

FUTURISTIC AUTHENTICATION IN CLOUD COMPUTING ENVIRONMENTS

Ankush Kudale¹, Dr. S. Hemalatha²

ABSTRACT

In today's in society, because of developed in technology our life is become easier. Most of the systems became computerized and these systems are available in the online and to access using the internet for remote access. Cloud computing is altering the way we interact with devices, software, data and processes. Cloud computing based applications have many benefits but it has several security problems like Authentication and Access Control, Trust, Legal Issues, Confidentiality, Data Encryption, Early Approaches, Querying Encrypted Data, Denial of Services, Malicious Insiders, Data Breach, Vulnerability in virtualization, etc. To access the cloud based application, user need to login, but many users do not know that their login is secure or not, and providing login credentials to correct site etc. For user authentication the password is

mostly used. But it is not a enough way to use just a password since it has many drawbacks, like guessing them, brute force attacks, key-loggers and social engineering. There are various techniques and ways are available to access cloud but still there is a security issue. This paper is trying to list out Futuristic Authentication and how the security connected to cloud.

Keywords : Cloud Computing, Security, Futuristic Authentication, Biometric

1 INTRODUCTION

Cloud computing [11] is a kind of computing that depend on sharing computing resources rather than having the local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where the different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet. Cloud computing is comparable to grid computing, a type of computing where the unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

1.1 Cloud Computing Services

- a. Software as a Service [SAAS][12] SasS is software (application/s) is hosted by cloud service provider or cloud vendor and it is accessible to customer via network using internet.
- b. Platform as a Service [PAAS] It is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for

¹Research Scholar, Dept. of Computer Science, KAHE, Coimbatore, India, ankush.kudale@gmail.com

²Research Guide, Dept of CS,CA & IT KAHE, Coimbatore, India, drhemashanmugam@gmail.com

running the existing applications or developing and testing new ones.

- c. Infrastructure as a Service [IAAS]: IaaS service providers having their own equipments to support operations which include hardware, servers, storage and components for networking etc to client on per usage basis.

2 Cloud Authentication

As Cloud Computing has been spreading widely, users and service providers enable to use resources or services cheaply and easily without owning all the resources needed. However, Cloud Computing has some security issues such as virtualization technology security, massive distributed processing technology, service availability, massive traffic handling, application security, access control, and authentication and password. User authentication among them requires a high-guaranteed security.

2.1 Cloud Authentication issues

Service provider of cloud, stores customers' information on cloud, providers may access client's information. This may a privacy issue towards client's

information. Several service level agreements have provided the confidential data, though client cannot verify the rules are applied on it. There is less clarity on customer's information. If customer wants to use various cloud service, need to store login credentials on various cloud, this is one of the security issue with service provider of cloud. Different service providers having different authentication methodology for authenticating user, this may have fewer impacts on SaaS than PaaS and IaaS, but it is challenge to the customers [5].

2.2 Classic Authentication

Authentication is one of the key aspects of any security system. An authentication service is the ever-vigilant guard at the gateway to the digital fortress; it is responsible for checking the identity of any party seeking entrance (i.e., access) to the system; it verifies certain credentials to ensure that an entity is indeed and what it claims itself to be.

In Table 1, Comparison of traditional authentication mechanisms with advantages and disadvantages.

Mechanism	Idea	Advantages	Disadvantages
User ID/ Password	Pre-registered username and secret password	Simple, popular, easy-to-deploy	Must be renewed Frequently
Public Key Infrastructure	Trusted Certificate authority issues private keys	No sharing of secret key	Single point of trust; challenges in scalability
Kerberos	Trusted authority issues Tickets	Mutual authentication between client and server	Single point of failure; requires Time synchronization

Single Sign-On	One step authentication to multiple applications	User friendly	Any breach in sign-in security affects multiple applications
One Time Password	PIN typically used in multifactor authentication	Easy-to-use; Compatible with password based authentication	Secure generation and transmission of OTP is challenging
Mobile Trusted Module	Chip for hardware authentication	Optimized for mobile devices; small footprint	Deployment and management is challenging

As there are different classical methods for authentication are found but still it requires more security. The biometric authentication is more secure than the classical one.

3 What is Biometrics Security?

Biometric Security is now days a very familiar and trustworthy security system which has a massive demand of today and will not suffer any kind of depression in its and a want in the upcoming future. The security factor in the biometric security system in highly improvised by concatenating the data with a unique physical quality. The term "biometrics" is infested from the Greek language and is taken up from two special words bio (meaning life) and metric (to examine). Biometrics (a security measure) is the recognition of the humans by the help of their physical traits/behavior. The main purpose of biometrics in Computer science is to serve a method of identification.

The system is provided with the biometric identity (like fingerprint or voice sample), which is then real against a stored template. It is an invincible security measure which cannot be defeated by anybody which makes it a significant reason for being given the first preference and first while thinking about the security essentials with respect to IT or Cloud Computing. The two

different modes in which the biometric systems can be used are Verification by identity: This mode is used when the user is previously enrolled in the system (ID card or login name) In such a case, there takes place the comparison between the user's biometric data and the user's data which is already present in the database. Identification (also known as recognition) occurs when the identity of the user is a prior unknown to someone else. In such a case the user's biometric data is compared with all the records available or stored in the database as the details of the user may be present any where in the database other user may not any info previously stored [9].

Biometric characteristics can be divided in two main classes, as represented in the following figure [1]:

- ▶▶ Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, hand and palm geometry and iris recognition.
- ▶▶ Behavioral pattern are related to the behavior of a person. Characteristic implemented by using biometrics are signature verification, keystroke dynamics, and voice






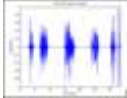

Physiological		Behavioral	
Finger prints		Signature verification	
Face recognition		Keystroke dynamics	
Hand and palm geometry		Voice	
Iris recognition			

Figure 1: Biometric characteristics

A. Physical Biometrics

Physiological biometrics is the one which is based on size and data extracted from direct measurement of part of the body. The various leading physiological biometrics techniques are fingerprint, retina-scan, iris-scan, facial recognition and hand geometry. In Physical Biometrics, the physical impression is used instead of artificial impression for the passwords. The physical impression is quickly scanned and a pathway no matter it gets matched or not. If the impression gets matched, then the user advances to the next step for security.

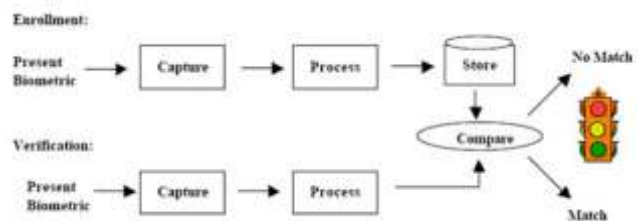
B. Behavioral Characteristics

Behavioral characteristics are based on how the person reacts to the specific conditions. Behavioral biometric

are based on the dimensions and extracted from an action, and they measure the characteristics of the human body. It includes characteristics like voice recognition, keystroke-scan, and signature-scan are important behavioral biometric technologies present in today's scenario. One of the major characteristics of a behavioral biometric is the inclusion of time as a measure [3].

Following figure[2] shows working system of biometric, initially enrollment can be done with biometric image, it need to capture and then it has to store. To verify need to capture a biometric and compare with the stored and matching result will found.

Figure 2: Working of biometric system



4 Literature Review and Related Work

Jessica Hullinger, Mental Floss[5], suggested replacement for password. This includes, your brain print, your heartbeat, your face, your google searches, sound verification between your computer and your phone, The Veins in Your Palm and Electronic Tattoos. Heather Kelly[6], says "The wristband detects a wearer's unique heartbeat and could be used to unlock devices, start cars and open doors.". And your heart beat, your ear shape, your walk, your typing speed, face recognition. Recently a popular social website facebook has stated face recognition application for their uses. Aria Bendix , wrote an article for new password, from selfies to heartbeat recognition, bioengineering is the future of digital security. The brain print can be identified 100% even brain print

requires a special reader, but there are some programs are available now, who give 100% accuracy.

Ramzi Saifan, Asma Salem, Dema Zaidan, Andraws Swidan [14] Password authentication is the most commonly used authentication method for local access, network access, and internet access. However, password authentication suffers from many drawbacks due to password nature. Therefore, some techniques are required to strengthen password. Researcher's survey focused on typing behavior keystroke dynamics. From the last three decades, typing behavior authentication were being invested starting from classical keyboards and end up with touch screens in digital devices and cell phones, which have replaced the classical keyboards. Jyotika Chhetiza, Nagendra Kumar[10], Multiple factor Authentication (MFA) can contribute compelling benefits to an enterprise, but the technology being so complex and the mechanism itself can differ vastly from vendor to vendor. Many of the leading MFA products are already out for commercial space. Here Authors have broadly discussed about security factors, threats, authentication strategies and Multifactor Authentication mechanisms in significance. Along with password or PIN as the baseline authentication standard, additional layers of security and verification can be pulled from a wide pool of sources. Although its implementation may be a little expensive for naive users; secure, usable and affordable MFA is still possible in the future but multifactor is the combination of biometric and it is secured one.

A.S. Falohun, O.D. Fenwa, A.O. Oke[13], Have implemented a biometrically controlled door system using Iris and fingerprint templates has been successfully designed and constructed. The hardware was successfully designed, constructed and a computer program that enabled the door's operation via an electric circuit was also developed. This will provide a

more secured and fool proof access control system. Ankita Yadav, Nagendra Kumar[14] carried out a survey on traditional method authentication system, has several advantages and still there are many challenges in it. So there is a scope to work in futuristic authentication techniques.

5 Proposed Framework

To prepare a model for cloud authentication using common device, which will easily adopted in the current access point.

6 Conclusion

There are many proposed schema available in the cloud. But it is opt for the best. Only a few out of various biometric methods developed were able to gain approval. Even if the precision of the biometric techniques are not perfect till now, there are many mature biometric systems are available now, in order to compete against the previous systems. Correct design and execution of the biometric system can truly a boost for overall security, especially the smartcard or smartphone based solutions seem to be very promising in the near future. Thus this research work gives a detailed view of all the futuristic authentication, which will give a secured access for cloud user.

REFERENCE

- [1] Krishna Dharavath, F. A. Talukdar, R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review", Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on Computational Intelligence and Computing Research, Dec 2013.
- [2] Renu Bhatia, "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

- [3] Mrs. S.M.Barhate, Dr. M. P. Dhore, "User Authentication Issues In Cloud Computing", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 4, 2016
- [4] Steven Furnell, "FROM PASSWORDS TO BIOMETRICS IN PURSUIT OF A PANACEA", Centre for Security, Communications & Network Research Plymouth University United Kingdom.
- [5] Jessica Hullinger, 8 Futuristic Password Replacements (6 Use Your Body), Mental Floss Article 2017.
- [6] Future of Biometrics- Published by Acuity Market Intelligence August 2009.
- [7] Ramzi Saifan, Asma Salem, Dema Zaidan, Andraws Swidan, "A Survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices", January 2016, Journal of Social Sciences (COES&RJ-JSS), Volume 6, Issue 5, May 2016.
- [8] Ankita Yadav, Nagendra Kumar, "A Survey of Authentication Methods in Cloud Computing" International Journal of Innovative Research in Computer, and Communication Engineering, Vol. 4, Issue 11, November 2016.
- [9] Shivashish Ratnam, Mimzee Gupta, Dr. Ajay S. Singh, Thirunavukkarasu, A Survey On Biometric Security Technologies From Cloud Computing Perspective, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 5, ISSUE 04, APRIL 2016.
- [10] Jyotika Chhetiza, Nagendra Kumar, A Survey of Security Issues and Authentication Mechanism in Cloud Environment with Focus on Multifactor Authentication, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016.
- [11] Ankush Kudale ,Dr. Binod Kumar, "Protected Authentication by Login Credential and OTP for Cloud Based Application", International Journal of Computer Application (2250-1797), Volume 5- No. 3, April 2015.
- [12] Ankush Kudale ,Dr. Binod Kumar, "Review -A Study On Authentication And Access Control For Cloud Computing", International Journal of Research in computer Science and Management, July 2014.
- [13] A.S. Falohun, O.D. Fenwa, A.O. Oke, An Access Control System using Bimodal Biometrics, International Journal of Applied Information Systems (IJAIS), Volume 10 - No.5, February 2016
- [14] Ankita Yadav, Nagendra Kumar, "A Survey of Authentication Methods in Cloud Computing" International Journal of Innovative Research in Computer, and Communication Engineering, Vol. 4, Issue 11, November 2016.