ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Two-Factor Access Control Protocol Using a Lightweight Security for Cloud Computing Services

N.Poojitha[1], Prof. Bimal Kumar[2]

M. Tech Student, Dept of CSE, SSSS College, Affiliated to JNTUA, AP, India [1]

Associate Professor & HOD, Dept of CSE, SSSS College, Affiliated to JNTUA, AP, India[2]

ABSTRACT: Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources. Those advantages, ironically, are the causes of security and privacy problems, which emerge because the data owned by different users are stored in some cloud servers instead of under their own control. To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Data security is the key concern in the distributed system. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present 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.

KEYWORDS: multi-authority, attribute-based encryption.

I. INTRODUCTION

CLOUD computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a cloud It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users‟ control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users‟ data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user‟s attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.
They are counterparts to each other in the sense that the decision of encryption policy (who can or cannot decrypt the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

message) is made by different parties.

In the KP-ABE, a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user‟s identity (e.g. IIT AND (Ph.D. OR Master)). A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the keys, so the encrypted does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when are-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to there-encrypted files, and this process causes considerable problems in implementation. On the other hand, those problems and overhead are all solved in the CP-ABE [. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users‟ attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypted holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots**.**

II. LITERATURE SURVEY

K. Yang, X. Jia, K. Ren, and B. Zhang[4] This paper describes Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems.

W.-G. Tzeng [5], This paper describes propose efficient and secure (string) oblivious transfer (OT1n) schemes for any n

2. We build our OT1 n scheme from fundamental cryptographic techniques directly. The receiver’s choice is unconditionally secure and the secrecy of the unchosen secrets is based on the hardness of the decisional Diffie-Hellman problem.

S. Yu, C. Wang, K. Ren, and W. Lou[5] This paper describes Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

A. Shamir, [1] This paper introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other 's signatures without exchanging private or public keys, without keeping key directories , and without using the services of a third party. The scheme assumes t h e existence of trusted key generation centers, whose sole purpose is t o give each user a personalized smart card v when he first join st he network.

A. Sahai and B. Waters,[2] This paper introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, $\omega\_$, if and only if the identities ω and ω are close to each other as measured by the “set overlap” distance metric.

V. Goyal, O. Pandey, A. Sahai, and B. Waters,[3] This paper describes As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level(i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

III. 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

IV. PROPOSED WORK

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..

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

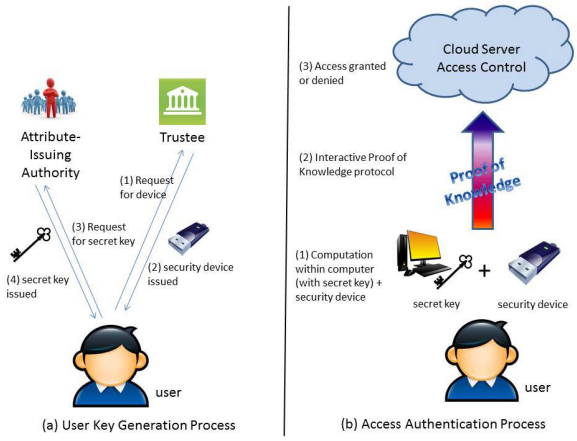

Fig 1.1: architecture of system

Implementation:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it‟s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

IMPLEMENTATION:

Attribute Authorities:
Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

Data Consumers:
Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:
Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

Cloud Server:
Then, the owner sends the encrypted data to the cloud server together with the cipher-texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

III. CONCLUSIONS AND FUTURE WORK

In this paper, a new 2FA (including each person secret key and a light-weight protection system) get entry to control system for internet-based cloud computing services is proposed. Based on the attribute-based totally get right of entry to manipulate mechanism, the proposed 2FA get entry to control system has been identified to not handiest enable the cloud server to restrict the get entry to the ones customers with the identical set of attributes but additionally maintain user privacy. Detailed security evaluation suggests that the proposed 2FA access manipulate system achieves the favored safety requirements. Through overall performance evaluation, we verified that the construction is "possible". We go away as destiny work to similarly enhance the performance even as retaining all nice capabilities of the system.
.

REFERENCES

[1] Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
[2] Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13thCCS*, 2006, pp. 89–98.
[4] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903.
[5] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," *IEEE Trans. Comput.*, vol. 53, no. 2, pp. 232–240, Feb. 2004.
[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.