Attribute based Encryption Access Control Scheme in Cloud

Mr. Patil Prashant Balgonda[1] Prof. Deshmukh A. O.[2]
[1]ME Student [2]Assistant Professor
[1,2]Flora Institute of Technology, Pune, Maharashtra, India

Abstract— Cloud computing refers to the practice of transitioning computer services such as computation or data storage to multiple redundant offsite locations available on the Internet, which allows application software to be operated using internet-enabled devices. Clouds can be classified as public, private, and hybrid. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Since the cloud computing environment is distributed and untrusted, data owners have to encrypt outsourced data to enforce confidentiality. To achieve practicable access control of encrypted data in an untrusted environment is an urgent issue that needs to be solved. Attribute-Based Encryption is a promising scheme suitable for access control in cloud storage systems. This system proposes a hierarchical attribute-based access control scheme with constant-size cipher text.

Key words: Access Control; Cipher Text-Policy Attribute Based Encryption; Constant Size Cipher Text

I. INTRODUCTION

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. The data owner generally specifies access control policy to enforce over the resources shared to authorized users with the permissible action. In collaborative data sharing in cloud computing, only authentication and general access control policy are not sufficient for an effective data access control. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

With rapid development of cloud computing, more and more enterprise s will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data.

Cloud computing, as an emerging computing paradigm, enables users to remotely store their data in a cloud, so as to enjoy services on-demand. Migrating data from the user side to the cloud offers great convenience to users, since they can access data in the cloud anytime and anywhere, using any device, without caring about the capital investment to deploy the hardware infrastructures. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and the flexibility to scale (or shrink) investments on-demand, by using cloud-based services to manage projects, enterprise-wide contacts and schedules, and the like.

However, allowing a cloud service provider (CSP) operated for making a profit, to take care of confidential corporate data, raises underlying security and privacy issues. For instance, an untrustworthy CSP may sell the confidential information about an enterprise to its closest business competitors for making a profit. Therefore, a natural way to keep sensitive data confidential against a un trusted CSP is to store only the encrypted data in the cloud.

Although the cloud computing paradigm brings many benefits, there are many unavoidable security problems caused by its inherent characteristics such as the dynamic complexity of the cloud computing environment, the openness of the cloud platform and the high concentration of resources. One of the important problems is how to ensure the security of user data. a user's private key is associated with a set of attributes and encrypted cipher text will specify an access policy over attributes. A user can decrypt the cipher texts if and only if his attributes satisfy the cipher text's policy.

Security problems, such as data security and privacy protection in cloud computing, have become serious obstacles which, if not appropriately addressed, will prevent the development and wide application of cloud computing in the future. In 2009, a few serious security incidents with cloud service occurred at many IT companies, including Google, Microsoft, and Amazon. These incidents affected the information services to millions of consumers. Therefore, it is important that security problems in cloud computing receives significant attention.

In cloud computing, users store their data files in cloud servers. Thus, it is crucial to prevent unauthorized access to these resources and realize secure resource sharing. In traditional access control methods, we generally assume data owners and the storage server are in the same secure domain and the server is fully trusted. However, in the cloud computing environment, cloud service providers may be attacked by malicious attackers.

These attacks may leak the private information of users for commercial interests as the data owners commonly store decrypted data in cloud servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in a UN trusted environment are problems that must be solved by cloud computing technologies and applications. However the disadvantages of these schemes relate to the size of cipher text, and the computation of encryption and decryption depends linearly on the number of attributes. In cloud computing, it will limit the application of attribute-based encryption in practice if the number of attributes is too large and the length of cipher text is too long. In addition, the huge user numbers in a cloud computing environment means it is impractical to complete the

authorization and distribute secret keys using only one attribute authority.

Moreover, since the number of users is large in a cloud computing environment, how to realize scalable, flexible and fine-grained access control is strongly desired in the service-oriented cloud computing model .This paper proposes a hierarchical cipher text-policy attribute-based encryption access control scheme with constant-size cipher text that can realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing.

The proposed scheme adopts cipher text-policy - attribute-based encryption with constant cipher text size and maintains the size of cipher text and the computation of bilinear pairing at a constant value, which improves the efficiency of the system and reduces the extra overhead of space storage, data transmission and computation. Second, we design a hierarchical access control system.

This system supports inheritance of authorization that reduces the burden and risk in the case of single authority. Finally, we prove our scheme has indistinguishable security under an adaptive chosen cipher text attack and we analyze the performance of our scheme. The system presents a simulation model to apply our scheme in a cloud environment.

II. EXISTING SYSTEM

In existing system, various access control models have been proposed since the 1970s, e.g. DAC, MAC, Bell-La Padula, Biba etc. In1996, Sandhu et al. proposed the Role-Based Access Control Model (RBAC). Various improved RBAC models have been proposed and been widely used in practice. With the development of information technology, traditional access control is not very suitable for access control in cloud computing for the following reasons. First, the flexibility of the access policy is inadequate and it is more difficult to extend it to a hierarchical and large-scale application in a cloud computing environment. Second, these access control scheme needs to strengthen their adaptability to a cloud computing environment. Third, their adaptability to dynamically change roles is simply not enough.

The role of users changes dynamically in many applications. For example, when a doctor works in an outpatient department during the day he can access the data of an outpatient in the health-care information system. But when he works in the inpatient department at night, he can access the data of an inpatient in the system. How to achieve a dynamic change of role is a problem that should be solved regarding traditional access control. Finally, high security requirements need a new access control model. In traditional access control schemes, we generally assume the storage server is fully trusted.

However, in a cloud computing environment the data owners and storage server are not in the same secure domain and the cloud service provider may be un trusted. A general solution for this problem is to store the encrypted data file in a server and decryption keys to authorized users. Thus, unauthorized users (includes cloud service provider) cannot decrypt the encrypted files and we can control the decryption ability of users to achieve access control. This method provides an idea for realizing the confidentiality of data stored on untrusted server.

The first fully functional IBE scheme was presented by Bone hand Franklin. They constructed an IBE scheme by exploiting the Weil pairing and they proved its selective security in the random oracle model. Similarly to IBE, a number of identity-based cryptographic primitives have been proposed. Several advanced cryptographic primitives allow defining more controllable decryption. Hierarchical identity-based encryption (HIBE), first proposed system is an identity based cryptographic primitive that extends IBE with key delegation to relieve the private key generator in IBE from heavy key management burden when there is a large number of users in the system.

III. DISADVANTAGES

- The flexibility of the access policy is inadequate and it is more difficult to extend it to a hierarchical and large-scale application in a cloud computing environment.
- These access control schemes needs to strengthen their adaptability to a cloud computing environment.
- Their adaptability to dynamically change roles is simply not enough.
- The role of users changes dynamically in many applications.
- High security requirements need a new access control model.

IV. PROPOSED SYSTEM

In proposed system the system proposes a hierarchical attribute-based access control scheme with constant-size cipher text. The scheme is efficient because the length of cipher text and the number of bilinear pairing evaluations to a constant are fixed. The proposed scheme adopts cipher text-policy -attribute-based encryption with constant cipher text size and maintains the size of cipher text and the computation of bilinear pairing at a constant value, which improves the efficiency of the system and reduces the extra overhead of space storage, data transmission and computation.

Then the system designs a hierarchical access control system. This system supports inheritance of authorization that reduces the burden and risk in the case of single authority. Finally, the system proves our scheme has indistinguishable security under an adaptive chosen cipher text attack and we analyze the performance of our scheme. The system presents a simulation model to apply our scheme in a cloud environment.

The system model utilizes a hierarchical structure which is formed with root authority, top-level domain authorities and low-level domain authorities to realize attribute management and authority. The structure can disperse the burden and risk of the authority of the single central attribute authority in a cloud computing environment. Moreover, the systems propose a hierarchical Cipher Text-Policy -Attribute-Based Encryption access control scheme with constant-size cipher text and discuss the algorithms in detail for our scheme.

The cloud service provider manages the cloud servers and provides a data storage service. Data owners encrypt their shared data files and store them in the cloud. CT

is the cipher text of DEK by an ATTRIBUTE-BASED ENCRYPTION algorithm. Since the access structure is implied in cipher text, only the user with corresponding attribute scan decrypt the cipher text. Unauthorized users cannot access the data file. Therefore, we realize access control based on attribute-based encryption with constant size cipher text. To access the shared data files, users download a previously encrypted data file from the cloud and then decrypt the first part of the file CT based on the set of attributes to get the symmetric key. The access polices are expressed in terms of the set of attributes. The user obtains the data file by using the symmetric key to decrypt the cipher text of the data file.

This scheme can fix the size of cipher text and the computation of encryption and decryption at a constant value in addition to improving the efficiency of the system. The data owner first encrypts the data file using asymmetric key DEK and then encrypts DEK by using the proposed scheme with a specific access control policy. The data owner uploads the final cipher text and stores it in the cloud servers. Whether a user can access and decrypt the data file depends on how to obtain the symmetric key, which is decided by the user's set of access attributes.

V. ADVANTAGES

- It improves the efficiency of the system.
- It reduces the extra overhead of space storage, data transmission and computation.
- It maintains the size of cipher text and the computation of bilinear pairing at a constant value.

VI. SYSTEM ARCHITECTURE

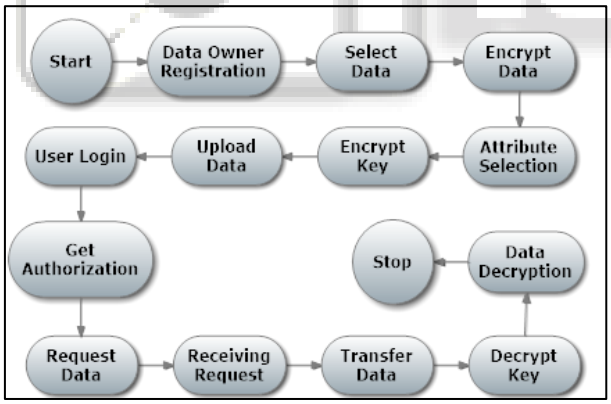

Fig. 1:

VII. FLOW DIAGRAM

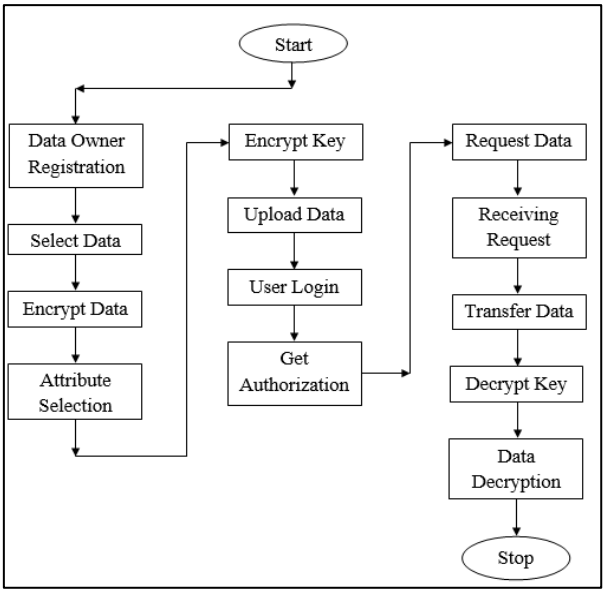

Fig. 2:

VIII. MODULES

a) Data Owner Registration
b) Attribute Management
c) User Authorization
d) Users Access

A. Data Owner Registration

Data owner have to register. After registration select the file which wants to send then encrypt the file by using the key. The cloud service provider manages the cloud servers and provides a data storage service. Data owners encrypt their shared data files and store them in the cloud. The access structure is implied in cipher text, only the user with corresponding attributes can decrypt the cipher text.

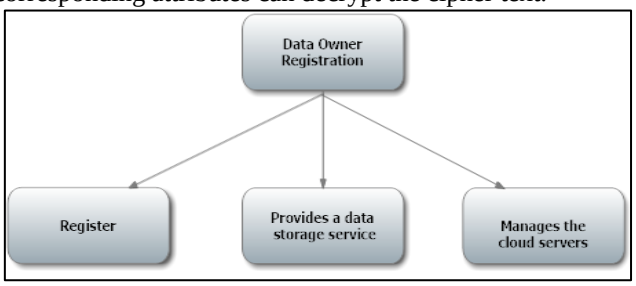

Fig. 3:

B. Attribute Management

Data owner selects the attribute from the domain authority & encrypts the key in data owner. Then the encrypted data and the encrypted key are transferred to the cloud service provider. The system model utilizes a hierarchical structure which is formed with root authority, top-level domain authorities and low-level domain authorities to realize attribute management and authority. The structure can disperse the burden and risk of the authority of the single central attribute authority in a cloud computing environment.

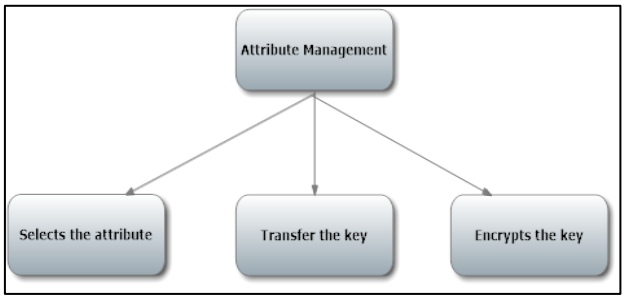

Fig. 4:

C. Users Authorization

Users send the request to the domain authority & select the attributes from the domain authority. Authorization details are transferred to the cloud service providers. This scheme can fix the size of cipher text and the computation of encryption and decryption at a constant value in addition to improving the efficiency of the system. The data owner first encrypts the data file using asymmetric key DEK and then encrypts DEK by using the proposed scheme with a specific access control policy.

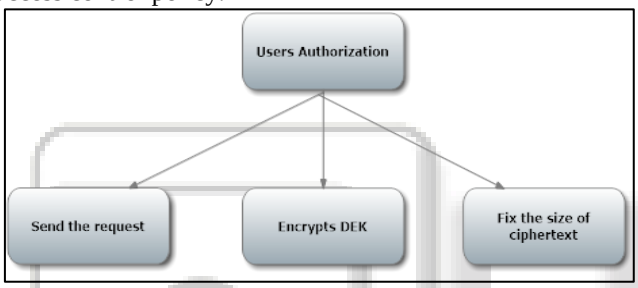

Fig. 5:

D. Users Access

User gets the encrypted data and encrypted key from the cloud service provider and decrypts the encrypted key by using the attribute key. The decrypted key is used for the data decryption. The data owner uploads the final cipher text and stores it in the cloud servers. Whether a user can access and decrypt the data file depends on how to obtain the symmetric key, which is decided by the user's set of access attributes .Unauthorized users cannot access the data file. Therefore, we realize access control based on attribute-based encryption with constant size cipher text. To access the shared data files, users download a previously encrypted data file from the cloud and then decrypt the first part of the file CT based on the set of attributes to get the symmetric key. The access polices are expressed in terms of the set of attributes. The user obtains the data file by using the symmetric key to decrypt the cipher text of the data file.

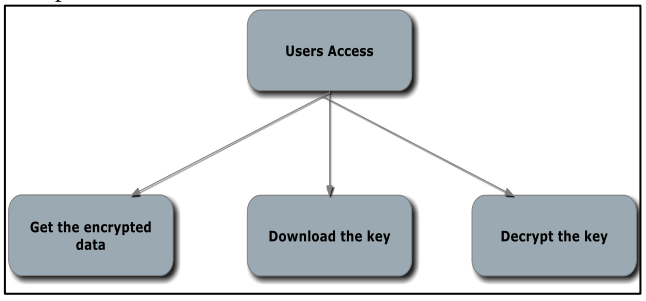

Fig. 6:

IX. ALGORITHM DESCRIPTION

A. Cipher Text- Policy -Attribute- Based Encryption Algorithm

The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters [5]. It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Attribute-based encryption is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string. attribute-based encryption goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy attribute-based encryption - kp-attribute-based encryption) or policies defined over a set of attributes (cipher Text-policy attribute-based encryption). Attribute-based encryption can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipient's attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.

X. CONCLUSION

In this project, the system proposed Attribute-based access control with constant-size cipher text to achieve practicable access control of encrypted data in an untrusted environment. Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

REFERENCES

[1] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Encryption Policies for Regulating Access to Outsourced Data", in ACM Transactions on Database Systems (TODS), April, 2010.
[2] Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," IEEE INFOCOM 2010, San Diego, CA, March, 2010.
[3] Zhiguo Wan, Jun-e Liu, Robert H. Deng: HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. IEEE Transactions on Information Forensics and Security 7(2): 743-754, 2012.

[4] Kan Yang, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security 8(11): 1790-1801, 2013.
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.

