



Cloud and Biometrics: The Future of Authentication

Syed Luqman Quadri
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
luqman.quadri@gmail.com

Areeba Kazim
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
aribakazim1995@gmail.com

Aditya
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
aditya0025@yahoo.com

Abstract: Technologies to provide security to this hi-tech world are the most promising thing now days. We usually hear about flaws and crimes due to password leakage PIN theft etc. With the numerous passwords one has to remember in order to authenticate her, they are often forgotten, misplaced or stolen. As there is a problem there must be a way to wave out those problems. There should be some methodology that can identify each human individually, and the bio-metrics is the one. Bio-metrics is the branch of science that deals with study of human physical and behavioural characteristics like fingerprint, iris scan, face recognition, voice recognition, DNA etc. We are so much concerned about the security that we are using this authentication purposes in banking sector, airports security, online authentication and more. As most of the organizations (governments and NGOs) are moving towards bio-metric based authentication, a huge amount of bio-metric data is to be stored and handled. And here comes the big word "Cloud". We use cloud computing to store and process these huge amounts of data. Cloud computing is the ability to utilize the immense power of distributed storage and computation. Citizen of one country can go to another country and she may use the services there by authenticating herself using bio-metrics. This is a great advantage of using cloud computing for bio-metrics. We are using various technologies of cloud computing and bio-metrics together for better performance of the authentication system.

Keywords: Cloud computing, Biometric, Biometric Authentication as a Service, SaaS

I. INTRODUCTION

Authentication is the act of confirming the truth of attribute of entry. This might involve confirming the identity of a person or software program tracing the origins of an artifact or ensuring that a product is what it's packaging and labeling claim to be. When talking about Internet authentication, in most cases, people are still talking about passwords. One of the biggest problems with current authentication approaches is the existence of too many password-account pairings for each user, which leads to forgetting or using the same user name and password for multiple sites. [1]

A possible solution to this problem can be found in the use of bio-metrics. [2] Bio-metric authentication techniques use physiological or behavioral traits of human-being for authentication purposes, while their use on the Internet is still relatively modest. The main reason for this setting is open issues pertaining mainly to the accessibility and scalability of existing bio-metric technology. Countries which are developing or are already developed are using bio-metrics at a very large scale for making their infrastructures secure and responsive. There comes the power of cloud computing which makes authentication process very fast and highly available. There's nothing like being in New York and being asked for a code that went to a phone at home in India. [3] In a world of bio-metric based security, you are the password [3]. Biometric authentication is also very important for cloud forensics [12].

Providing bio-metric based authentication as a service is the concern of this paper. We know that cloud is known

to provide "Anything as a service", and here we are exploiting this power to deliver "Bio-metric based authentication as a service".

II. BIOMETRICS

Bio-metrics is the science and innovation of measuring and measurably dissecting natural information [3]. In data innovation, bio-metrics as a rule alludes to innovations for measuring and breaking down human body attributes, for example, fingerprints, eye retinas and irises, voice designs, facial examples, and hand estimations, particularly for confirmation purposes[3][4]. Bio-metric traits can be split into two main categories:

Physiological bio-metrics: it is based on direct measurements of a part of the human body. Fingerprint, face, iris and hand-scan recognition belong to this group. [2]

Behavioral bio-metrics: it is based on measurements and data derived from an action performed by the user, and thus indirectly measures some characteristics of the human body. Signature, gait, gesture and key stroking recognition belong to this group. [2]

However, this classification is quite artificial. For instance, the speech signal depends on behavioral traits such as semantics, diction, pronunciation, idiosyncrasy, etc. (related to socioeconomic status, education, place of birth, etc.). However, it also depends on the speaker's physiology, such as the shape of the vocal tract. On the other hand, physiological traits are also influenced by

user behavior, such as the manner in which a user presents a finger, looks at a camera, etc.

Bio-metric systems can be operated in two modes, named identification and verification. We will refer to recognition for the general case, when we do not want to differentiate between them. However, some authors consider recognition and identification synonymous

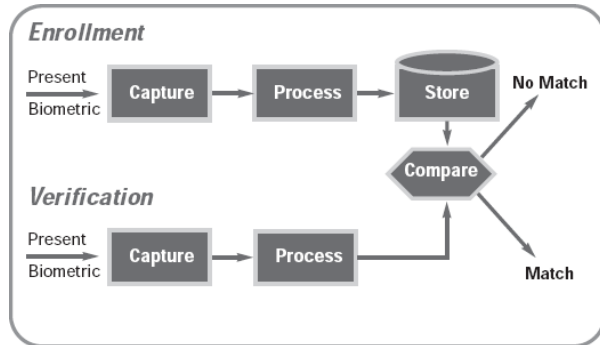


Figure 1: Working of biometric based authentication system.

III. CLOUD COMPUTING

Cloud services can be provided through the network, but not all of Internet services are the cloud services. The definition of cloud computing based on the National Institute of Standards [6] and Technology is “*a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or interaction of service provider.*” [6]

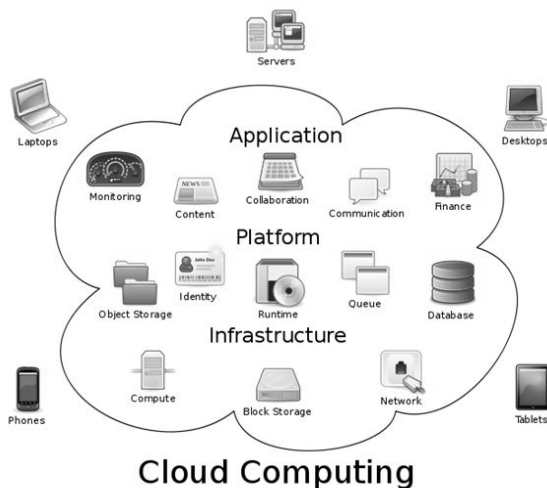


Figure 2: Basic overview of cloud computing[11]

Such a cloud model promotes availability and is composed of five essential characteristics,

- **Rapid elasticity** - elasticity is defined as the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing as needed [6] [7].
- **Measured services** – certain aspects of the cloud service are controlled and monitored by the cloud

provider. This is crucial for billing, access control, resource optimization, capacity planning and other tasks [6] [7].

- **On-demand self-service** - a consumer can use cloud services as needed without any human interaction with the cloud provider [6] [7].

- **Ubiquitous network access** - the cloud provider’s capabilities are available over the network and can be accessed by various clients through standard mechanisms [6] [7].

- **Resource pooling** - allows a cloud provider to serve its consumers via a multi-tenant model. Physical and virtual resources are assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location [6] [7].

Table I. Various model of cloud computing and their examples.

| Model | Purpose | Examples |
|-------|--|-------------------|
| PaaS | Storage and networking | Virtual Machines |
| IaaS | Controlling infrastructure as a service | Development tools |
| SaaS | Constructing application to assist with operations | Email |

There are three service models [6] of cloud, including Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS).

Cloud computing is now established as a widely used model to offer “everything as a service”. [8][9] Over the internet, the cloud computing reveals a remarkable potential to provide on-demand services to consumers with greater flexibility in a cost effective manner. While moving towards the concept of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability.

IV. CURRENT STATUS OF CLOUD AND BIOMETRICS

Now almost everywhere cloud is being used for making the system more reliable and robust. The cloud infrastructure is used for making traditional services online at a very large scale. Authentication service is also one of those; biometric based authentication is being used since a long time. But as the use of biometric based authentication is increasing, requirement for high computation and storage is required. And that is why it is also being served via cloud as a service to the users.

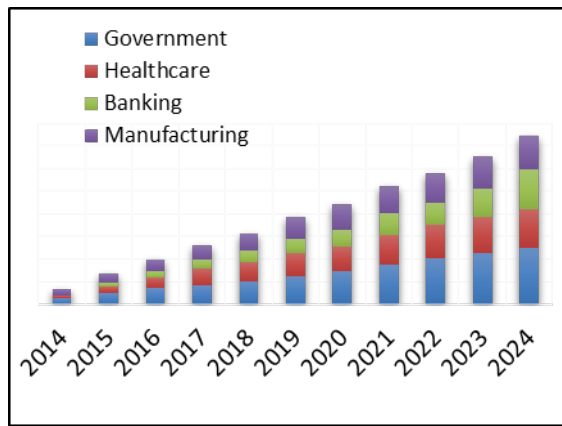


Figure 3: Usage of cloud in various industries.

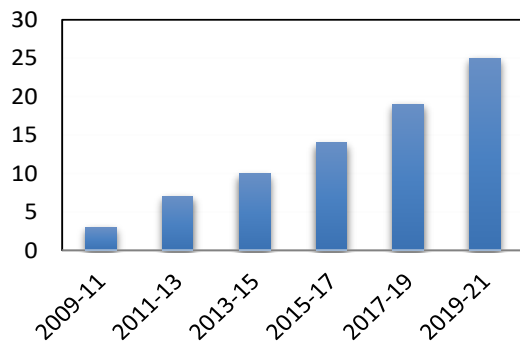


Figure 4: Usage of cloud and biometrics in various industries.

V. UNIFICATION OF BIOMETRIC IN CLOUD

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, etc. because now a days 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.

Cloud-based biometric technology is faster than the traditional biometric technology. You also get improved speeds because of the reduced system complexities.

Demand of cloud computing for biometric (Software as a service [9])

As the people are more concern/anxiety about the security, more and more people are moving towards the biometric looking it as the best available security option. But as the population is increasing rapidly storing and computing the biometric data has become difficult task so to fulfill that need we have to go toward the cloud computing for storing and processing that data.

As an example of finger print registration and verification (A case study) [11]:

The registration process uses a fingerprint reader to capture the (biometric) fingerprint data. In the next phase the quality of the captured sample is evaluated and if it is found to be adequate, the system extracts features from it and stores them in the form of a biometric template in the database. During the verification process features from the captured "live" fingerprint are again extracted and compared to those stored in the database. The comparison is made based on pattern matching procedures, which form the foundation for the validation of the identity claim. As the biometric templates are taken it is converted into the binary equivalent and that binary is stored in database in some encrypted format.

So it is very obvious that a huge storage and huge computational power is required for making authentication service robust and reliable.

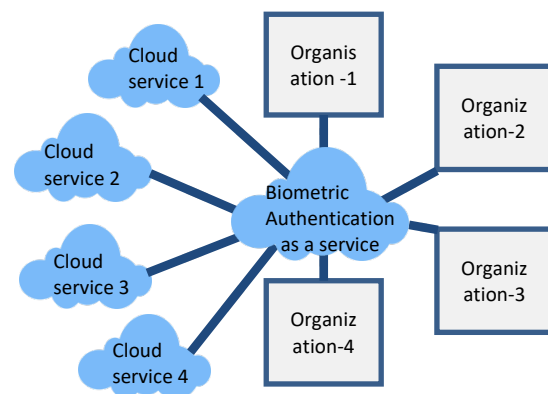


Figure 5: Using biometric authentication as a service

Advantages of using Biometrics as a service:-[10]

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.

V. CONCLUSION

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.

VI. ACKNOWLEDGMENT

We would like to express my sincere gratitude to Dr. Sameena Naaz, Assistant professor, Department of Computer Science and Engineering, SEST, Jamia Hamdard, for her kind guidance throughout the research work.

We would also like to acknowledge Dr. Syed Imtiyaz Hassan, Assistant professor, Department of Computer Science and Engineering, SEST, Jamia Hamdard, for his facilitation and support in completing this seminar paper.

We also extend heartfelt gratitude to Dr. Farheen Siddiqui, , Assistant professor, Department of Computer Science and Engineering, SEST, Jamia Hamdard.

VII. REFERENCES

- [1] D. Balfanz et al., "The future of authentication", IEEE Security & Privacy, vol 10, pp 22-27 2012.
- [2] Biometric Systems Technology, Design and Performance Evaluation by James Wayman, Anil Jain, Davide Maltoni and Dario Maio (Eds), Springer. pp 9-14
- [3] <http://www.imore.com/talk-mobile/future-authentication-biometrics-multi-factor-and-co-dependency-talk-mobile>
- [4] S. Suryadevara, S. Kapoor, S. Dhatteval, R. Naaz and A. Sharma, "Tongue New Prospects of Cloud Computing Security," in: International Conference on Information and Network Technology, vol. 4, 2011
- [5] NIST Special Publication 800-145 "The NIST Definition of Cloud Computing" Peter Mell Timothy Grance
- [6] Cloud computing use case discussion group, "Cloud Computing Use Cases: White Paper" available from: <http://cloudusecases.org/>.
- [7] <https://www.engineyard.com/infographics/everything-as-a-service> Last Visited: 21/03/2017
- [8] <https://www.servicenow.com/everything-as-a-service.html>. Last Visited: 19/03/2017
- [9] Diagram is taken from <http://www.brighthub.com/environment/green-computing/articles/127086.asp>
- [10] 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
- [11] https://www.researchgate.net/publication/3278329_Biometric_security_technology Journal of Network and Computer Applications 2012
- [12] 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.