International Journal of Contemporary Technology and Management
Volume VII, Issue I, January - 2018 ISSN (Online) 2278-8034

A Study on Combining Biometric and Behavioral Authentication Techniques for Secure Cloud Access

Shubham Sharma[1], Rahul Sharma[2]
Department of Computer Science
R.K.D.F School of Engineering
Indore (M.P)
shubham.sharma883@gmail.com [1]
sharma.rahul5656@gmail.com[2]

***Abstract*:** Cloud computing is one of the widely used technology and its use is increasing day by day due to its sharing of services over the internet. The area of concern is its security and privacy issues especially for the smart-phone users. Several security approaches had been introduced to safeguard users from unauthorized access but the security standard with the smart-phone devices are still not up to the mark and uses the typical username and passwords based authentication techniques. This paper is proposing a hybrid authentication approach combining two security modalities i.e. biometric and behavioral keystroke dynamics based user authentication which is designed to provide authentication with the existing username and password along with the biometric and behavioral keystroke dynamics based authentication with the use of biometric fingerprint scanner and keyboard thereby reducing the high cost of additional hardware devices since both are the integral part of the smart-phones these days. This approach will provide a secure access to the smart-phone users for a secure cloud environment efficiently than the existing methods.

Keywords: *Cloud Computing, Biometric Authentication, Keystroke Dynamics, Multi- Level Authentication, Cloud Security*

I. INTRODUCTION

A. Cloud Computing

Mobile cloud computing can be defined as the cloud computing which can be access by mobile devices anytime anywhere. With cloud computing, smart-phone users can access files from any device and access the services. The information being accessed is found in cloud server and user can access it from anywhere. Instead of keeping files on a local hard drive cloud storage servers makes it possible to save them to a remote database Cloud computing lifts and process data away from your and gave a facility to work from your home, office or anywhere.

B. Authentication and Access controls

The process in which the username and passwords provided are compared to the one stored in a database of cloud database server. If the credentials match, the user is granted permission for access. Authentication is the process of giving permissions to the right and authorized users.

Access Control System identifies the legitimate user and then permits them to access the services. Access control systems mostly uses for the communication of information. Access control ensures legitimate user to give access to the cloud services.

C. Types of Authentication

- ✓ Password-based authentication

Password based authentication makes use of user names and passwords. This ensures that the user is authentic. In this the users have to first register themselves at the cloud server to get the access.

- ✓ Multifactor authentication (MFA)

Multifactor authentication combines username and password along with some other security approach. MFA creates a security layer defense against unauthorized person to access database.

- ✓ Two-factor authentication (2FA)

Two-factor authentication is a additional layer of security and makes hard for the cyber attackers to gain access to the cloud servers thereby securing users username passwords and other details. It is like a strong wall standing in front of the attackers.

- ✓ Single factor authentication

Single-factor authentication is very simple authentication technique. In this, a user matches its credential to verify

himself or herself over the internet. This type of authentication technique is used mostly.

D. Why multi-factor authentication is more secure?

Multi-factor validation includes no less than at least two layer of personality confirmation to the procedure, so your assurance against hacking and extortion endeavors is substantially more grounded and more secure than a straightforward watchword. Multi-factor confirmation can incorporate a few unique elements, which two-factor verification is constantly restricted to two variables. Expecting clients to validate with three variables is more secure, yet clients anticipate that a MFA arrangement will be anything but difficult to utilize and with outrageous layer of security. Multi-factor validation (MFA) includes at least two free qualifications for more secure exchanges; frameworks with additionally requesting prerequisites for security and here and there included as fourth and fifth components. It gives a valuable component of layered security by expecting clients to demonstrate their personalities utilizing at least two check techniques before they can be validated. Thusly, in the event that one factor is traded off or broken, the attacker still has no less than one more boundary to cross before breaking into the objective.

II. BACKGROUND

A. Biometric Authentication

Biometric confirmation is a security procedure that depends on the one of kind organic qualities of a person to check that he is who is says he is. Biometric confirmation frameworks contrast a biometric information catch with put away, affirmed bona fide information in a database. On the off chance that the two examples of the biometric information coordinate, confirmation is affirmed. Biometric confirmation is a client personality check process that includes organic info, or the filtering or investigation of some piece of the body. Biometric confirmation has been broadly viewed as the most secure - or if nothing else the hardest to manufacture or parody.

Types of Biometrics -

Various biometric strategies have been presented throughout the years, however few have increased wide acknowledgment.

- ✓ **Keystroke dynamics-** Similar to signature dynamics but extended to the keyboard, recognizing not just a password that is typed in but the intervals between characters and the overall speeds and pattern.
- ✓ **Eye scans-** This favorite of spy movies and novels presents its own problems. The hardware is expensive and specialized, and using it is slow and inconvenient and may make users uneasy.
- ✓ **Fingerprint recognition-** Everyone knows fingerprints are unique. They are also readily accessible and require little physical space either for the reading hardware or the stored data.
- ✓ **Voice recognition-** This is different from speech recognition. The idea is to verify the individual speaker against a stored voice pattern, not to understand what is being said.
- ✓ **Facial recognition-** Uses distinctive features, including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes. Most technologies avoid areas of the face near the hairline so that hairstyle changes won't affect recognition.

B. Behavioral Authentication

Behavioral biometrics is the field of concentrate identified with the measure of extraordinarily recognizing and quantifiable examples in human exercises. Behavioral biometric confirmation strategies incorporate keystroke elements, voice ID, mouse utilize attributes, signature investigation and intellectual biometrics. Not at all like many sorts of physical biometrics, can behavioral biometrics regularly be assembled with existing equipment, requiring programming for investigation. That limit makes behavioral biometrics more straightforward and less exorbitant to actualize. To expand security and counteract utilization of biometric accreditations for wholesale fraud, biometric information is normally encoded amid social occasion and check. The database esteem is contrasted and the biometric input the end client has entered and confirmation is either endorsed or denied. On the off chance that the framework distinguishes a sudden change in a client's behavioral profile, it can naturally compel them through extra security steps and caution the security group. Behavioral Authentication concentrates on the "How" a client sorts and associates with their gadget instead of the "What" they write. It does this by always observing and dissecting keystrokes, mouse developments, finger weight, swipe examples and that's just the beginning, contrasting this movement and a special client model to score a match. A low score, reflecting noteworthy changes in the client conduct, fills in as a warning that some security strategy activity might be required.

III. LITERATURE SURVEY

The adoption of cloud computing involves many advantages in terms of flexibility, scalability, reliability but also implies new challenges on security, data privacy and protection of personal data [1]. The attack of unauthorized users to access

the cloud services is the dangerous threat to authorized user as well as to the computing environment [2]. Multi factor authentication is a methodology that uses two or more authentication techniques along with the password but still does not provide fool proof data security. The existing traditional password authentication does not provide enough security for the data residing in cloud and there have been instances when the password based authentication has been manipulated to gain access into the cloud data [3].

The use of biometric techniques can be considered as an effective solution to ensure a significant increase of security in the authentication. Keystroke dynamics is one of the authentication mechanisms which uses natural typing pattern of a user for identification [4]. Keystroke dynamics authenticates a user by testing the similarity of a test sample against a user's reference profile [5].

There is an approach called fusion that combines multi modalities in one authentication system [6]. The process of combining traditional username and password mechanisms along with bio-metric image processing technique is thoroughly explored for improving security in public cloud infrastructure [7].

IV. CONCLUSION

In conclusion, this research has proposed a solution to provid a secure cloud environment to the smart-phone based cloud users. Biometric and behavioural keystroke dynamics based this multiple level of authentication method can be used as a solution for the cloud providers to deliver security and privacy to their smart-phone users. This combination of two security approach along with the existing methods is very convenient cost saving and inexpensive for the cloud providers to safeguard the data of the users.

In the future work, for the secure cloud environment we are working on this method to implement it for the information security in the cloud without the need to deploy any additional hardware devices.

References

[1] Pietro Ruiu_, Giuseppe Caragnano_, Giovanni L. Masala†, Enrico Grosso "Accessing Cloud Services through Biometrics Authentication" 2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems.

[2] Nileshree R. Darve, Deepti P. Theng "Comparison of Biometric and Non-Biometric Security Techniques in Mobile Cloud Computing" IEEE SPONSORED 2ND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEM.

[3] P. Padma, Dr. S. Srinivasan "A survey on Biometric Based Authentication in cloud computing" .

[4] Elena Ivannikova, Gil David and Timo H¨am¨al¨ainen "Anomaly Detection Approach to Keystroke Dynamics Based User Authentication" 2017 IEEE Symposium on Computers and Communications (ISCC)

[5] Jiaju Huang, Daqing Hou, Stephanie Schuckers "A Practical Evaluation of Free-text Keystroke Dynamics".

[6] Alifa Nurani Putri 1, Yudistira Dwi Wardhana Asnar 2, Saiful Akbar "A Continuous Fusion Authentication for Android based on Keystrol<e Dynamics and Touch Gesture" .

[7] Dr.N. Venakatesan[l], M. Rathan Kumar[2], "Finger Print Authentication For Improved Cloud Security" 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions.

[8] Baljit Singh Saini, Navdeep Kaur, Kamaljit Singh Bhatia "Keystroke Dynamics Based User Authentication using Numeric Keypad".