**ABSTRACT:**

In this paper, we introduce a new Multi access System for cloud Computing Services Specifically, in our proposed access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a Trustee request. User can’t able to access the cloud data without secret key and trustee request, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfils the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed system.

**EXISTING SYSTEM:**

* Cryptography is the one the most important method to generate the public key.This on-line mediator is referred to a SEM (Security Mediator) since it provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer.
* The general idea of key-insulated security was to store long-term keys in a physically-secure but computationally-limited device. Short-term secret keys are kept by users on a powerful but insecure device where cryptographic computations take place. Short term secrets are then refreshed at discrete time periods via interaction between the user and the base while the public key remains unchanged throughout the lifetime of the system.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Key-insulated cryptosystem requires all users to update their keys in every time period. The key update process requires the security device.
* Once the key has been updated, the signing or decryption algorithm does *not*require the device anymore within the same time period.
* Normal authentication like login form is not much secure. Security should be very important for accessing the file in cloud. It should be not implemented in previous system.
* It is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser.
* The adversary acts as the role of the cloud server and tries to find out the identity of the user it is interacting with.
* Access without Secret Key: The adversary tries to access the system (within its privileges) without any secret key. It can have its own security device

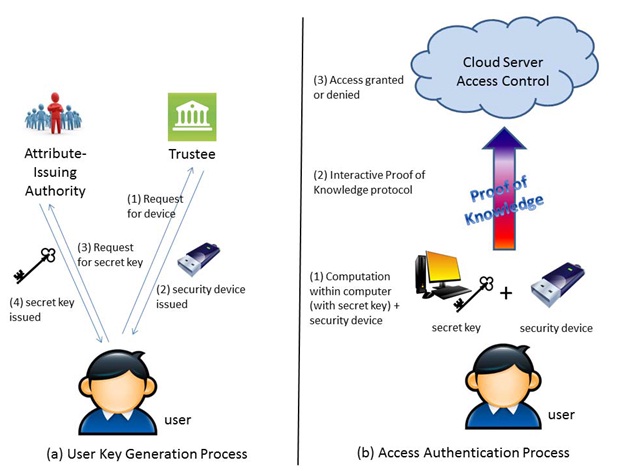
**PROPOSED SYSTEM:**

* With this System, our protocol provides a security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security System should be also connected to the computer in order to authenticate the user for accessing the cloud. The user can be granted access only if he has both items.
* Furthermore, the user cannot use his secret key with another device belonging to others for the access. Our protocol supports Multi access System for cloud Computing Services which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user. To show the practicality of our system, we simulate the prototype of the protocol.

**ADVANTAGES OF PROPOSED SYSTEM:**

* Our protocol supports Multi access System for cloud Computing Services which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user.
* To show the practicality of our system, we simulate the prototype of the protocol.
* Tamper-resistance. The content stored inside the security device is neither accessible nor modifiable once it is initialized. In addition, it will always follow the algorithm specification.
* It is capable of evaluation of a hash function. In addition, it can generate random numbers and compute exponentiations of a cyclic group defined over a finite field.
* Presented a new 2FA (including both user secret key and a lightweight security System) access control system for web-based cloud computing services.
* 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 2GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL