Resource pooling – Cloud provider schedules resources to the user as per their requirement.
4) Rapid elasticity – Cloud computing has ability to quickly allocate and de-allocate the services as per requirement.
5) Measured service – Cloud providers controlling on usage of resources.

C. Services

1) Software as a Service (SaaS) – In the SaaS model, cloud provider delivers application softwares like MS-OFFICE, Turbo C etc. as a service to cloud user.
2) Platform as a service (PaaS) – In PaaS model, cloud provider deliver a computing platform like operating system, database, web server etc. to the cloud user.
3) Infrastructure as a Service (IaaS) – Main objective of any company is to reduce time and money. IaaS model is used to fulfill these primary objectives.

D. Models

1) Public – This type of cloud model available for all users.
2) Private – This type of cloud model specifically applicable only for private company.
3) Community – This type of cloud model is shared by several companies and supports to a specific community.
4) Hybrid – This type of cloud model is a combination of two or more clouds.

According to international data corporation (IDC), there are several issues or challenges in cloud computing like security, availability, performance, on demand payment model may cost more, lack of interoperability standards, bringing back in-house may be difficult, how to integrate with in-house IT, and not enough ability to customize. According to the IDC's survey on the cloud services, security concerns are number one issue facing cloud computing [6]. To remove security issues specifically to identify authorized user, we proposed a new biometric authentication system called as face recognition system (FRS).

II. LITERATURE SURVEY

Now a days, cloud computing becomes more popular technology. For authenticate authorized user in cloud computing using face recognition system, we have survey some existing authentication schemes. At first, in cloud computing traditional username and textual password is used. But these are very easy to hack. Some systems have proposed graphical and 3D password but it requires more space and time consuming process. One of the authentication technique suggested by Ganesh Gujar, Shubhangi Sapkal, and Mahesh Korade called STEP-2 user authentication. In this, when user login through username and password then STEP-2 system generate token from hash table and sends to the registered email id. User must enter that token value as password within session time. So only if login is successful then user can access cloud services. But, token based systems are expensive and it is not guarantee that email will deliver on time due to the network failure and if session time is expired that token also get expired. Vishal Paranjape and Vimmi Pandey have proposed, authentication based on sending the password through SMS. But, it doesn't guarantee to deliver the SMS on time due to many reasons like network problem, cell problem etc. Some authors proposed to use SSL authentication protocol (SAP) for authentication but it low efficient.

So after review of all above mentioned authentication techniques, in this paper we have proposed Face Recognition System (FRS) which is based on biometrics characteristics of user for proper authentication in cloud computing,

III. AUTHENTICATION IN CLOUD

As cloud users store their information to various services across the Internet, it can be accessible by unauthorized people [5]. So security is the most important issue in cloud computing. To provide security we require proper authentication technique in cloud computing. Typically, authentication is done based on information about one or more of the following: i. Knowledge of the subject, such as password or secret information. ii. Possession of the user, such as smart card, passport, driver's license, etc. iii. Biometric traits of the client, such as fingerprint, voice, iris, etc. [7].

The data leakage and security attacks can be caused by insufficient authentication [8]. 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.

A. Traditional Authentication Techniques

1) Password – A login and password combination is the most universally used method of authentication but it is not secured [9]. It is very easy to hack by tools.
2) OTP – OTP is a One Time Password wherein password is provided upon request. An OTP can prevent a password from being stolen and reused [10]. This password is valid for a limited period of time and can only be used once. These systems are expensive.

B. Biometrics Authentication Techniques

Biometrics is most widely used security system now-a-days. It is helping to overcome a lot of drawbacks of above mentioned techniques of authentication. Biometrics can be defined as an automated methodology to uniquely identify humans using their behavioral or physiological characteristics [11].

That is biometrics is used as an authentication wherein the password is human organs or physiological characteristics. There are several biometrics techniques as stated below,
1) Voice Recognition – As the name suggests voice recognition involves authentication with respect to vocal data. Voice recognition is used to authenticate user's identity based on patterns of voice pitch and speech style. But a user's voice can be easily recorded and may use by unauthorized user. Also voice of a user may change due to sickness, so making identification is difficult.
2) Signature Recognition – Signature recognition is used to authenticate user's identity based on the traits of their unique signature. People may not always sign in a consistent manner so verifying an authorized user is difficult.
3) Retinal Recognition – Retinal recognition is for identifying people by the pattern of blood vessels on the retina. But this technique is very intrusive and expensive.
4) Iris Recognition – Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. As like retina this technique is also intrusive and expensive.
5) Fingerprint Recognition – Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. The dryness of fingers, soiled fingers can affect the system and it can show error.
6) Hand Geometry Recognition – Hand Geometry biometrics is based on the geometric shape of the hand. It includes the size of the palm, length and width of the fingers etc. But this technique has some drawbacks like not ideal for children as with increasing age there hand geometry tend to change, constant use of jewellery will result into change in hand geometry, not valid for persons suffering from arthritis, since they are not able to put the hand on the scanner properly.
7) Palm recognition – Palm recognition is based on ridges, principal lines and wrinkles on the surface of the palm. This technique is very expensive and not appropriate for children as there lines of palm change once they are fully grown up.

All the above techniques tend to tell us that none of it is feasible & not much useful due to its various drawbacks. To overcome drawbacks of all these security techniques and to provide proper security for user authentication in cloud computing, we proposed to use a biometric technique called *"FACE RECOGNITION".*

The human face plays an important role in our social interaction. Facial recognition is one of the preferred methods of biometrics because it is a neutral, non-intrusive, easy-to-use, which requires minimal physical contact as compared with other biometrics systems.

Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips, and chin or on the overall analysis of the face image that represent a face as a number of recognized faces [12]. Face image can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person.

Face Recognition System (FRS) enables only authorized users to access data from cloud server.

IV. ARCHITECTURE OF FACE RECOGNITION SYSTEM

Face recognition is a biometric security system. As the name suggests the face acts as a password for the systems. Face recognition security system is shown in the figure 2. Where, we proposed authentication scheme using face recognition system (FRS).

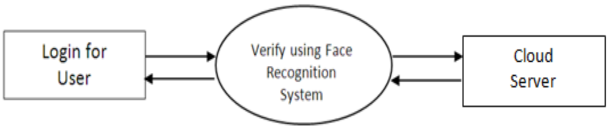


Fig. 2 System Architecture

As the diagram explains we have login option for the user after which the verification is conducted using face of the person. Detailed architecture is explained below.

A. Phases of Face Recognition System (FRS)

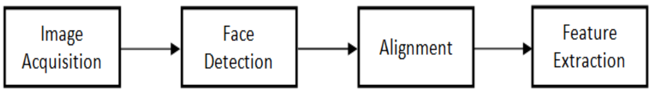


Fig. 3 Face Recognition System (FRS)

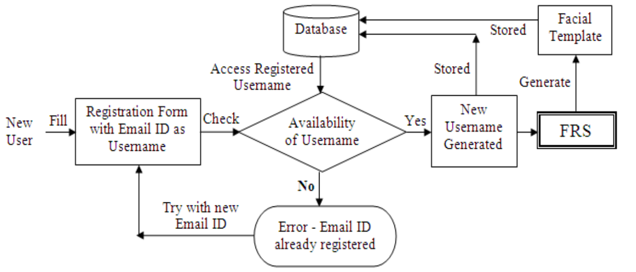
Now let us elaborate each phase in detail and understand it.

1) Image Capture – It is the step where image of the person is captured wherein his or her face is visible. In case of 2D facial recognition, a digital camera with normal resolution is needed.
2) Face Detection – Face detection involves identifying the face in the captured image. In simple words only the face of the person is seized & all other parts of the images are eliminated.
3) Alignment – The face captured in the camera may not be completely perpendicular to the camera and hence the alignment needs to be determined and compensated so that it is ready to use of recognition process.
4) Feature Extraction – Feature extraction involves a process of measuring various facial features and creating a facial template, for the purpose of matching and identification.

V. PROPOSED FACE RECOGNITION SYSTEM FOR USER AUTHENTICATION

A. Step I – New User Registration

Whenever user wants to access cloud resources, user has to register first on to the cloud server.



** FRS – Face Recognition System*

Fig. 4 New User Registration steps in Cloud using FRS

Following are the steps to register on the cloud server.

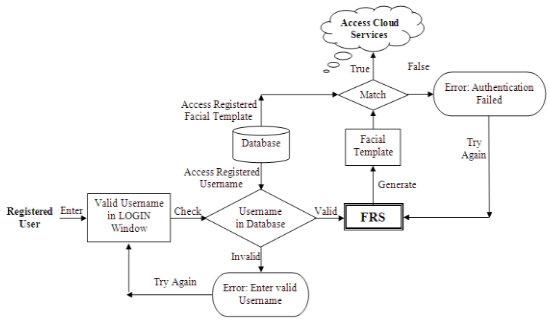
1) User has to fill the registration form which is provided by cloud provider. It contains detail information about the user.
2) User has to provide valid Email ID as a username to the face recognition system at the time of registration.
3) Face recognition system checks the Email ID against the availability of that username. Username should not repeat or match with existing user's username.
4) After checking the availability of username, the password must be created. Face image through web camera is stored in database as a password.
5) After providing valid username and storing face image as a password, the registration on cloud server is completed.

B. Step II – Registered User Login

When registered user wants to access resources on the cloud server, then registered user should login on to the cloud server.

Following are the steps to login on to the cloud server.

1) User should enter valid username in his login interface which was already provided by the user at the time of registration. And for password user's face is captured by web camera.
2) Face recognition system checks the username and face image as a password provided by the user.
3) After matching the username and face image as a password, face recognition system provides access of cloud services to the user.
4) If username or face image does not match then face recognition system displays an error message.



** FRS – Face Recognition System*

Fig. 5 Registered User Login steps in Cloud using FRS

VI. 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

VII. CONCLUSION

The services of cloud computing is based on the sharing. Cloud computing provides variety of services like Iaas, SaaS, and PaaS. These services are paid services, so security is a major concern to identify authorized user in cloud computing. 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.

So it is a better option to use face recognition system rather than traditional or other biometric authentication techniques. The security level of cloud provider in terms of secure authentication is much improved by using face recognition system.

REFERENCES

[1] Rajesh Piplode and Umesh Kumar Singh, “An Overview and Study of Security Issues & Challenges in Cloud Computing,” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume-2, Issue-9, September 2012.

[2] P. Senthil, N. Boopal and R.Vanathi, “Improving the Security of Cloud Computing using Trusted Computing Technology,” International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Volume-2, Issue-1, Jan-Feb 2012, pp-320-325.

[3] Ganesh V. Gujar, Shubhangi Sapkal and Mahesh V. Korade, “STEP-2 User Authentication for Cloud Computing,” International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume-2, Issue-10, April 2013.

[4] "The NIST Definition of Cloud Computing". National Institute of Science and Technology.

[5] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, “Research Challenges and Security Issues in Cloud Computing,” International Journal of Computational Intelligence and Information Security, Volume-3, No-3, March 2012.

[6] Nils Gruschka and Meiko Jensen, “Attack Surfaces: A Taxonomy for Attacks on Cloud Services,” Proceedings of the IEEE 3rd International conference on Cloud Computing, 2010, PP-276-279.

[7] Minhaz Fahim Zibran, “Biometric Authentication: The Security Issues,” University of Saskatchewan, 2012.

[8] S. O. Kuyoro, F. Ibikunle and O. Awodele, “Cloud Computing Security Issues and Challenges,” International Journal of Computer Networks (IJCN), Volume-3, Issue-5, 2011.

[9] Maninder Singh and Sarbjeet Singh, “Design and Implementation of Multi-tier Authentication Scheme in Cloud,” International Journal of Computer Science Issues (IJCSI), ISSN: 1694-0814 Volume-9, Issue-5, No-2, Sep. 2012.

[10] Aviel D. Rubin Bellcore, “Independent One-Time Passwords,” Fifth USENIX UNIX Security Symposium, Salt Lake City, Utah, Jun. 1995.

[11] Chunming Rong and Hongbing Cheng, “A Secure Data Access Mechanism for Cloud Tenants,” Cloud computing 2012: The Third International Conference on Cloud Computing, GRIDs, and Virtualization, ISBN: 978-1-61208-216-5, IARIA, 2012.

[12] Jitendra Choudhary, “Survey of Different Biometrics Techniques,” International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Volume-2, Issue-5, Sep.-Oct. 2012, pp-3150-3155.

Akshay A. Pawle received the M.Sc.(CS) degree from University of Pune, in the year 2008. Currently working as a lecturer in the College of Computer Science and Information Technology, Latur, Maharashtra. Pursuing PhD degree in SRTM University, Nanded.

Dr. Vrushsen P. Pawar received MS, Ph.D. (Computer) Degree from Dept. CS & IT, Dr. B. A. M. University & PDF from ES, University of Cambridge, UK also received MCA (SMU), MBA (VMU) degrees respectively. He has received prestigious fellowship from DST, UGRF (UGC), Sakal foundation, ES London, ABC (USA) etc. He has published 90 and more research papers in reputed national international Journals & conferences. He has recognized Ph. D Guide from University of Pune, SRTM University & Sighaniya University (India). He is senior IEEE member and other reputed society member. Currently working as an Associate Professor in CS Dept of SRTMU, Nanded.