International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

REVIEW ON BIOMETRIC TECHNOLOGIES IN CLOUD COMPUTING

Sumitha.J[1], Arish Venkat.M.B[2], Saranath.J[3]

[1]Assistant Professor, Department of Software Systems, Sri Krishna Arts and Science College, Tamil Nadu, India.
[2]Student, Department of Software Systems, Sri Krishna Arts and Science College, Tamil Nadu, India.
[3]Student, Department of Software Systems, Sri Krishna Arts and Science College, Tamil Nadu, India.

---***---

Abstract - *Cloud computing is fast developing technology to have better utilization of storage and security aspects all over the world. Using cloud computing we can access files, database, data, files and operating systems. Cloud computing is a web based service used with help of internet connection. Cloud computing has certain stages private, protected, public. In this platform user can develop their own software for their personal uses for example it is used in business fields, corporate sectors. The data we enter in it will be safe. These type of authentication is done by biometric cloud computing. This biometric is used for safeguard the data which is stored inside the cloud. It has many types of biometrics in it. Generally "bio" means human or living thing, "metric" refers that measurement or calculation, so biometric means to human measurement. Various types of biometric authentication are there few are listed here finger print, face recognition and keystroke*.

Key Words: **Cloud Computing, Biometric, Authentication**

1. INTRODUCTION

Cloud computing provides a variety of computing sources and storage to applications over the networking. Pay for what we use is known as Cloud computing. The Cloud computing allows the user without installation of software and applications in the computer. Cloud computing prefers change the way of computer applications and services that provides delivered managed. It is a model to enable the data and information over the access of network. Cloud computing enables each kind of application system according to need to again the computation strength, the storage space and each kind of software services.

The Cloud computing is a platform were thousands of operators are working in the Cloud centre all over the world. The data we stored in Cloud computing are not stored in our hardware and ram. It can be used to access the personal data in any of the system over a network. The Cloud can maintain and manage the sources by itself on large scale networking process. In day today's life Cloud computing are most probably used in technological devices and computers. Many companies and businesses sector are running under Cloud computing for the usage of data transfer and communications are shown in the fig 1.

Mobile
Storage
Applications
CLOUD COMPUTING
Server
Database
Private cloud
Public cloud
Hybrid cloud

Fig -1: **Cloud Computing**

2. CLOUD COMPUTING DEPLOYMENT MODELS:

There are four primary deployment models of Cloud computing are shown in fig 2 and are explained as follows:

2.1 Public Cloud:

It is common which is used by everyone on web – services, web applications. It can be used by anyone through network in means of public sector. It is maintained by the help of public organisation.

2.2 Private Cloud:

Private Cloud is used by a organisation to store the data but only one organiser can access their web applications and other services. It cannot be accessed by everyone in that organisation. It is not like public Cloud.

2.3 Hybrid Cloud:

This Cloud refers to the combination of two or more Clouds (public, private, community Cloud). It is a platform were multiples of externals and internals can be operated in the Cloud computing. For example, an organisation which is used for web services like IBM and etc..,

2.4 Community Cloud:

It is a mixture of two Clouds private, public and hybrid Cloud. It can be accessed by internal or anyone. It is accessed by the organisation with the Cloud security. Its cost is lesser than public Cloud. Even this Cloud also maintained privately.

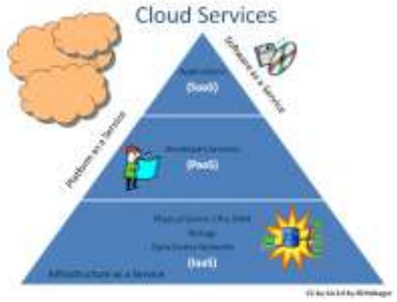


Fig -2: Cloud Deployment Models

3. CLOUD COMPUTING SERVICES:

The term “Service” provides access to the cloud users by using web browser and it plays a major role in cloud computing. The Primary Services are given shown in fig 3.The services have different types of abstraction levels with their architecture. The Services provided by the vendors are of three types they are explained as below.

3.1 Infrastructure as a service: PaaS

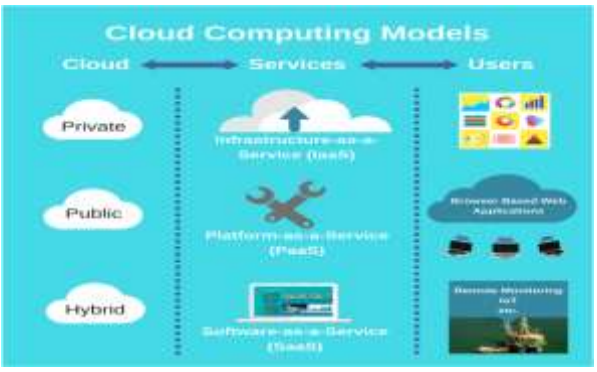
It is easy and quick service provider to computing sources. It is equipment used to support the operations done in Cloud. Its main source is to support the user in needs of helpful. Most probably used in networking components and other resources for E.g.: IBM and telecom providers.

3.2 Software as a service: SaaS

It is web based service. SaaS provides the user to access over networking (internet) instead of installation of application software. It is commonly used in business sectors were the vendors will run the computer on behalf of their applications instead of buying it for example Google, Gmail, yahoo, salesforce.com and etc.

3.3 Platform as a service: PaaS

It accesses the software development platform to allow them to create the new Cloud applications based on the programming language libraries, services and tools. User should control over the applications. Using internet PaaS users can access their resources like application building and they can also user their services by without any need of installation of software.


Cloud Computing Models
Cloud
Services
Users
Private
Public
Hybrid
Infrastructure-as-a-Service (IaaS)
Platform-as-a-Service (PaaS)
Software-as-a-Service (SaaS)
Browser Based Web Applications
Remote Monitoring IoT etc.

F
ig -3: Cloud Computing Services

4. OVERVIEW OF AUTHENTICATION:

The meaning of authentication is to process an action that needs to be proved with the needs of valid information. For example is most probably used in websites like Cloud computing for security purpose. Authentication methods are proof of knowledge, proof of possession, and proof of characteristics.

1. Proof of knowledge has few types PIN number, password and phone number.
2. Proof of possession has their type’s smart card, tokens and driving license.
3. Proof of characteristics with the few types finger print, face reorganization, iris, retina and signature pattern.

Proof of knowledge refers that something what we know it is used by every user for an application. Its basic task is to identify the person’s login using password or PIN. Most of the users tend to common password on multiple web sites [1].

Proof-of-possession is not safety in day today’s life because possibilities of loss of smart card, driving license etc. These kind of proof are threat or stolen easily by the hackers. So it is not the safety one.

Proof-of-characteristic focuses on the human’s characteristic by verifying their identity. We have introduced some significant improvement over the above schemes in-order to improve the process of authentication in the cloud environment [8].

More than the knowledge or possession the characteristic is more safety to use in application because it is used only by the means of human body like finger print, Iris, face image. The only major drawback of this authentication is that in many instance, there is a need for an external hardware device to facilitate the authentication process [1].

5. ROLE OF BIOMETRIC IN AUTHENTICATION:

Biometrics generally refers body measurement and calculations. The security factor in the biometric security system in highly improvised by concatenating the data with a unique physical quality [2]. Biometrics identifiers are used to label and describe about the individuals. The token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems are called as traditional methods of biometric.

Biometric security devices are easy to identify the unique characteristics of a human. Main purpose of using biometric security is extremely difficult for someone to break into a system. Biometrics can be used by anyone in day today's life. There are lots of attributes that could be used for identification purposes. With these attributes, probably the fingerprint was the first one to be examined in more systematic manner. Everyone's finger forms of a unique pattern of different loops, spirals and curves of very high but still finite diversity [5].

In biometric authentication the person is verified at starting of the process and then allowed to process the process. It is an interface between individual users in the means of physical characteristics. Biometrics can't be easily broke or hack by any person because it is a security system. If a user wants to use a Cloud he/she must enrol their name along with finger print, Iris etc. The biometric database of the user is maintained by the authentication service provider [2]. User should register their details in Cloud platform and once it is completed the details are stored in database of Cloud

6. TYPES OF BIOMETRICS:

There are two types of biometric which are involved in securing the data and the information from the third party. They are: Physical Biometrics and Behavioural Biometrics are shown in the following fig along with real time example.

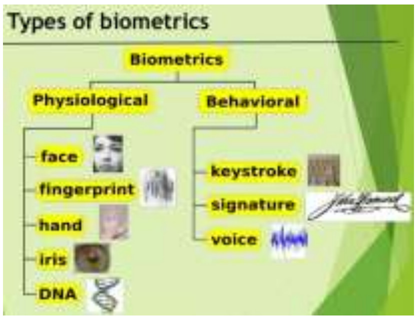


Fig 4: Types of Biometric

6.1PHYSICAL BIOMETRICS

Physical biometrics is based on the measurement of human part of the body. The various leading physiological biometrics techniques are finger print, Iris-scan, facial recognition, palm print and hand geometry and etc [2]. After the scanning only the next process is valid. It can be quickly scanned.

6.2 BEHAVIOURAL BIOMETRIC:

Behavioural biometrics is a study to measure the unique identification and measure patterns in human activities. This biometrics verification includes keystroke dynamic, signature, voice id. This biometrics is used for secure purpose in financial institution, businesses, and government fields. Biometric data are gathered and verified, after it gathered it picks up a software application to match the points of data.

7. DIFFERENT BIOMETRIC METHODS:

7.1*Finger print*:

The finger print is a highly distinctive feature in human beings as no two individuals share the same finger prints. It is best proof for authentication while performing. It is most powerful Authentication technique.

7.2 *Palm print*:

This palm print is similar to finger print scanner. It is mostly used in biometrics authentication process. The sub characteristics used to authentication include principal lines, wrinkles, ridges, proximal transverse crease, pores, minutiae etc [1]. Palm print is better than finger print.

7.3 *Iris identification*:

Iris identification is a method of identifying people based on unique patterns within the ring shaped region surrounding the pupil of the eye [3]. Iris recognition is similar to face scan which is most commonly used in common places.

7.4 *Hand Geometry*:

This authentication mechanism involves the study of hand geometric features such as thickness, width of palm, length and width of fingers in minute level to facilitate verification [1]. It identifies user by the shape of their hand. Hand geometry scans in many dimensions and measure the hand of the user for which the measurement stored in file is correct or not then only it can process the next step of the security level.

7.5 *Face recognition*:

The face recognition is done using the help of human face. This face recognition is done by identifying and analyzing patters based on the persons facial contours. This process can be more secure or valuable for many fields. Face recognition is verified using eyes, eyebrows, nose, chin, lips of mouth and hair.

7.6 *Keystroke dynamic*:

Keystroke is based on the habitual rhythm patterns in the way a person types [3]. Keystroke dynamic is part of larger classes of biometrics known as behavioural biometrics. It contains persons typing speed, time required between specific key and time required of that keys are released.

7.7 Voice recognition:

This voice recognition is used to check the voice of human like pitch, tone, frequency, etc. It is also known as speech recognition system. This technology is less in cost, easy to use non-intrusive [3]. The voice can be varied in terms of their vocal frequency. The drawback is that the voice of individual can change with age, illness, mental state [1].

7.8 Signature recognition:

Signature recognition is verified using the human static sign image. The sign can be almost near to duplicate authentication. The static signature recognition provides scope for forgery as cyber criminals can easily replicate a sign to look similar to that of an image and that is a drawback [1].

Fig 5: Biometric Authentication Icons

8. SECURITY CHALLENGES IN BIOMETRICS

The biometric features, although unique, face several threats in reality. One of the most common threats involves spoofing, where by users biometrics templates can be misused [7]. One of them is that person uses fake biometrics during enrolment. People use fake template to open the source to replace their biometrics. Imposters can easily enter into system because of increase in false acceptance rate (zero-effect attack) [7]. Many challenges can be faced in biometrics by using fake templates.

These are the challenges faced in feature technology

1. Access data stored in different standards.
2. Accommodate flexibility with biometric matchers.
3. Allow real time calibration.
4. Flexibility s given in the response as well as in the speed
5. Implementation of failure, recovery and shared data services.

CONCLUSION:

Cloud Computing is said to a fast and efficient booming technology with lots of characteristics and benefits to the user in the society. Based up on the user's data the confidentiality of information should be safe guarded with more security parameters. Biometric authentication provides a better results in keeping the data with authenticity and it also is also a famous technology which is ruled by everywhere in the world to protect the data from third party. So as a solution to have a better data protection over the cloud channel we require more than one biometric tool to have a better secured environment. This paper en lights about the biometric which are available for the security. In future our future will be focusing on the cryptography techniques which are based on the biometric methods.

REFERENCES

1. Akshay A.pawle, Vrushsen P. Pawar. A study of different biometric authentication techniques in Cloud computing.
2. Dr. Divyakant Meva, Dr. Kalpesh Popat,"Cloud computing security and biometrics".
3. Jain.A,Hong.L,pankanti.S. biometrics identification
4. Martin drahansky. Biometric security systems.
5. P.Padma, Dr.S.Srinivasan ,"A survey on biometric based authentication in Cloud computing"
6. Shivashish ratnam, mimzee gupta, Dr.ajay S.singh, Thirunavukkarasu.K,"A survey on biometric security technologies from Cloud computing perspective".
7. Tapalina bhattasali, Khalid saeed, nabendu chaki, rituparna chaki, "A survey of security and privacy issues for biometrics based remote authentication in Cloud",