International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

A Study on Future Authentication Biometric in Cloud Era

S.Raviteja & Devarakonda Krishna
Assistant Professor, CSE Department, St.Martins Engineering College,JNTUH

Abstract:

Advancements to give security to this hitech world are the most encouraging thing now days. We as a rule catch wind of blemishes and violations because of secret key spillage PIN burglary and so on. With the various passwords one needs to recollect keeping in mind the end goal to verify her, they are regularly overlooked, lost or stolen. As there is an issue there must be an approach to wave out those issues. There ought to be some philosophy that can recognize every human exclusively, and the bio-measurements are the one. Bio-measurements are the branch of science that arrangements with investigation of human physical and behavioral qualities like unique mark, iris filter, confront acknowledgment, voice acknowledgment, DNA and so on. We are such a great amount of worried about the security that we are utilizing this verification purposes in managing an account area, air terminals security, online validation and then some. As the greater part of the organizations (governments and NGOs) is moving towards bio-metric based confirmation, an immense measure of bio-metric information is to be put away and dealt with. What's more, here comes the enormous word "Cloud". We utilize cloud computing to store and process these enormous measures of data. Cloud registering is the capacity to use the colossal energy of disseminated stockpiling and calculation. Subject of one nation can go to another nation and she may utilize the administrations there by confirming herself utilizing bio-measurements. This is an incredible preferred standpoint of utilizing cloud computing for bio-measurements. We are utilizing different advances of cloud computing and bio-measurements together for better execution of the confirmation framework.

Keywords

Cloud Computing, Biometric.

1. Introduction

Humans have used body characteristics such as face, voice, gait, etc. for thousands of years to recognize each other. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using a number of body measurements to identify criminals in the mid 19th century. Just as his idea was gaining popularity, it was obscured by a far more significant and practical discovery of the distinctiveness of the human fingerprints in the late 19th century. Soon after this discovery, many major law enforcement departments embraced the idea of first “booking” the fingerprints of criminals and storing it in a database (actually, a card file). Later, the leftover (typically, fragmentary) fingerprints (commonly referred to as latents) at the scene of crime could be “lifted” and matched with fingerprints in the database to determine the identity of the criminals. Although biometrics emerged from its extensive use in law enforcement to identify criminals (e.g., illegal aliens, security clearance for employees for sensitive jobs, fatherhood determination, forensics, positive identification of convicts and prisoners), it is being increasingly used today to establish person recognition in a large number of civilian applications. What biological measurements qualify to be a biometric? Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:
Universality: each person should have the characteristic;
• Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
• Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
• Collectability: the characteristic can be measured quantitatively. However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:
• Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
• Acceptability, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
• Circumvention, which reflects how easily the system can be fooled using fraudulent methods. A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

2. Biometric System

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

• In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

• In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

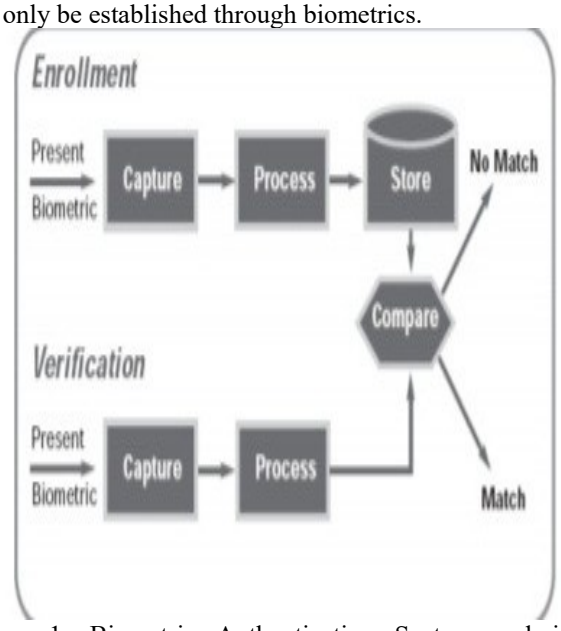

Figure 1: Biometric Authentication System and its Process

3. Cloud Computing

Cloud computing allows you to get on-demand, convenient, ubiquitous network access to shared configurable computing resources such as storage, networks, servers, services, and applications. More and more businesses are moving and integrating their biometric identification management systems to cloud platforms because of the many benefits this brings. Although the market for Biometric systems is growing, widespread applicability of these systems still faces a lot of constraints. Issues faced by biometrics are to achieve large-scale operational capabilities, huge no. Dataset, storage problem because now a day's peoples are more going attractive toward the technologies and biometric and cloud computing play a major role in it to fulfill that expectation of the client or user. So dealing with these huge data we can use cloud computing in the sense of storing and computing that data. By the use we can say that it can give the benefits like: Powerful virtualization through virtual servers as well as cloud hosting providers makes migrating of the massive database to the cloud seamless. This gives you very good deployment possibilities. These include smart space, access control applications, among others. Cloud computing offers parallel processing capabilities. Several people can work on the same data with no problem at all.

4. Proposed Work

Biometric Authentication with Cloud Era

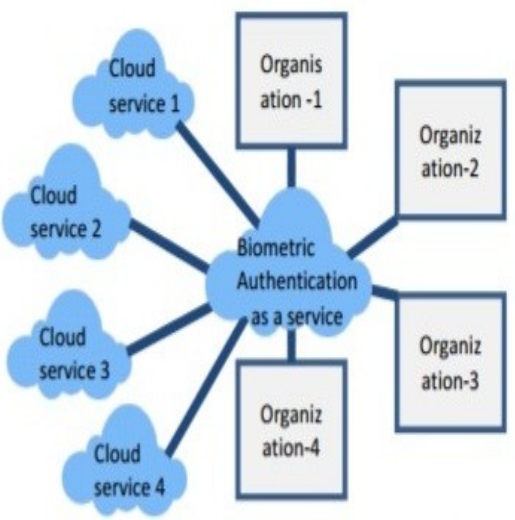

Figure 2: Biometric Authentication System in Cloud Era

Availability: Most providers offer a Service Level Agreement which guarantees 99%availability. That is the authentication system will not go down. Mobility: Ease of access anywhere, where internet is provided. Manageability: Cloud computing provides enhanced and simplified IT management and maintenance capabilities through central administration of resources, vendor managed infrastructure. Backup and Recovery: Since all your data is stored in the cloud, backing it up and

restoring the same is relatively much easier than storing the same on a physical device. In this paper we have analyzed the aspects of biometrics and cloud when implemented as "biometric authentication as a service. As we did deep dive into biometric and cloud computing, we found that both of these can be combined together to make the future system of authentication. In the countries which are still developing with a noticeable population, Bio-metric can be proved to be the best way to authenticate any individual.

Fingerprint: Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [25]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about US $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

5. Conclusion

A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. This paper describes the future of the Biometric as a Service in the cloud computing environments.

6. References

. *[1] Cloud computing use case discussion group, "Cloud Computing Use Cases: White Paper" available from: http://cloudusecases.org.*

[2] https://www.engineyard.com/infographics/everythin g-as-a-service Last Visited: 21/03/2017

[3] https://www.servicenow.com/everything-as-a- service.html. Last Visited: 19/03/2017

[4] Diagram is taken from http://www.brighthub.com/environment/green-computing/articles/127086.asp

[5] Biometric Authentication as a Service on Cloud: Novel Solution International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-4, September 2012

[6] https://www.researchgate.net/publication/3278329_ Biometric_security_technology Journal of Network and Computer Applications2012

[7] Sameena Naaz, Faizan Ahmad Siddiqui,"Comparative Study of Cloud Forensics Tools", Communications on Applied Electronics (CAE) ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA Volume 5 – No.3, June 2016, page 24-30.