Biometric Authentication as a Service on Cloud: Novel Solution

Himabindu Vallabhu, R. V. Satyanarayana

Abstract: ***Authenticating the user based on behavior based biometrics is more reliable than the more traditional means of password authentication .Since Biometric identification is unique and slow intrusive .Biometric systems provide the solution to ensure that the rendered services are accessed only by a legitimate user and no one else. Biometric systems identify users based on behavioral or physiological characteristics. The advantages of such systems over traditional authentication methods, such as passwords and IDs, are well known; hence, biometric systems are gradually gaining ground in terms of usage. As security is the main concern in using cloud computing fused biometric authentication technique which can be used as single sign on so that the services can be more secure and reliable ,and that biometric authentication is provided as a service by a cloud provider.***

Keywords: Biometrics,cloud ,authentication, Single Sign On, fused

I. INTRODUCTION

The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure).Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Computer science, biometrics to be specific, is used as a form of identification [1].

Behavioral biometrics are related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the behavior class of biometrics [1].Biometric systems allow identification of individuals based on behavioral or physiological characteristics [2].Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods.

To achieve more reliable verification or identification we should use something that really characterizes the given person. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. These characteristics are unique and slow intrusive.

Biometric systems can be used in two different modes. Identity *verification* occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. *Identification* (also called *search*) occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all [4].

Manuscript received September 02, 2012.

Himabindu Vallabhu, She worked as Assistant Professor from 2004 till date in various colleges

R. V. Satyanarayana HOD for Computer Science and Engineering from Bonam Venkata Chalamaya Engineering College (BVCE)

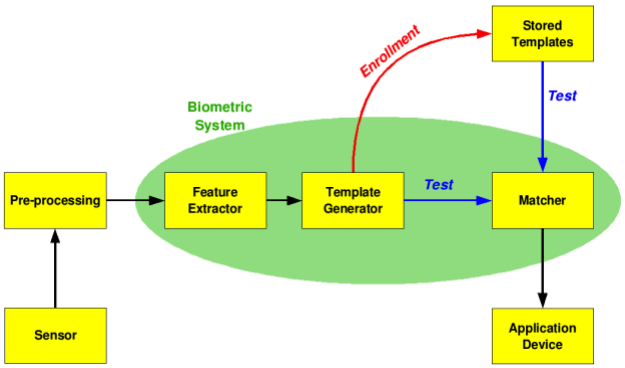

Figure1: Basic block diagram for biometric system

The figure1 shows the above specified identification and verification process.

Cloud Computing Basics:

In [8]Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Service Models: From [8] the service models and development models are given as: *Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary.

II. TYPES OF BIOMETRIC METHODS

Two classes of biometric methods are:

1) Physical Biometrics:
   Physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics.
2) Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation of time as a metric – the measured behavior has a beginning, middle and end [3].

A number of biometric methods have been introduced over the years, but few have gained wide acceptance.

III. PROS AND CONS OF DIFFERENT BIOMETRICS METHODS

Theoretically biometrics is a great way of authenticating a user.

Finger prints: It's impossible to lose your finger prints, no chance of forgetting them. However in practice according to the problem that has been pointed out by Guy Churchward, CEO of LogLogic ,uniqueness the thing that makes using biometric data an inherently flawed choice for a primary method of authentication."Once you have your fingerprint scanned it will give a unique data sequence which if compromised is not exactly something you can change," he says. "Imagine having an option of only one password 'ever'. One loss and you are screwed"[4].The above problem can be solved by using biometric and password together for authentication.

Hand scans: Hand scans requires low data storage but may not be unique to every user.

Retina Scans and iris scans: Retina scans are highly accurate and require low storage space but they need expensive hardware and user identification frequency is less. Iris scans are low intrusive and they are more accurate and needs less storage space

Voice authentication: Voice authentication is unique and non intrusive method and also the hardware requirements required for this type of authentication are cheap and are available readily. Microphones can be used for this purpose.

However the back ground noise must be controlled, high storage is required for this kind of authentication. This type of authentication can also be extraneously influenced by once sore throat and cold.[6]

Facial scans: One major advantage is that facial-scan technology is the only biometric capable of identification at a distance without subject complicity or awareness. Another advantage of facial-scan technology is the fact that static images can be used to enroll a subject. [7]

Disadvantages include acquisition environment and facial characteristic changes that effect matching accuracy and the potential for privacy abuse. Images are most accurate when taken facing the acquisition camera and not sharp angles. The users face must be lit evenly, preferably from the front [7].

Selecting biometric methods for authentication.

By comparing the information given above, considering cost and practicality we can choose the following biometric methods for authentication our paper. Finger prints and voice recognition can be considered.

IV. PASSWORD HACKING AND DATA INTRUSION IN CLOUD

One of the Security risks in cloud computing according to Garfunkel [11] is hacked passwords or data intrusion. If someone hacks a password they get control over the resources. They can manipulate the information or disable the services. Furthermore, there is a possibility for the user's email (Amazon user name) to be hacked (see [10] for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password [9].

V. NOVEL SOLUTION TO PASSWORD HACKING IN CLOUD

Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. Conversely, Single sign-off is the property whereby a single action of signing out terminates access to multiple software systems. [13]

A Hybrid biometric method can be developed by fusing finger prints and voice biometric methods. The fused value can be used as signal sign on for multiple resources provided by cloud. This encrypted data is used for authentication

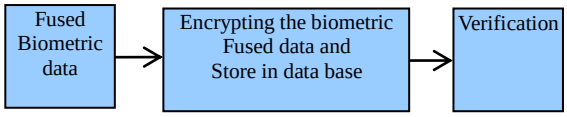

Fig 2. Fused biometric data encrypted and stored in database.

VI. BIOMETRIC AUTHENTICATION SYSTEM AS A CLOUD SERVICE: ARCHITECTURE

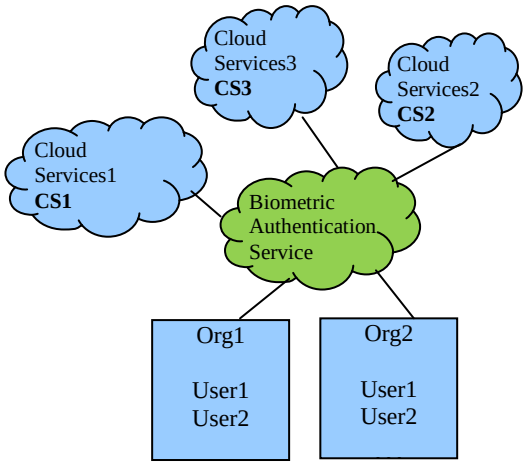

Fig3: Biometric Authenticating System in cloud

As shown in fig3 the user from an organization uses Biometric authentication service from a cloud and then the user connects to the required cloud.

VII. BIOMETRICS AUTHENTICATION SYSTEM WORKING

The authentication service provider maintains the biometric data base .The data has to be stored in encrypted format using cryptography on biometric for the security reasons. In this paper we site a blind protocol technique which is given by Upamanyu.M, the protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography [12].

Registration process:

The user initially enrolls with the biometric system which is provided by a cloud, once the identity is registered his/her biometric authentication details are stored in cloud service provider database. The authorization details are also entered at the registration time which is also encrypted.

Whenever the user wants to use any cloud service user first uses the biometric authentication service rather than a traditional password mechanism. Once authenticated, the user is redirected to the actual cloud service for which he is authorized to use.

VIII. CONCLUSION

In summary, as Biometrics allow for increased security, convenience we can say that fused biometric authentication system will be novel solution for authenticating users on cloud computing ,which can be provided as service on cloud and can be used as a single sign on.

REFERENCES

1. http://en.wikipedia.org/wiki/Biometrics
2. J.L.Wayman, "Fundamentals of Biometric Authentication
3. Xhtp:/ww.engr.sisu.edu/biometrics/nbtcw.p
4. http://www.indexbiometrics.com/physiological_or_behavioral.htm
5. http://www.fi.muni.cz/reports/files/older/FIMU-RS-2000-08.pdf
6. http://www.netsecurity.org/secworld.php?id=8922
7. http://ntrg.cs.tcd.ie
8. http://www.sans.org/reading_room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning
9. NIST Special Publication 800-145 “The NIST Definition of Cloud Computing” Peter Mell Timothy Grance
10. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
11. Cloud Computing Security: From Single to Multi-Clouds
12. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=614956
13. S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003
14. S.L. Garfinkel, "An evaluation of amazon’s grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007
15. ”Blind Authentication: A Secure Crypto-Biometric Verification Protocol”
16. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5422721&contentType=Journals+%26+Magazines&searchField%3DSearch_All%26queryText%3Dbiometric+authentications+encryptons.
17. http://en.wikipedia.org/wiki/Single_sign-on

AUTHORS PROFILE

Himabindu Vallabhu received B Tech Degree in Computer Science and Engineering from Bonam Venkata Chalamaya Engineering College (BVCE) in 2004. She is currently pursuing her M Tech from BVCE. She worked as Assistant Professor from 2004 till date in various colleges.

R V Satyanarayana HOD for Computer Science and Engineering from Bonam Venkata Chalamaya Engineering College (BVCE) .