International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Anonymous Attribute based Access Control in Cloud Computing

N. Meddah
PhD Student
Department of Computer Science and Engineering
Laboratory of Systems and Information Technology Engineering
ENSA, University Ibno Zohr, Agadir, Morocco.

A. Toumanari
PhD Professor
Department of Computer Science and Engineering
Laboratory of Systems and Information Technology Engineering
ENSA, University Ibno Zohr, Agadir, Morocco.

L. Fetjah
Assistant Professor
University of sciences ain chock HASSAN II, FSAC,
LIAD, Casablanca, Morocco

***Abstract*- Cloud computing is an emerging paradigm that provide technology and computer resources as a service. Cloud computing is revolution computing that effects, peoples, processes and information technology, and brought a wide range of advantages, specially, easiest and fasted storage, and access from any where at any time to data. However, moving the infrastructure and sensitive data from trusted domain of the data owner to public cloud will pose severe security and privacy risks. So the security remains the critical issue in cloud computing, mostly access control and data privacy. In this paper we propose a fine-grained access control system using a combination of key-Policy attribute-based encryption KP-ABE system and an anonymous proxy re-encryption** with CCA security and collusion resistance**This proposed scheme is an efficient model that enforcing access policies based on data attributes, allowing the delegation of computation implicated in fine-grained access control to untrusted cloud servers without disclosing the data content and resolving the vulnerability of Chosen Cipher-text Attacks CCAs. Our model is applied to health information ([PHR: Personal Health Record] Doctors can encrypt and submit their prescription and diagnostic notes to servers using KP-ABE Patients may also encrypt their information and the PHR.**

Index terms--Cloud computing, access control, data privacy, ABAC, ABE, KP-ABE, CP-ABE, PRE, CCAs, PHR.

I. INTRODUCTION

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. According to the NIST (National Institute of Science and technology):Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Cloud computing incorporate, virtualization, utility computing, on-demand deployment and internet delivery services, There are tree categories of cloud: public cloud, private cloud and hybrid cloud. Cloud Computing models are:

SaaS: Software as a service, to use the provider's applications, running on a cloud infrastructure and accessible, from various client devices through a thin client interface such as a Web browser.

PaaS: Platform as a service, to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (java, python, .Net)

IaaS : Infrastructure as a service, To provision processing, storage, networks, and other fundamental computing resources where theconsumer is able to deploy and run arbitrary software, which can include operating systems and applications.

The new concept, introduced by the Cloud Computing such as resources sharing, computation outsourcing and external data warehousing, increase the cloud computing attacks. The main attacks are [2]:

1. DOS, DDOS (Distributed denial of service)
2. Side channels attacks
3. Authentication attacks
4. Man-in-middle cryptography attacks
5. Inside jobs attacks

Furthermore the main issues in cloud computing access control are [3]:

1. Account and service hijacking
2. Malicious insiders
3. Authentication mechanism
4. Privileged user access
5. Browser security

Due to this attacks and issues access control, a security policy must be strong.

II. ACCESS CONTROL

Access control is generally a policy that allows denies or restricts access to systems. It is a mechanism that is very much important for protection in computer security. Classical Access control models full in to three types [4]:

1. MAC: mandatory Access control
2. DAC: Discretionary Access Control
3. RBAC: Role Based Access Control

These access control models known as Identity based access control wish based on the fact that the server is in the trusted domain, So in the cloud these approaches are very limited and not applicable, as there is a necessity ofdecentralization, scalability and flexibility for access control data located in the cloud. Due to this problem, various studies prove that the encryption of data is the most efficient method for access control [4]. Yet the standard encryption is inefficient when selectively sharing data with many users. Since data needs to be re-encrypted using every public key [4]. To overcome this new problem, about the limited of traditional encryption, sahai and al [4], introduce a new public key primitive called ABE (Attribute Based Encryption), which has significant advantages over traditional PKC (Public key Cryptography) primitives. Thus it's envisioned as an important tools for addressing the problem of secure fine-grained access control.

B. ATTRIBUTE BASED ACCESS CONTROL ABAC

With the development of large distributed systems attribute based access control (ABAC) has become increasingly important. According to the NIST "ABAC is An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions "[14].Attribute Based Encryption (ABE) is category of ABAC. ABE proposed to support fine-grained access control

ABE can be viewed as an extension of Identity Based Encryption system IBE [5]. IBE has resolving the problem public key sharing in which an arbitrary string can be used as a public key (email, IP Address, phone number phone…).

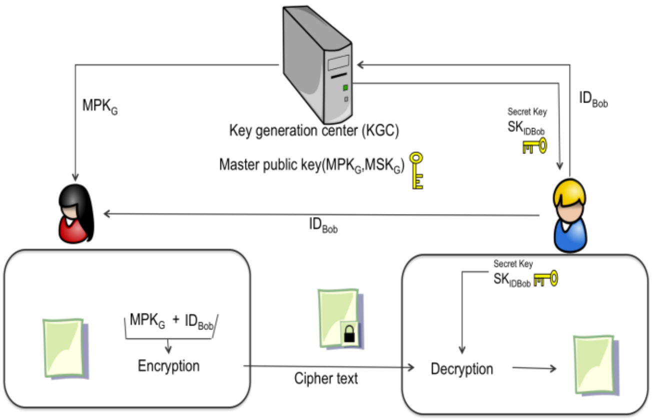

Fig.1: Identity Based Encryption system

Compared with IBE in which, encrypted data is targeted for decrypting by single known user, inABE system, the user's identity is generalized to a set of descriptive attributes instead of a single string specifying the identity of the user. Compared with the identity-based encryption, ABE has an important advantage because it makes a more flexible encryption instead of one-on-one; it is seen as a promising tool to solve the secure data-sharing problem grained and decentralized access control. ABE is used in various applications, like Electronic Health records management (HER), and PHR (Personal Health Records)[13]. In the ABE system the decryption key should bematched with the attributes of cipher text and the key will decrypt the cipher text. The private keys are constructed by the Access tree as in ABE system root node [6].

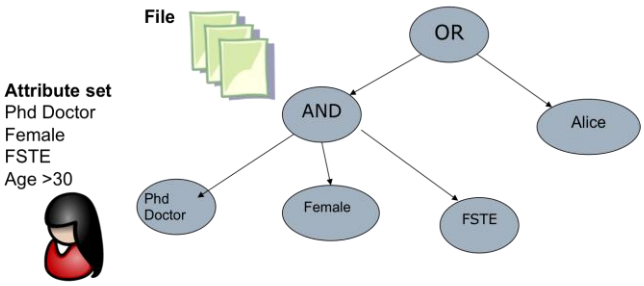

Fig.2: ABE scheme

In the cloud computing system the single authority will not able to control the multiple attributes for each user and all access rights, to address this problem for single authority ABE, the multi ABE system is introduced [9].

Due to this requirement the ABE system has been divided into two classes of multi authority ABE system: KP-ABE and CP-ABE.

VI. TECHNIQUE PRELIMINARIES

A. Key Policy Attribute Based Encryption "KP-ABE"

Key Policy Attribute Based Encryption, KP-ABE system introduced in 2006 by Goal and al[4], is defined as the private key in the form of access tree structure, in which cipher-texts are labelled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy, that specifies which type of cipher-texts the key can decrypt. KP-ABE has proved efficiently solution for fine-grained access control; the system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Ostrovsky et al. [6] proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including no monotone ones, by integrating revocation KP-ABE scheme [4]. A KP-ABE scheme is composed of four algorithms which can be defined as follows [Z]:

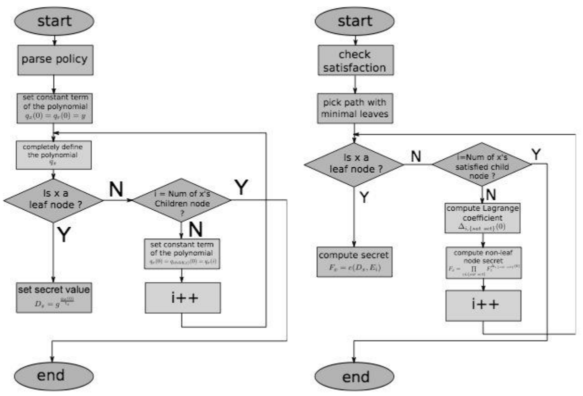

Fig 3. Essential algorithms for KP-ABE

However KP-ABE scheme cannot predict who are all having access rights, also The KP-ABE system is based on the predefined set of attributes and cannot handle the dynamic changes in the access structure, and these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management. Therefore the only solution introduced by Shucheng Y and al [7]to make a complete fine-grained access control by KP-ABE is combining techniques of attribute-based encryption (ABE), proxy re-encryption. This combined system of KP-ABE and PRE will offer the full security of access control but it degrades the performance and generates the high cost and it's vulnerable to CCAs (Chosen Cipher Text Attacks) by using a basic PRE [7].

B. Access Tree (Access Structure)

KP-ABE is a cryptography system built upon bilinear map and LSSS (Linear Secret-Sharing Scheme) introduced by Adi Shamir [17],A famous example of LSSS is the Shamir t-out-of-n threshold scheme. In that scheme, the hardness of secret reconstruction depends on the hardness of polynomial reconstruction.In the access-tree construction, cipher-texts are labelled with a set of descriptive attributes. Private keys are identified by a tree-access structure in which each interior node of the tree is a threshold gate and the leaves are associated with attributes. (We note that this setting is very expressive. For example, we can represent a tree with "AND" and "OR" gates by using respectively 2 of 2 and 1 of 2 threshold gates.) A user will be able to decrypt a cipher-text with a given key if and only if there is an assignment of attributes from the cipher-texts to nodes of the tree such that the tree is satisfied. An illustrate example of Access tree is defined as follow:

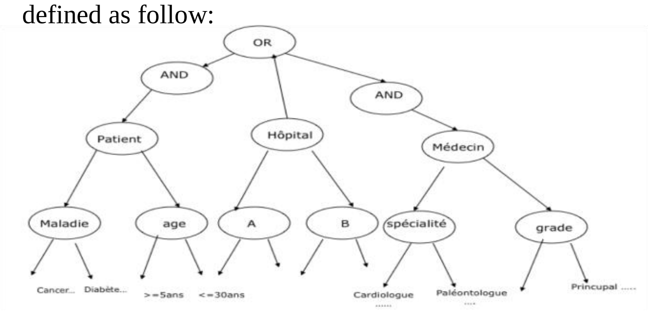

Fig 4. PHR (Personal Health record) Access Tree

C. Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher-text encrypted under Alice's public key into another cipher-text that can be opened by Bob's private key without seeing the underlying plaintext. More formally, a PRE scheme allows the proxy, given the proxy re-encryption key $rk_a \leftrightarrow b$, to translate cipher-texts under public key pka into cipher-texts under public key and vise versa. for more details on proxy re-encryption schemesPlease refer to [16].

In our scheme we use new PRE system with CCA security, collusion resistance, and anonymity in the random oracle model [15].

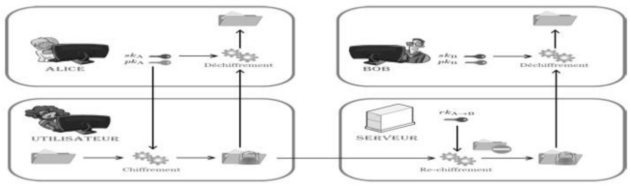

Fig 5. Re-encryption Proxy

In order to attain secure and efficient fine-grained access control, we adopt an advanced approach which combining a powerful cryptographic techniques: KP-ABE, and anonymous proxy re-encryption A-APRE with CCA security, collusion resistance, and anonymity which is obtaining by Schnorr signature method [15], that guarantees the integrity of the original cipher-text. we exploited KP-ABE to ensure secure and fine-grained access control, in the odder hand the challenging issues of heavy computation overhead and cumbersome online burden towards the data owner is resolved by re-encryption proxy (PRE)[16], that enable data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents and allow the data owner to control access of his data files with a minimal overhead in terms of computation effort and online time, and thus fits well into the cloud environment. Data confidentiality is also achieved since Cloud Servers are not able to learn the plaintext of any data file. data integrity is also achieved by using a anonymous PRE that use Schnorr signature [15] which is existentially unforgeable. The anonymity property of PRE has resolved the vulnerability of CCAs (Chosen Cipher text Attacks). An illustrate example of our proposed scheme as follows:

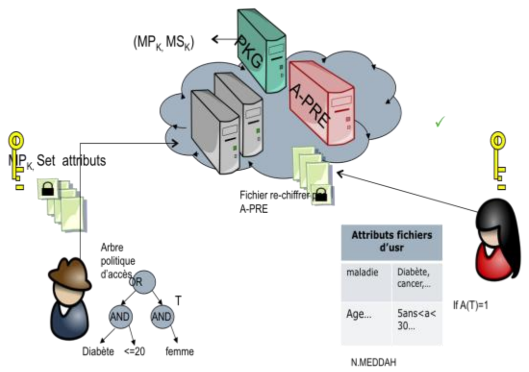

Fig 6. KP-ABE with A-PRE

IX. CONCLUSION AND FUTURE WORKS

Cloud computing can be even a revolution in the computing world, by given all the types of computing resources as service (Software, platform, infrastructure), but security remains a major obstacle for the migration to the cloud computing. Migrating into the "Cloud" is not that easy but if carefully planned and deployed it will bring advantages in many areas like decreasing cost and resources. In this papers we have presented a efficient system that provide secure and fine-grained data access control in cloud Computing system based on KP-ABE and a new PRE system with CCA security, collusion resistance, and anonymity in the random oracle model . One challenge in this context is to achieve fine-grained access control, data confidentiality, data integrity, scalability and system resistant to CCAs (Chosen Cipher text Attacks), which is not provided by current work. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. In future work, we would applied our proposed scheme to ensure fine-grained access control of Personal Health Records (PHR) allowing the doctors and patients to encrypt their PHRs and store them on semi-trusted cloud servers such that servers do not have access to sensitive PHR contexts.

REFERENCES

(1) P. Mell and T. Grance, "The NIST denition of cloud computing," Special Publication 800-145, 2011.
(2) Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", Journel of Security Engineering, vol.2, 2012.
(3) Issa M. Khalil, Abdallah Khreishah, Muhammad Azeem. "Cloud Computing Security: A Survey",open access computers journal", 3 February 2014.
(4) V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data, "in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS "06). ACM, 2006, pp. 89–98.
(5) A. Shamir . Identity-Based Cryptosystems and Signature Schems. Crypto84, vol. 196 , LNCS, pp. 47-53, 1984.
(6) R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007.
(7) Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. Dept. of ECE, Worcester Polytech. Inst., Worcester, MA, USA,14-19 mars 2010.IEEE.
(8) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy (SP '07), pp. 321–334, May 2007.
(9) M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130
(10) Vaduganathan D,Ramasami S,Santhiya C, Vanishree K A," Survey on Fine-Grained Access Control with Efficient Data Sharing of Cloud Storage in Cloud Computing ",International Journal of Engineering Research & Technology (IJERT),02, February-2015
(11) Guojun Wang, Qin Liu, Jie Wu," Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", National Natural Science Foundation of China under Grant Nos. 90718034 & 60773013.
(12) Z.Wan, J.Liu, R.H.Deng, "HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Forensics and Security, vol 7, no 2, APR 2012.
(13) Yao Zheng,"Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption",Thesis, WORCESTER POLYTECHNIC INSTITUTEJune 2011.
(14) (a survey of access control models" NIST, Working Draft, 2012.
(15) Jun Shao1, Peng Liu, Guiyi Wei and Yun LingAnonymous proxy re-encryption, SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2011) ,Wiley Online Library DOI: 10.1002/sec.326
(16) Pei-Shan Chung1, Chi-Wei Liu2, and Min-Shiang Hwang, A Study of Attribute-based Proxy Re-encryption Scheme in Cloud Environments,International Journal of Network Security, Vol.16, No.1, PP.1-13, Jan. 2014
(17) R. Rivest, Adi Shamir, (How to Share a Secret), Massachusetts Institute of Technology,Communications of the ACM,November 1979 Volume 22 Number 11.

II. ACCESS CONTROL

Access control is generally a policy that allows denies or restricts access to systems. It is a mechanism that is very much important for protection in computer security. Classical Access control models full in to three types [4]:

4. MAC: mandatory Access control
5. DAC: Discretionary Access Control
6. RBAC: Role Based Access Control

These access control models known as Identity based access control wish based on the fact that the server is in the trusted domain, So in the cloud these approaches are very limited and not applicable, as there is a necessity of