iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1116

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Cloud Computing Security and Biometrics

Dr. Divyakant Meva[1], Dr. Kalpesh Popat[2]
[1, 2]*Faculty of Computer Applications, Marwadi University, Rajkot, Gujarat*

Abstract: With the increased usage of cloud computing, there is a need to address the security issues also. No. of techniques have been proposed and is there in use. Still there are few problems related to authentication in cloud environment. This paper throws a light on such problems and their solution with the use of Biometric techniques.
Keyword: Cloud computing, Biometrics, Security

I. INTRODUCTION

In the era of internet, it is required to maintain security of the resources as well as transaction of data online. In the current era of internet, we are still using password authentication mechanism for authentication and authorization of the user. But it is required to have more robust and more secure mechanism. Another problem with password mechanism is to remember many accounts on the internet and also remembering password of each. Instead of that we can go for biometric authentication for internet user authentication services. Till this date, biometric services are being used for personal verification in organizations as server based or standalone systems.

But in the emerging era of cloud computing, it needs to be implemented, so that we can have more processing capabilities with increasing number of users and more system storage capabilities and can maintain unique identity of the users.

If we consider the example of UID – Aadhaar card, behind which the objective is to maintain single identity proof of the Indian national, they also require to store fingerprints data of all the users as well as facial database. The same database can be used by different authorities of Indian Government for various legal purposes.

Fig 1.Aadhaar Card Sample

For the above stated purpose, it is required to store the database on cloud environment and should be accessible by different authorities.

II. CLOUD COMPUTING AND BIOMETRICS

A. Cloud computing

As per the definition given by NIST, Cloud computing is 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 [1].

Essential characteristics:

1) On-demand self service
2) Broad network access
3) Resource pooling
4) Rapid elasticit
5) Measured service
6) Private cloud
7) Community cloud

8) Public cloud
9) Hybrid cloud

B. Biometrics

Biometrics is a technology which uses physiological or behavioral traits of a human being for the purpose of either identification or verification. The widespread use of biometrics technology is there now a day because of no need to remember any password or other things or no need to carry something like token or smart card with you. The person will be identified based on his unique physical or behavioral characteristics.

Commonly used biometrics technologies are: fingerprint, face, hand geometry, iris, retina, voice, keystroke etc.

The following can also be considered as benefits of biometrics technology:

1) Robustness
2) Distinctiveness
3) Availability
4) Accessibility

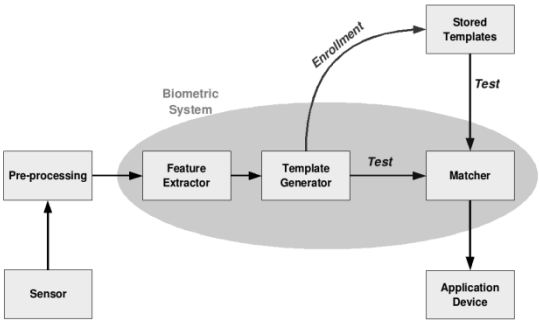


Fig 2. Typical working of Biometric system

As shown in the figure 2, initially sensor in the hardware device captures the image of the trait. Then preprocessing is done in the second phase e.g. thinning of the image, rotating the image. Then, in the next phase, feature extraction is done from the image. And template is generated from the extracted feature. In the next phase, matching is done with template. And at the end, result is generated as positive or negative identification or verification.

Now let us take a look at the scenario of Cloud and Biometrics.

III. CHALLENGES IN BIOMETRIC PROGRAMS

A. Abel Sussman[2] in his presentation debated the following challenges for advances in biometrics program:

1) Management and development of more efficient and effective large-scale operational capabilities
2) Establishment of standards for plug-and-play performance and system interoperability

B. Other challenges are

1) The ability to collect, share and consolidate meaningful biometric information
2) The ability to analyze biometric information in a timely and efficient manner
3) The ability to use biometric information to support authentication and authorization processes

Most of the existing biometric systems have reached limits of their scalability because of expanding needs and growth in population. The important question is to have architecture for large scale biometric identity management system.

C. The following are the requirements for next generation biometric systems:

1) Access data stored in different standards
2) Accommodate flexibility with biometric matchers
3) Allow real time calibration aligned with ROC curve
4) Prove flexibility in expected response and search speed
5) Implement failover, recovery and distribution of data services
6) Implement a model for data sharing

7) Provide data consistency
8) Allow data sharing between applications
9) Provide controlled parallelism

In addition to the above requirements, it is necessary to consider the challenges related to legislation aspects of cloud and biometrics technology. Other concerns are privacy and data protection [3].

IV. CLOUD BASED BIOMETRIC SERVICES

Cloud computing provides cost efficient processing and management solutions for Biometrics. The following key points must be considered when building cloud based biometric services:

1) Design fault tolerant software so the system can be built over inexpensive commodity hardware
2) Distribute the data and processing to maximize aggregate disk I/O throughput and enable redundancy
3) "Move the computation to the data" to minimize data copy/transit costs and thus decrease query and processing latency
4) Exploit parallel processing and distributed storage to the highest degree possible to promote linear scalability and linear speedups
5) Use innovative information retrieval techniques to speed up searches by reducing the search space and heavily parallelizing searches
6) Aggressively eliminate scalability bottlenecks

Peter Peer et al. suggested the following architecture for cloud based biometric services:

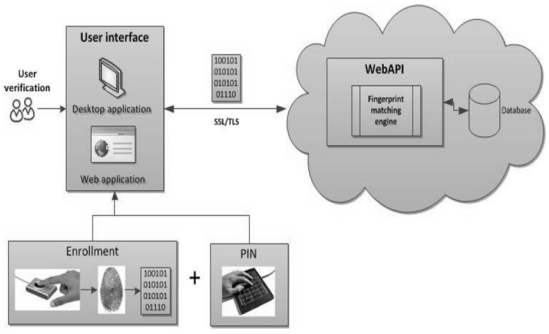


Fig. 3 Biometric verification system in cloud computing environment [3]

As shown in Figure 3, the following steps must be considered in implementation:
The fingerprint of a given user is first captured via a fingerprint scanner (here scanner libraries that allow capturing fingerprint images need to be integrated into the local (desktop or/and web) application);
The application then communicates through a (REST) API with the biometric web service hosted in the cloud and sends an encoded image to the fingerprint processing library (i.e. FingerIdent library) that provides the functionality for the cloud service;
The transmitted fingerprint image is processed in the cloud and finally the result is sent back to the local application.

A. IaaS component

IaaS contains outsourcing of servers, storage and network.

1) Virtual servers – They are main point of contact for business. The main component for virtual server is Biometric operating system supporting open and closed operating systems like Windows, Linux etc.
2) Storage –Biometric templates are stored at this level.
3) Networks – Biometric service in the cloud will have connectivity to biometric devices at physical locations of business. Each biometric application in cloud will have unique IP address, so that the business and its cloud based infrastructure can be identified uniquely.

B. SaaS component

The SaaS component may have two options:

1) COTS approach or purchase on demand
2) A software platform where customized development may take place

The business can have either customized development as per their requirement or they can purchase software from Biometric system vendors.

C. PaaS component

PaaS not unique like SaaS and IaaS, but simply they are vehicle for application development. The PaaS will support larger biometric applications, such as 1:N identification.

BioID has implemented powerful face and voice biometric services for cloud known as BioID Web Services (BWS). This is cost effective pay-per-use model. It is also device independent. Another is FingerID@Cloud, which is cloud based fingerprint verification system. It is scalable for performance and storage requirements. Another example is GoCloudId providing cloud authentication with biometric services for payment gateway.

V. ADVANTAGES AND DISADVANTAGES OF BIOMETRIC SERVICES IN CLOUD ENVIRONMENT

A. As far as implementation is concerned, we can think of the following advantages:

1) Time to set up environment is less.
2) It is on demand.
3) It is affordable
4) It is highly scalable
5) Redundancy is easy and cost effective

B. The following are disadvantages of Biometric technology in Cloud:

1) Changes in biometric business processes.
2) Cloud resources need to be scalable on demand.
3) Legal and privacy rights can become serious issues.

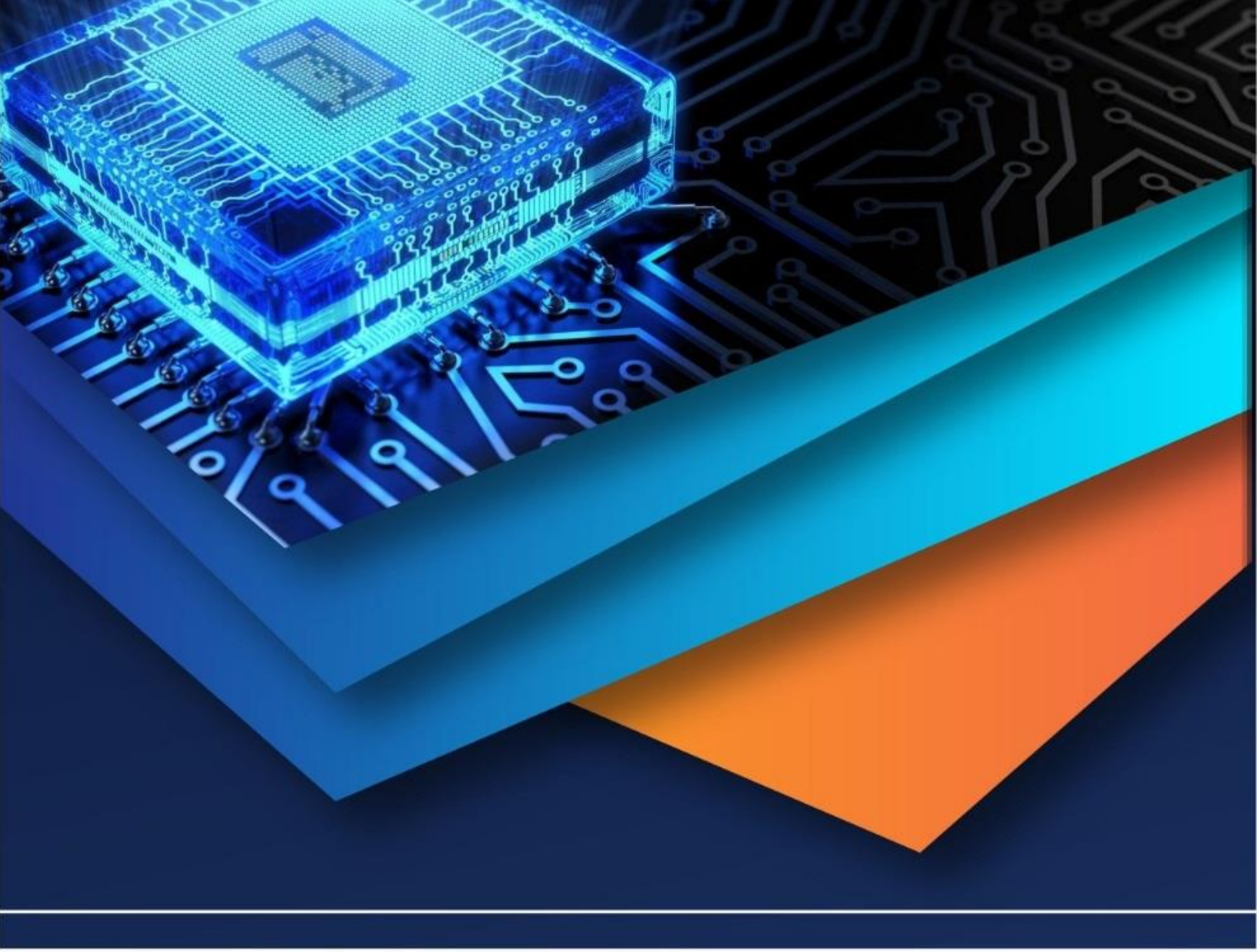
Another issue is about acceptance of Biometric technology in the geographical region. In developing countries, this acceptance rate is fast. But in the developed countries like USA, this rate is slow. This will play a role of catalyst in modelling Biometrics in Cloud environment.

VI. CONCLUSION

Clearly, deploying Biometric services in cloud environment is solution for the problems of scalability and time as well as access. But it will take a time to prove its acceptance and implementation. Few of the solutions are available in the market nowadays provided by Animetrics, BioID and Face.com. Another example is fingerprint services implemented by e-learning platform – Moodle. Another area of research is to implement multimodal biometric systems in cloud environment. Undoubtedly, implementing Biometric services on the cloud is the solution of the problems of scalability and performance for next generation.

REFERENCES

[1] Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, Special publication by NIST, Sept, 2011
[2] Abel Sussman, “Biometrics and Cloud Computing”, Biometrics Consortium Conference, 2012
[3] Peter Peer et al., “Building Cloud based Biometric Services”, Informatica, 2013, pp. 115–122
[4] Ravi Das, “Biometrics in the Cloud”, Keesing Journal of Documents & Identity, 2013, pp. 21-23



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY