**CHAPTER 1**

**INTRODUCTION**

Information Technology has always been considered a major pain point of enterprise organizations, from the perspectives of both cost and management. However, the information technology industry has experienced a dramatic shift in the past decade – factors such as hardware commoditization, open-source software, virtualization, workforce globalization, and agile IT processes have supported the development of new technology and business models. Imagine yourself in the world where the users of the computer of today’s internet world don’t have to run, install or store their application or data on their own computers, imagine the world where every piece of information or data would reside on the Cloud (Internet).

As a metaphor for the Internet, "the cloud" is a familiar client, but when combined with "computing", the meaning gets bigger and fuzzier. Some analysts and vendors define cloud computing narrowly as an updated version of utility computing: basically virtual servers available over the Internet. Others go very broad, arguing anything to consume outside the firewall is "in the cloud", including conventional outsourcing.

Cloud computing is currently one the most hyped IT innovation Cloud computing technology is a new concept, which provides great opportunities in many areas. Cloud computing is a collection of computers and servers that are publically accessible via internet . Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing provides the variety of internet based on demand services like software, hardware, server, infrastructure and data storage.

**Benefits of Cloud Computing**

1) Increase throughput – Cloud computing get more work done in less time with less people.

2) Reduce costs – In cloud computing, user shares computer hardware, software and data so there’s no need to spend money on hardware or software.

3) Improve accessibility – In cloud computing user can access data, files anytime from anywhere via internet.

4) Requires Less Training – Cloud computing takes fewer people to do more work. So there is requirement of minimum training of hardware, software problems to user.

National Institute of Standard and Technology (NIST) describes cloud computing with five essential characteristics such as on-demand self-service, broad network access, rapid elasticity, measured service, and resource pooling, three service models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) and also four deployment models such as public, private, community, and hybrid



**Fig 1.1 Services By Cloud Computation**

**1.1 Characteristics**

1) **On-demand self-service** – Cloud provides all needed computing resources as per requirement to user.

2) **Broad network access** – User can access cloud services using desktop, laptop, mobile phone etc. over the internet

3) **Resource pooling** – Cloud provider schedules resources to the user as per their requirement.

4) **Rapid elasticity** – Cloud computing has ability to quickly allocate and de-allocate the services as per requirement.

5) **Measured service** – Cloud providers controlling on usage of resources.

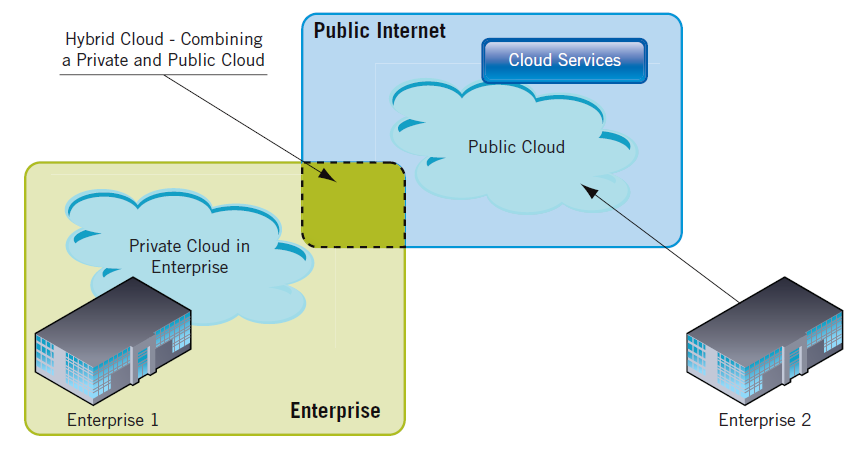
**1.2 Services**

1) Software as a Service (**SaaS**) – In the SaaS model, cloud provider delivers application softwares like MS-OFFICE, Turbo C etc. as a service to cloud user

2) Platform as a service (**PaaS**) – In PaaS model, cloud provider deliver a computing platform like operating system, database, web server etc. to the cloud user.

3) Infrastructure as a Service **(IaaS**) – Main objective of any company is to reduce time and money. IaaS model is used to fulfill these primary objectives.

**1.3 service Models**

******

**Fig 1.2 Service Models**

1) Public – This type of cloud model available for all users.

2) Private – This type of cloud model specifically applicable only for private company.

3) Community – This type of cloud model is shared by several companies and supports to a specific community.

4) Hybrid – This type of cloud model is a combination of two or more clouds.

According to international data corporation (IDC), there are several issues or challenges in cloud computing like security, availability, performance, on demand payment model may cost more, lack of interoperability standards, bringing back in-house may be difficult, how to integrate with in-house IT, and not enough ability to customize. According to the IDC’s survey on the cloud services, security concerns are number one issue facing cloud computing. To remove security issues specifically to identify authorized user, we proposed a new biometric authentication system called as face recognition system (FRS).

**1.4 Authentication In Cloud**

As cloud users store their information to various services across the Internet, it can be accessible by unauthorized people. So security is the most important issue in cloud computing. To provide security we require proper authentication technique in cloud computing. Typically, authentication is done based on information about one or more of the following:

i. Knowledge of the subject, such as password or secret information.

ii. Possession of the user, such as smart card, passport, driver’s license, etc.

iii. Biometric traits of the client, such as fingerprint, The data leakage and security attacks can be caused by insufficient authentication Cloud services are paid services so to identify authorized user is major concern in cloud computing. In this paper, we focus on the security issues of cloud computing, particularly on authentication. To solve authentication problem in cloud computing, there are

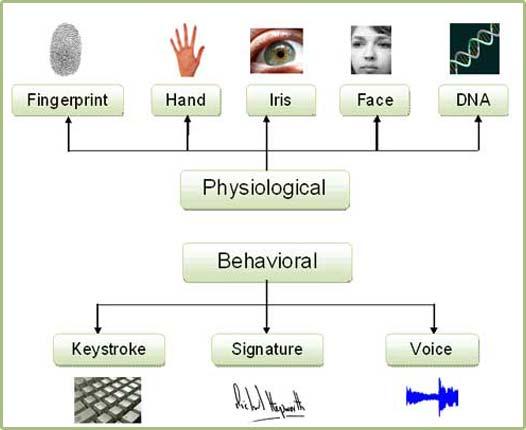
## 1.5 Key Characteristics

* **Cost** is greatly reduced and capital expenditure is converted to operational expenditure. This lowers barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and minimal or no IT skills are required for implementation.
* **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they are using, e.g., PC, mobile. As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet the users can connect from anywhere.
* **Multi-tenancy** enables sharing of resources and costs among a large pool of users, allowing for: (gt)
  + **Centralization** of infrastructure in areas with lower costs (such as real estate, electricity, etc.)
  + **Peak-load capacity** increases (users need not engineer for highest possible load-levels)
  + **Utilization and efficiency** improvements for systems that are often only 10-20% utilized.
* **Reliabilit*y*** improves through the use of multiple redundant sites, which makes it suitable for business continuity and disaster recovery. Nonetheless, most major cloud computing services have suffered outages and IT and business managers are able to do little when they are affected.
* **Scalability** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads. Performance is monitored and consistent and loosely-coupled architectures are constructed using web services as the system interface.
* **Security**typically improves due to centralization of data, increased security-focused resources, etc., but raises concerns about loss of control over certain sensitive data. Security is often as good as or better than traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. Providers typically log accesses, but accessing the audit logs themselves can be difficult or impossible.
* **Sustainabilit*y*** comes about through improved resource utilization, more efficient systems, and carbon neutrality. Nonetheless, computers and associated infrastructure are major consumers of energy.

**CHAPTER 2**

**BIOMETRICS**

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearences.



**Fig 2.1 Biometrics Types**

Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be.

Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. Its nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

**2.1 Traditional Authentication Techniques**

1) Password – A login and password combination is the most universally used method of authentication but it is not secured . It is very easy to hack by tools.

2) OTP – OTP is a One Time Password wherein password is provided upon request. An OTP can prevent a password from being stolen and reused. This password is valid for a limited period of time and can only be used once. These systems are expensive.

**2.2 Biometrics Authentication Techniques**

Biometrics is most widely used security system now-a-days. It is helping to overcome a lot of drawbacks of above mentioned techniques of authentication. Biometrics can be defined as an automated methodology to uniquely identify humans using their behavioral or physiological characteristics . That is biometrics is used as an authentication wherein the password is human organs or physiological characteristics. There are several biometrics techniques as stated below,

1) **Voice Recognition** – As the name suggests voice recognition involves authentication with respect to vocal data. Voice recognition is used to authenticate user’s identity based on patterns of voice pitch and speech style. But a user’s voice can be easily recorded and may use by unauthorized user. Also voice of a user may change due to sickness, so making identification is difficult.

2) **Signature Recognition** – Signature recognition is used to authenticate user’s identity based on the traits of their unique signature. People may not always sign in a consistent manner so verifying an authorized user is difficult.

3) **Retinal Recognition** – Retinal recognition is for identifying people by the pattern of blood vessels on the retina. But this technique is very intrusive and expensive.

4) **Iris Recognition** – Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. As like retina this technique is also intrusive and expensive.

5) **Fingerprint Recognition** – Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. The dryness of fingers, soiled fingers can affect the system and it can show error.

6) **Hand Geometry Recognition** – Hand Geometry biometrics is based on the geometric shape of the hand. It includes the size of the palm, length and width of the fingers etc. But this technique has some drawbacks like not ideal for children as with increasing age there hand geometry tend to change, constant use of jewellery will result into change in hand geometry, not valid for persons suffering from arthritis, since they are not able to put the hand on the scanner properly.

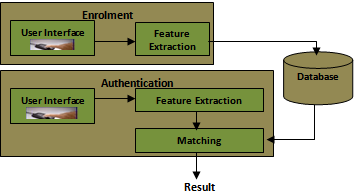
7) **Palm recognition** – Palm recognition is based on ridges, principal lines and wrinkles on the surface of the palm. This technique is very expensive and not appropriate for children as there lines of palm change once they are fully grown up.

**CHAPTER 3**

**SYSTEM ANALYSIS**

All the mentioned techniques before tend to tell us that none of it is feasible & not much useful due to its various drawbacks. To overcome drawbacks of all these security techniques and to provide proper security for user authentication in cloud computing, we proposed to use a biometric technique called *“***FACE RECOGNITION”.**

The human face plays an important role in our social interaction. Facial recognition is one of the preferred methods of biometrics because it is a neutral, non-intrusive, easy-to-use, which requires minimal physical contact as compared with other biometrics systems. Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips, and chin or on the overall analysis of the face image that represent a face as a number of recognized faces.Face image can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person. Face Recognition System (FRS) enables only authorized users to access data from cloud server



**Fig 3.1 Face Recognition**

**3.1Why We Choose Face Recognition Over Other Biometric**

There are a number reasons to choose face recognition. This includes the following

1. It requires no physical interaction on behalf of the user.
2. It is accurate and allows for high enrolment and verification rates.
3. It does not require an expert to interpret the comparison result.
4. It can use your existing hardware infrastructure, existing camaras and image capture devices will work with no problems.
5. It is the only biometric that allow you to perform passive identification in a one to many environment (eg: identifying a terrorist in a busy Airport terminal.

**CHAPTER 4**

**ARCHITECTURE OF FACE RECOGNITION SYSTEM**

Face recognition is a biometric security system. As the name suggests the face acts as a password for the systems. Face recognition security system is shown in the figure 2. Where, we proposed authentication scheme using face recognition system (FRS).



**Fig4.1 System Architecture**

As the diagram explains we have login option for the user after which the verification is conducted using face of the person. Detailed architecture is explained below



**Fig 4.2 Face Recognition System (FRS)**

Now let us elaborate each phase in detail and understand it.

1) **Image Capture** – It is the step where image of the person is captured wherein his or her face is visible. In case of 2D facial recognition, a digital camera with normal resolution is needed.

2) **Face Detection** – Face detection involves identifying the face in the captured image. In simple words only the face of the person is seized & all other parts of the images are eliminated

3) **Alignment** – The face captured in the camera may not be completely perpendicular to the camera and hence the alignment needs to be determined and compensated so that it is ready to use of recognition process.

4) **Feature Extraction** – Feature extraction involves a process of measuring various facial features and creating a facial template, for the purpose of matching and identification.

**4.1 Face Recognition System For User Authentication**

**Step I – New User Registration**

Whenever user wants to access cloud resources, user has to register first on to the cloud server.



**Fig 4.3 New User Registration steps in Cloud using FRS**

Following are the steps to register on the cloud server.

1) User has to fill the registration form which is provided by cloud provider. It contains detail information about the user.

2) User has to provide valid Email ID as a username to the face recognition system at the time of registration.

3) Face recognition system checks the Email ID against the availability of that username. Username should not repeat or match with existing user’s username.

4) After checking the availability of username, the password must be created. Face image through web camera is stored in database as a password.

5) After providing valid username and storing face image as a password, the registration on cloud server is completed.

**Step II – Registered User Login**

When registered user wants to access resources on the cloud server, then registered user should login on to the cloud server. Following are the steps to login on to the cloud server.



**Fig 4 . 4 Registered User Login steps in Cloud using FRS**

1) User should enter valid username in his login interface which was already provided by the user at the time of registration. And for password user’s face is captured by web camera.

2) Face recognition system checks the username and face image as a password provided by the user.

3) After matching the username and face image as a password, face recognition system provides access of cloud services to the user.

4) If username or face image does not match then face recognition system displays an error message.

**4.2 Advantages**

In this proposed system, there are security advantages as stated below,

1) **Non-intrusive**

Does not change its timing or processing characteristics. **Nonintrusive** testing usually involves additional hardware that collects timing or processing information and processes that information on another platform

2) **Unique** I

Independent system, biometric is an intellectual part of human and hence system remains unique.

**3) Cheap Technology**

Technology implementation does not requires much resources and hardware support also,it could need hardware only in the time of face image collection. Apart from that resource utilization is minimal. Arrives for cost effective system.

**4) Fast Identification**

As biometric used along with cloud computation, technology deals everything in the terms of internet, so only need of fast computation, makes works to b faster.

**4.3 Applications**

* Replacement of PIN,physical tokens
* No need of human assistance for identification
* Prison visitor systems
* Border control
* Voting system
* Computer security
* Banking using ATM
* Physical access control of buildings, areas etc

**CONCLUSION**

The services of cloud computing is based on the sharing. Cloud computing provides variety of services like Iaas, SaaS, and PaaS. These services are paid services, so security is a major concern to identify authorized user in cloud computing. To provide cloud services only to the authorized user, secure authentication is necessary in cloud computing. There are so many authentication techniques like password, OTP, Voice recognition, finger recognition, palm recognition etc. but still it has some drawbacks like at times password techniques are not feasible, password can be easily stolen by hacker or if user uses complex password, user may forget that password etc. So it is a better option to use face recognition system rather than traditional or other biometric authentication techniques. The security level of cloud provider in terms of secure authentication is much improved by using face recognition system.

**REFERENCES**

[1] Rajesh Piplode and Umesh Kumar Singh, “An Overview and Study of Security Issues & Challenges in Cloud Computing,” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume-2, Issue-9, September 2012.

[2] P. Senthil, N. Boopal and R.Vanathi, “Improving the Security of Cloud Computing using Trusted Computing Technology,” International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Volume-2, Issue-1, Jan-Feb 2012, pp-320-325.

[3] Ganesh V. Gujar, Shubhangi Sapkal and Mahesh V. Korade, “STEP-2 User Authentication for Cloud Computing,” International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume-2, Issue-10, April 2013.

[4] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, “Research Challenges and Security Issues in Cloud Computing,” International Journal of Computational Intelligence and Information Security, Volume-3, No-3, March 2012.

[5] Nils Gruschka and Meiko Jensen, “Attack Surfaces: A Taxonomy for Attacks on Cloud Services,” Proceedings of the IEEE 3rd International conference on Cloud Computing, 2010, PP-276-279.

[6] Minhaz Fahim Zibran, “Biometric Authentication: The Security Issues,” University of Saskatchewan, 2012. [8] S. O. Kuyoro, F. Ibikunle and O. Awodele, “Cloud Computing Security Issues and Challenges,” International Journal of Computer Networks (IJCN), Volume-3, Issue-5, 2011.

[7] Maninder Singh and Sarbjeet Singh, “Design and Implementation of Multi-tier Authentication Scheme in Cloud,” International Journal of Computer Science Issues (IJCSI), ISSN: 1694-0814 Volume-9, Issue-5, No-2, Sep. 2012.