ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Efficient Auditing Mechanism for Data Storage in Cloud Using Abs

P.Suresh[1], R.Malathi[2]

Research Scholar, Department of Computer Science, H.H The Rajah's College (Autonomous) [1]

Assistant Professor, Department of Computer Science, H.H The Raja's College (Autonomous) [2]

Abstract: Cloud comp ting's multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenets. In order to achieve safe storage, policy based file access control, poly based file assured delectation and policy based renewal of a file stored in a cloud environment. a suitable encryption technique with key management should be applied before outsourcing the data. Exciting system attribute based encryption is new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. key policy attribute based encryption (KP-ABE) is an important type of ABE, which enable senders to encrypt message under a set of attribute and private keys are associated with access structure that specify which cipher texts the key holder will be allowed to decrypt. in this paper (ABS) attribute based signature new algorithm can be easily implemented and greatly raise the computational efficiency of original ABS algorithm. a verifier will be convinced of the fact that whether the signer's attribute satisfy the predicate while remaining completely ignorant of the identity of signer.ABS is much useful in a wide range of application including private access control for ad hoc networks, attribute based messaging, etc.

Keywords: Attribute based signature, Cloud storage, Cloud service provider, Data owner, Encryption.

I. INTRODUCTION

Now a day's cloud computing is a rationally developed technology to store data from more than one client. Cloud computing is an environment that enables users to remotely store their data. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. it helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backup remotely to third party cloud storage providers rather than maintain data center on their own. an individual; or an organization may not require purchasing the needed storage device. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware/software failures. Much of the data stored in clouds is highly sensitive, for example/medical records and social networks. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. in one hand, the user should authenticate it lf before initiating any transaction, and on the hand ,it must be ensured that the cloud does not tamper with the data that is outsourced .user privacy is also required so that the cloud or other users do not know the identity of the user. he cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the service it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, the is also a need for law enforcement. Access control in clouds gaining attention because it is important that only authorized users have access to valid service. a huge amount of information is being stored in the cloud, and much of this sensitive.

Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in google docs or drop box) or even personal information (as in social networking).it is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. Thus user might want to post a comment on an article. But does not want his/her identity to disclose. However, the user should be able to prove to the other user that he/she is a valid user who stored the information without revealing the identity. There are cryptographic protocols like ring signatures [13].mesh signatures [14].group signature [15]. This can be used in these situations. Ring signature is not feasible option for clouds where there are a large number of users. group signature assume the preexistence of a group which might not be possible in clouds. After comparing the drawbacks of all the cryptographic protocols mentioned above. a new protocols known as attribute based signature (ABS) has been proposed in this paper.ABS was proposed helps to identify the users as an authorized one, without revealing its identity. Other users or the cloud can verify the user and the validity of the message stored.ABS can be combined with ABE to authenticated access control without disclose the identity of the user to the cloud.

II. LITERATURE SURVAY

Attribute based signature were first introduced by magji, prabhakaran, and Rosales (2008) as a way to let a signature attest not to be the identity of the individual who

DOI 10.17148/IJARCCE.2015.4877

endorsed a message, but instead to a(possibly complex) claim regarding the attribute she process. They constructed an ABS scheme that supports a power full set of predicate, namely, any predicate consists of AND.OR, and threshold gates. Hover the security of their scheme is week as their construction is only proved in the generic group model. Since then, there have been lots of works on this subject (Escala; herants; morillo, 2011; khader, 2007a; 2007b; au; susilo ;xie; ren, 2010; li; kim. 2007; 2010; maji; prabharan; rosulek. 2011; okamoto; takashima, 2011; shahandashti; safavinaili.2009).recentl,.magi,prabhakaran, and rosulek (2011) presented an ABS scheme which is proven secure in the standard model. but it is much less efficient and more complicated than the scheme in (maji;prabhakaran;rouslek,2008),since it employs the groth-sahai NIZK protocol (2008) as building blocks .okamoto and Takashima (okamoto;takashima.2011) presented a fully secure attribute based signature (ABS)scheme in the standard model. The admissible predicates of the scheme support non-monotone predicates. Escala. Herranz and morillo (2011) proposed a fully secure attribute-based signature (ABS) scheme in the standard model. This scheme supports an an additional property of revocability, so that an external judge can break the anonymity of a signature when necessary. Another related notion to ABS is fuzzy identity based signature which was proposed and formalized in (shanqing;yingpei;2008;tang;cao;dong,2011).it allows a user with identity ω to issue a signature whitch could be verified with identity 'ω' if and only if ω and ω' are within distance judged by some metric. However, this kind of signatures does consider the anonymity for signer.

Our contribution

Maji,prabharan,resulek(Maji;prabhakaran;rosulek,2008;2011)and okamoto,Takashima (2011) pointed that the future work of ABS ,on the theoretical fornt,is to base the security of ABS on a standard hardness assumption, while still reserve the efficiency for the most part .in this paper, we attempt to propose such an ABS scheme which is secure in the standard model based on decisional parallel blinear Diffie-Hellman exponent assumption (Water 2011) which is more practical than generic group model of (Maji;prabharan;rosulek,2008).

The proposed ABS scheme is efficient and practical, we compare our scheme with the existing ABS scheme in the standard model .Maji, prabharan, and rosulek's (2011)(two typical instantiation),okamoto and takashima's (2011),and Escala. herranz, and morillo's 2011),as well as the ABS scheme in the generic group model (Maji;prabhakaran;rosulk,2008)(as a benchmark).all of these scheme can be implemented over a pairing group and the size of group element is about the size of zp(e.g 256 bits).our construction is inspired by the attribute based encryption scheme (ABE)of water (water 2011).roughly speaking, a secret signing key sks with attribute set S corresponds to secret decryption key sks in ABS(water 2011).no counterpart of signature σ in our construction exisits in the ABE(water 2011).

III. PROPOSED WORK

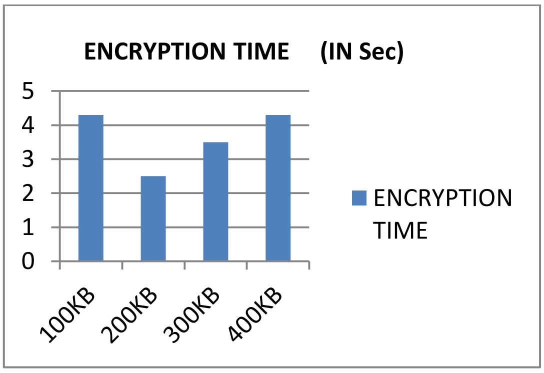
Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, they can collaboration, and the like. However, allowing cloud services providers (CSOs), which are not in the same trusted domains as enterprise user's to make of confidential data, may raise potential security and privacy issues. To make the sensitive user data confidential against untrusted CSPs,a natural way is to apply cryptographic approach. By disclosing decryption keys only to authorized users. However .when enterprise users outsource confidential data for sharing on cloud servers. the adopted encryption system should not only support fine grained access control ,but also provide high performance, full delegation ,and scalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises. And achieving a dynamic set of user.

IV. EXPERIMENTAL RESULT

The hardware used to carry out this experimental is interring core i3 processor with 2GB Ram. The program is writer in C# programming it is used for compilation and execution purpose.

Encryption

In the first graph show the comparison of time required for encryption using ABS algorithm.

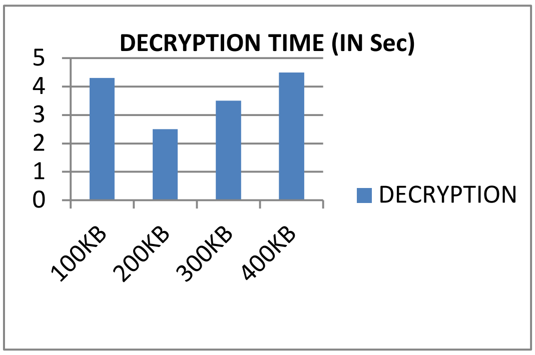


This graph gather FIVE different file with different sizes to measure the performance metrics using encryption time .The time will vary with different file size and type of the file.

Decryption

In the second graph shows the comparison of time ABS algorithm.
This graph gathers FIVE different encrypted files received from sender and decrypted using ABS public key. in this process to measure the performance metrics using decryption time. The time very with different encrypted file formats.

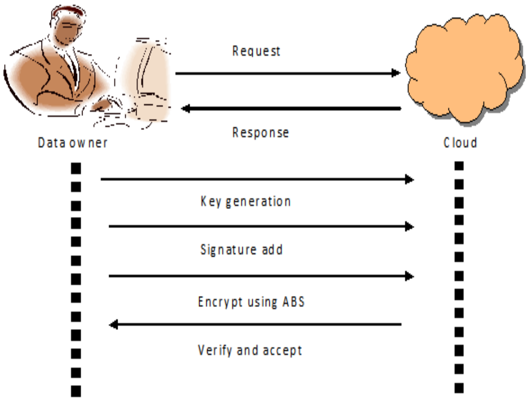
DOI 10.17148/IJARCCE.2015.4877



Summary

So the detailed analysis between the encryption and decryption time with different file formats. after analyzing the results, that shows the ABS algorithm time dependant on file format, also this work conclude ABS is efficiency handle encryption and decryption with performance matrices. In ABS the decryption time is much less from the taken in encryption method.

METHODOLOGY USED



Cloud Computing

Cloud computing is becoming a well-known buzzword nowadays. as a brand new infrastructure to offer services, cloud computing system have many superiorities in comparing to those exited traditional service provisions, such as reduced upfront investment, expected performance, high availability, infinite scalability, tremendous fault-tolerance capability and so on and consequently chased by most of the it companies, such as google, Amazon, Microsoft, salesforce.com. Based on their overwhelming predominance in traditional service provisions and capital accumulation, most of these it companies have more chance to adapt their service into such a new environment earlier, say cloud computing system. on the other hand ,a large number of new companies are spawned with competitive services relayed on those provided cloud computing system. in terms of their provisions ,we divide those service into servel categories are software as service(SaaS),platform as a service (PaaS),identity and policy management as a service(ipmaas),network as a service (Naas).infrastructure as a service(IaaS).detailed analysis to these services are provide the corresponding service categories.

Cloud auditing

A party that can conduct independent assessment of cloud services, information system operation. Performance and security of the cloud implementation. a cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. for security auditing a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly. Operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. public auditing is the service which is used to ensure integrity of the data stored on the cloud user's computation resources. To perform the auditing task the TPA known as third party audit the stored data on cloud.TPA verify the correctness of the cloud data on demond without retrieving a copy of the whole data. The TPA, has expertise and capabilities that can periodically check the integrity of all the data stored which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud.

ABS: attribute based signature

attribute based signature (ABS) is a new and versatile cryptographic primitive proposed in [1,2].in which a signature attests not to the identity of the individual who endorsed a messgae, but instead to a (possibly complex) claim regaring the attribute authority.ABS offer an unforgeability guarantee for the verifier, that the signature was producted by a single party whose attribute satisfy the policy being made;ie not by collusion of individuals who pooled their attributes together. Although the scheme in [2] reveals the set of attributes satisfying the policy, subsequent research of ABS offer an attribute signer privacy guarantee for the signer. That is ,a legitmate signer remains anonymous without the fear of revocation and is indistinguishable among all the users whose attribute satisfying the policy specified in the signature.ABS is useful in many important applications such as anonymous authentication and attribute based messaging system. In ABS in which a signer is defined by a set of attribute instead of a single string reprinting the signer's identity. In ABS, a user obtains a set of attributes from one pr multiple attribute authorities. An attribute based signature assures the verifier that a signer, whole set of attribute satisfies a (possibly) complex predicate, has endorsed the message. The following example illustrates the concept. Suppose we have the following predicate: professor **OR** (((Biology Department **OR** Female) OR above 50 years old) AND university A) Alice’s attributes are (University A, female).Bob's attribute are (above 50 years old, professor).although their attribute are quite are quite different. it is clear that alice and Bob can generate a signature on this predicate, and such a signature releases no information regarding the attribute or identity of the signer,i.e.Alice or Bob, except that the attribute of the signer satisfile the predicate.

ALGORITHM STEPS

DOI 10.17148/IJARCCE.2015.4877

System initialization

Select a prime q and groups g1, g2.define the mapping e g1*g1→g2.let H→ hash function. Let Ao=ho å and (Tsig,tver)mean Tsig is the private key with which a message is signed and TVer is the public key used for verification.

1. Secret for the trustee is TSK=($a_{0,}$ TSig)

2. Puplic key is TPK=(G_1, G_2, H $, g_{1,} A_{0,} h_{0,} h_{1,} \ldots\ldots h_{tmax, g2,}$ TVer)

User registration

for a user with identity Uu the KDC draw at random $K_{base} \epsilon G.$ LETKO $= K_{BASE}^{1/ao}$.Token is generated as:$\gamma = (u, k_{base, Ko, \rho})$

kdc setup

Choose a,b ϵZ_q^* randomly and compute A_{ij}, h_j^a and $B_{ij} = h_j^b$

1. Private key of KDC is ASK[i] =(a,b)

2. Public key of KDC is APK [I] =($A_{ij}, B_{ij} | j\epsilon [{}^{t}max]$)

Attribute generation

The token verification algorithm verifier the signature contained in γ using the signature verification key TVer in TPK. this algorithm extract K_{base} from γ and $\Lambda K_x = K_{base}^{1/(a+bx)}$.the key K_x can be checked for consistency using algorithm ABS.$keycheck(TP, APK[I], \gamma, K_X)$Which checks $e^{\Lambda}(K_x, A_{ij} B_{ij}^{x}) e^{\Lambda}(K_{base}, h_j)$.

Sign

The algorithm ABS .sign($TPK, \{APK[i]: i\epsilon AT[U]\}, \gamma, \{K_X : X\epsilon J_u\}, MSG,$)has input the public key of the trustee, the secret key for the message to be signed and the policy claim y.

1. Compute $\mu = Ḥ(MSG \| y)$

2. Choose r_o and r_i then compare Y,W

3.$Y = K_{base}^{ro}, s_i = \left(k_i^{vi}\right)^{ro} . \left(g_2 g_1^{\mu}\right)^{ri} (\forall i \in ju)$

4.W = $K_O^{ro}, p_j = \Pi_{I \epsilon AT[U]} (A_{ij} B_{ij} \pi'^{i})^{M_{ij}} r_i \; (\forall j \epsilon [t]$

5. Signature:$\sigma = Y, W, S1, S2, \ldots\ldots S_t, p_1 \ldots p_t)$

Verify

This uses the algorithm ABS. verify$(TPK, \sigma = \left(Y, W, S1, S2, \ldots S_t, p_1, p_2, \ldots p_t\right) MSG, Y)$

1. Compute $\mu = Ḥ(MSG \| y)$
2. if Y=1→ AB. verify = 0 → false
3. or else check $e^{\Lambda}(W, A_o) = e^{\Lambda}(Y, h_0)$

V. CONCLUSION & FUTURE WORK

we introduced a new encryption primitive called attribute based signature (ABS),and presented a construction that provably meets that requirements of ABS. the security proof we provide is in the key generation and encrypt using ABS. the construction is fairly efficient. for reasonably complex claim predicates.ABS scheme supports multiple attribute authorities and multiple signature-trustees, who need not trust each other.IN THIS future work, on the theoretical front, one would like to base the security on a standard hardness assumption, without sacrificing too much of the efficiency. the evident drawback of relying on security in the generic group model is in evaluating the underlying group used by a candidate implementation. in fact, even the "standard" hardness assumption, as the algorithmic study of such groups is relatively in its infancy.

REFERENCES

[1] SushmitaRuj,Milos stojmenvoic and and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in cloud",IEEE.2014.

[2] C.Wang Q.Wang, k.Ren, N.Cao, and W.lou,"Toward secure and dependable storage services in cloud computing,"IEEE Trans. Services computing, Apr-june 2012.

[3] H, Li, Dai, L.Tian, And H.yang,"Identity -Based Authentication for cloud computing,"Proc, First int'1 Conf.cloud computing, 2009.

[4]C.Gentry,"A Fully Homomorphi Encryption Scheme, "Phd dissertation, Stanford Univ, 2009.

[5]A-R Sadeghi, T.Schneider, and M.Winandy "Token Based Cloud computing" Proc. Third Int;1 Conf.Trust and Trustworthy computing(TRUST),2010.

[6]M.Li,S.yu,K,Ren.and W.Lou "Securing Personal Health Records In Cloud Computing :Patient -Centric and Fine -Grained Data Access Control In Multi-owner Settings ,"proc.Sixth Int;1 icst conf. security and privacy in com.Networks(SecureComm) ,2010.

[7]S.Yu, C.Wang K.Ren and Wang.K.Ren and W.Lou, "Attribute Based Data Sharing With Attribute Revocation."Proc.ACM Symp. Information, Computer and. Security (ASIACCS), 2010.

[8]G.Wang,Q.Liu, And J.WU, "Hierarchical Attribute Based Encryption For Fine Grained Access Control in cloud Storage Service."Proc.17th ACM Conf. Computer and comm. security (CCS), 2010.

[9]S.Ruj, A.nayak, and I.Stojmenovic,"DACC:Distributed Access Control in Cloud."pro.IEEE 10th Int'1 Conf.Trust, Security and Privacy in compiting and communication (trust),

[10]F.Zhao, T.Nishide, and K.shakurai,"Realing Fine Grained Flexible Access Control To Outsourced Data with Attributed Based Cryptsystem, "Proc.Senventh Int'1 Conf. Information Security Practice Experience (ISPEC), 2011.

[11]S.Seenulropia, R.Vijaylakshmi, "decentralized Access Control Of Data Stored In cloud Using Key Policy Attribute Based Encryption "International Journal Of Invention In Computer Science And Engineering,2014.

[12]http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud,2013.

[13]R.L Rivest, A.shamir, and Y.Tauman,"how to Leak a secrat"Proc.Senventh Int;1 Conf.Theory and Application of Cryptology and Information Security (ASIACRYPT),2001.

[14]X,Boyen."Mesh Signature"Proc.26th Ann.Int'1 conf. Advances in crytology (EUROCRYPT), 2007.

[15] D.Chaum and E.V Heyst"group signatures"proc.Int Conf, Advance in cytology (EUROCRYPT) 1991.

DOI 10.17148/IJARCCE.2015.4877