INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 16th July 2017. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-5

Title: A Novel Security Approach For Double Trusted Access Control Over Cloud Services.

Volume 06, Issue 05, Page No: 1894 – 1898.

Paper Authors

***K.HIMA BINDU, M.ANUSHA.**

* Dept of CSE, Sri Venkateshwara Engineering College.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A NOVEL SECURITY APPROACH FOR DOUBLE TRUSTED ACCESS CONTROL OVER CLOUD SERVICES

***K.HIMA BINDU,** M.ANUSHA**

*PG Scholar, Dept of CSE, Sri Venkateshwara Engineering College, Suryapet, T.S, India.

**Assistant Professor, Dept of CSE, Sri Venkateshwara Engineering College, Suryapet, T.S, India.

ABSTRACT:

In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. However, the main barrier to its widespread adoption is the security and privacy issues. In order to create and maintain mutual trust among the customers and the cloud service providers, a well defined trust foundation should be implemented. The data stored in the cloud remotely by individual customer or an organization, so they lost control over the data, thus creating a security dilemma. The most challenging and hot research area in cloud computing now a day is the data security and access control. An effective measure to protect cloud computing resources and services in the start is to implement an access control mechanism. In this paper the features of various access control mechanisms are discussed and a novel framework of access control is proposed for cloud computing, which provides a multi step and multifactor authentication of a user. The model proposed is well-organized and provably secure solution of access control for externally hosted applications. In addition, the key generation mechanism is implemented. The secret key sends in encryption methods.

Keywords: Two factor Authentication, DES

INTRODUCTION:

Even though cloud computing endow with a lot of benefits that consist of economy of size, active stipulating, amplified litheness and near to the ground principal expenses, yet it also bring in a variety of new-fangled security threats. Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. It no longer depends on a server or a number of machines that physically exist, as it is a virtual system. There are many applications of cloud computing, such as data sharing data storage, big data management medical information system etc. End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market. Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web-based cloud services. As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password-based system. First, 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. Second, 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. A recently proposed access control model called attribute-based access control is a good candidate to tackle the first problem. It not only provides anonymous authentication but also further defines access control policies based on different attributes of the requester, environment, or the data object. In an attribute-based access 1 control system,

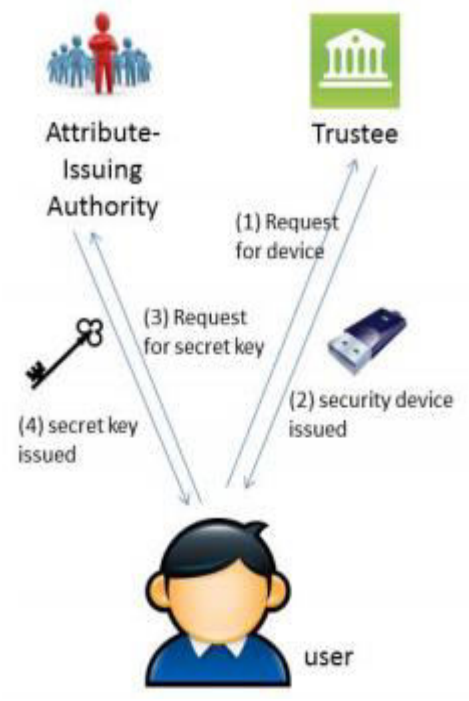
Related Work:

We review some related works including attribute-based cryptosystems and access control with security device in this Attribute-Based Cryptosystem Attribute-based encryption (ABE) is the cornerstone of attribute-based cryptosystem. ABE enables fine grained access control over encrypted data using access policies and associates attributes with private keys and cipher texts. Within this context, cipher text-policy ABE (CP-ABE) allows a scalable way of data encryption such that the encryptor defines the access policy that the decryptor (and his/her attributes set) needs to satisfy to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data with respect to the pre-defined policy. This can eliminate the trust on the storage server to prevent unauthorized data access. Besides dealing with authenticated access on encrypted data in cloud storage service, ABE can also be used for access control to cloud computing service, in a similar way as an encryption scheme can be used for authentication purpose: The cloud server may encrypt a random message using the access policy and ask the user to decrypt. If the user can successfully decrypt the cipher text (which means the user's attributes set satisfies the prescribed policy), then it is allowed to access the cloud computing service. In addition to ABE, another cryptographic primitive in attribute-based cryptosystem is attribute-based signature (ABS). An ABS scheme enables a user to sign a message with fine-grained control over identifying information. Specifically, in an ABS scheme, users obtain their attribute private keys from an attribute authority. Then they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that the signer's attributes satisfy the signing predicate if the signature is valid. At the same time, the identity of signer remains hidden. Thus it can achieve anonymous attribute-based access control efficiently. Recently, we proposed an attribute-based access control mechanism which can be regarded as the interactive form of ABS.

The Proposed Model:

In our proposed model, it is assumed that the components which make the system operational is composed of an owner of the data, a lot of entities which will used the data created by the owner of the data called the user of the data and the provider of the cloud services and data center. The authentication of the user is a multistep process, and after the successful authentication the user will only access the data file store by the owner, in a confidential manner by the implementation of the digital certificate. It is also assumed that it is not necessary for the user or owner to be online all the time. The owner comes online when it needs to register a new user or make some update to the certificate available on provider of cloud service, and the provider of cloud services is assumed to be online all the time to provide access to the data store at data center. Another assumption that we make is that the owner of the data will be able to perform / implement binary codes at cloud services for administration of data along with the storing of such data in encrypted type. The idea behind the choice of DES encryption involving user and the cloud service is, since DES encryption will need all associations to generate digital certificate for all users, and which is only one of its kind for every user. By implementing this mechanism of DES encryption we are able to accomplish a protected data communications for all latest session. The DES is considered to be more efficient, safe and sound mean of encryption, and also the digital certificate are make use of an encrypted session, therefore the rest of the users are unable to observe the data or information which is in transit over the network. The user is refraining from accessing other's data files, as the access provided by the owner has put some limitation on the user because of their capabilities. The proposed framework and its operational architecture are presented in this section.

Fig 1: Authentication model


Attribute-Issuing Authority
Trustee
(1) Request for device
(3) Request for secret key
(2) security device issued
(4) secret key issued
user

The data which will contain request of the user for the data and his identification credentials are sent to cloud services, and checked it with the available information in the validation information at data center and also the communication between owner and provider of cloud services ought to be secured during the transaction, to oppose any attack. The framework proposed, will clarify they way to attain the level of security required and controlled the mechanism of access.

Entities:

- Trustee: It is responsible for generating all system parameters and initializes the security device.
- Attribute-issuing Authority (Key generator/ data owner): It is responsible to generate user secret key for each user according to their attributes.
- Data User: It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.

Analysis of the Proposed Framework:

The proposed scheme is being analyzed for the characteristics of security in this section.

Authentication and Authorization: The user is authenticated and authorized by a multi – factor and multi step approach at the cloud service center. All the interactions of the owner of the data and cloud service is also authenticated, the mechanism followed is, the owner uses his private key for the encryption of the scrambled data file, and the Cloud Services uses his public key to authenticate the owner of data. The authentication user of the data is performed with owner private key when adding a new client, while the owner authentication is performed at cloud service by the private encryption at cloud service with owner private key.

Data Confidentiality and Integrity: In order to perform the analyses of the data confidentiality for this proposed approach, it is compared with the already existing encryption techniques that use the symmetric keys. The provider of cloud service is unable to visualize the original data and digest of the owner as the key is symmetric and only shared among the user and data owner. The data after encryption with symmetric keys is once again encrypted with the private key of the data owner, and public key of the provider of cloud services. To wrap up the discussion that data is not available to be decrypted in to its original form by the cloud services. The integrity is ensured for the data under consideration by employing the DES algorithm. The user of the data computes a fresh has and then match it up to the one already appended to the original data file. The integrity violation will be reported and the owner of the data will be informed accordingly, if the hash calculated by the user does not match to the original hash present in the message.

CONCLUSION:

In this paper, we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. The model proposed in this paper give power to the owner of the data to implement the security process on the data to be outsourced, and hence retain the control over the data. The model also proposed the combination of cryptography and access control to keep the data safe from vulnerabilities. A multistep, multi – factor authentication approach is employed for the authentication and authorization of the client, which increase the confidentiality and integrity of the data. The paper also presented the private key, hash and public encrypted ciphers among the owner, the client and the service provider which guarantee the isolation and safe execution of the cloud environment.

REFERENCES:

[1] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J.zhour Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4):50–57, 2013.

[2] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A Secure cloud computing based framework for big data information management of smart grid. IEEE T. Cloud Computing, 3(2):233–244, 2015.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.

[4] J Han, W. Susilo, Y. Mu, and J. Yan. Privacy-preserving decentralized key-policy attribute-based encryption. IEEE Trans. Parallel Distrib. Syst., 23(11):2150–2162, 2012.

[5] JHur. Attribute-based secure data sharing with hidden Policies in smart grid.IEEE Trans. Parallel Distrib. Syst., 24(11):2171–2180, 2013.

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, J. Zhou. k-times attribute-based anonymous access control for cloud computing. IEEE Trans. Computers, 64(9):2595–2608, 2015.

[7] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techno., 4(1):60–82, 2004.

[8] Y. Chen, Z. L. Jiang, S. Yiu, J. K. Liu, M. H. Au, and X. wang. Fully secure ciphertext-policy attribute based encryption with security mediator. In ICICS ‘14, volume 8958 of Lecture Notes in Computer Science, pages 274–289. Springer, 2014