**Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services**

**ABSTRACT:**

In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, 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 fulfills 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 2FA system.

**EXISTING SYSTEM:**

* Mediated cryptography was first introduced as a method to allow immediate revocation of public keys. The basic idea of mediated cryptography is to use an on-line mediator for every transaction. 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.
* The traditional account/password-based authentication is not privacy preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems.
* 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:**

* In this paper, we propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.
* In this paper, we propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties. It can compute some lightweight algorithms, e.g. hashing and exponentiation; and it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.
* With this device, our protocol provides a 2FA security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through USB) 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 fine-grained attribute-based access 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 fine-grained attribute-based access 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 not accessible nor modifiable once it is initialized. In addition, it will always follow the algorithm specification.
* Capability. 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 device) 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:**



**MODULES**

* Data User Module
* Authority Module
* Trustee Module
* Cloud server

**MODULES DESCRIPTION**

**Data User Module**

* Every user need to register while accessing to cloud.
* After user registered, at the time of user login then user need to provide one time key to access user home.
* One time key will be provided by cloud. key will be corresponding user mail id.
* After user access the user home, User can view the all files upload in cloud.
* User need to send the file request for both trustee and authority.
* After user have the two factor access control, user can download the corresponding file.

**Two Factor Access Control:**

* If user need to access file in cloud. They need to get the two factor access control.
* 1. Trustee: Need to get security response from trustee for corresponding file.
* 2. Authority: Need to get secret key from authority for corresponding file.

**Authority:**

* Authority will upload the file in cloud. And uploaded file will store in drive HQ in encrypted format.
* Authority will give secret key for all files whenuser request for any file and the secret key will be send to corresponding user mail Id.

**Trustee Module**

* It acts as admin for cloud server.
* Trustee will give request for all files security response when user request for any file.

**Cloud Server Module**

* Cloud view uploaded files in cloud.
* Cloud view Downloaded files by user in cloud.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

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

**REFERENCE:**

Joseph K. Liu, *Member, IEEE*, Man Ho Au, *Member, IEEE*, Xinyi Huang, Rongxing Lu, *Senior Member, IEEE*, and Jin Li, “Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services”, **IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, MARCH 2016.**