IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Attribute Based Encryption with Anonymous Authentication of Data Stored in Cloud

Shailesh Vijay Gawai

ME-II Student, Computer, PVPIT, Bavdhan, Pune, India

Abstract: I propose a new decentralized access control technique for data securly storing in clouds that supports anonymous authentication. In the proposed technique, the cloud verifies the authenticity of sequence without knowing the users identification before storing files. My technique also has the extra feature of access control in which only authorised users are able to (decode) decrypt the saved data. This technique restricts the replay attacks and confirms the creation, modification, and reading data stored in the cloud. I also includes and supports user revocation. Moreover, my authentication and access control technique is decentralized and robust, unlike other access control techniques designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

Keywords: Access control, authentication, attribute based signatures, attribute-based encryption, cloud storage, Information Security.

I. INTRODUCTION

Research in cloud computing is receiving plenty of attention from each educational and industrial worlds. In cloud computing, users will source their computation and storage to servers (also referred to as clouds) mistreatment net. This frees users from the hassles of maintaining resources on-site. Clouds will offer many varieties of services like applications (e.g. Google Apps, Microsoft online), infrastructures (e.g., Amazons EC2, Eucalyptus, Nimbus), and platforms to contribute developers write applications (e.g. Amazons S3, Windows Azure) Much of the information keep in clouds is very sensitive, for exam- ple, medical records and gregarious networks. Security and privacy are the vital problems in cloud computing. In one hand, the user ought to evidence itself before initiating any dealings, and on the conflicting hand, it must be ensured. That the cloud doesnt tamper with the information thats outsourced. User privacy is additionally needed so the cloud or different users dont understand the identity of the user. The cloud can hold the user accountable forth data it outsources, and likewise, the cloud is itself responsible for the services it provides. The validity of the user WHO stores the information is additionally verified. Except for the technical solutions to confirm security and privacy, theres conjointly a necessity for enforcement Recently, Wang et al. [2] self-addressed secure and dependable cloud storage. Cloud servers vulnerable to Byzantine failure, wherever a storage server will fail in whimsical ways in which [2]. The cloud is additionally vulnerable to knowledge modification and server colluding attacks. In server colluding attack, the soul can compromise storage servers, in order that it will modify knowledge files as long as theyre internally consistent. To provide secure knowledge storage, the info must be encrypted. However, the info is usually changed and this dynamic property must be taken under consideration whereas comingup with efficient secure storage techniques. Efficient search on encrypted knowledge is additionally a crucial concern in clouds. The clouds shouldnt understand the question but oughtto be able to come the records that satisfy the query. This canbe achieved by means that of searchable encoding [3], [4]. The keywords square measure sent to the cloud encrypted, and the cloud returns the result while not knowing the particular keyword for the search. The matter here is that the info records ought to have keywords related to them to enable the search. The proper records square measure came solely when searched with the precise keywords. Security and privacy protection in clouds are being explored by several researchers. Wang et al. [2] Self-addressed storage security victimization Reed- Solomon erasure-correcting codes. Authentication of users victimization public key crypto logical techniques has been studied in [5].Several holomorphic encoding techniques are recommended [6], [7] to ensure that the cloud isnt able to scan the info whereas performing the action of mathematical calculation on them. Victimization homomorphism encryption, the cloud receives cipher text of the info and performs computations on the cipher text and returns the encoded worth of the result. The user is in a position to rewrite the result, however the cloud doesnt understand what knowledge operated on. In such circumstances, it should be doable for the user to verify that the cloud returns accurate results. Accountability of clouds may be a terribly difficult task and involves technical problems and enforcement. Neither clouds nor users ought to deny any operations performed or requested. its vital to own log of the transactions performed; but, its a vital concern
to come to decision how much data to stay within the log. Answerability has been self-addressed in Trust Cloud [8]. Secure place of origin has been studied in [9]. Considering the subsequent situation: A educate, Alice, desires to send a

series of reports concerning some malpractices by authorities of University to all the professors of University, analysis chairs of universities in the country, and students happiness to Law department in all universities within the province. She desires to stay anonymous whereas business enterprise all proof of malpractice. She stores the knowledge within the cloud. Access management is important in such case, so solely approved users will access the info. Its additionally vital to verify that the information comes from a reliable supply. The issues of access management, authentication, and privacy protection should be solved at the same time. We have a tendency to address this downside in its completeness during this paper defined by the system. For instance, solely college members and senior secretaries might need access to information however not the junior secretaries.ABAC is addi- tional extended in scope, in which users are given attributes, and therefore the information has connected access policy. Solely users with valid set of attributes, satisfying the access policy, will access the info. The execsand cons of RBAC and ABAC are mentioned. . All these work use a science primitive referred to as attribute based coding (ABE). The protractible access management markup language [17] has been projected for ABAC in clouds [18] an area wherever access management is wide being employed is health care. Clouds area unit being employed to store sensitive information regarding patients to alter access to medical professionals, hospital employees,researchers, and policy manufacturers. It is vital to manage the access of information in order that solely authorized users will access the info. Using ABE, the records area unit encrypted underneath some access policy and hold on in the cloud. Users area unit given sets of attributes and corresponding keys. Only if the users have matching set of attributes, will they rewrite the data hold on in the cloud.

Access management is additionally gaining importance in on-line social networking wherever users (members) store their personal information,pictures, and videos share them with selected groups of users or communities they belong to. Access control in on-line social networking has been studied in [19]. Such information area unit being hold on in clouds. Its important that solely the approved users area unit given access to those information.An analogous state of affairs arises once information is hold on in clouds, as an example, in Drop box, and shared with bound groups of individuals. It is simply not enough to store the contents firmly within the cloud however it would even be necessary to confirm namelessness of the user. As an example,a user would love to store some sensitive data however doesnt need to be recognized. The user would possibly need to post a inquire into an editorial, but does not need his/her identity to be disclosed. However, the user ought to be able to sway the opposite users that he/she may be a valid user WHO hold on the data while not revealing the identity. There are a unit science protocols like ring signatures [20], mesh signatures [21], group signatures [22], which may be utilized in these things. Ring signature isnt a possible possibility for clouds wherever the area unit a large range of users. Cluster signatures assume the existence of a bunch which could not be attainable in clouds. Mesh signatures dont guarantee if the message is from a single user or several users colluding along. For these reasons, a brand new protocol referred to as attribute-based signature (ABS) has been applied. ABS was planned by Majiet al. [23].Itsa dditionally quite natural for clouds to own several KDCs in numerous locations within the world. In an earlier work, Ruj et al.[16] planned a distributed access control mechanism in clouds. However, the theme didnt provide user authentication. The opposite down- side was that a user will produce and store a file and alternative users will solely scan the file. Write access wasnt permissible to users apart from the creator.Within the preliminary version of this paper [1], we extend our previous work with additional options that allows to evidence the validity of the message while not revealing the identity of the user WHO has keep info within the cloud. During this version we tend to conjointly address user revocation, that wasnt self-addressed in [1]. We use ABS scheme [24] to attain legitimacy and privacy. Unlike [24], our theme is proof against replay attacks, in which a user will replace recent knowledge with stale knowledge from a previous write, though it not has valid claim policy. This is an important property as a result of a user, revoked of its attributes, and might not be ready to write to the cloud. We, therefore, add this further feature in our theme and modify [24] appropriately. Our theme conjointly permits writing multiple times that wasnt permissible in our earlier work.

II. REVIEW OF LITERATURE

A. Privacy Preserving Access Control with Authentication for Securing Data in Clouds:
In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

B. Ciphertext policy attribute-based encryption (CP-ABE):
In this paper, the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. One of

the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Ciphertext policy attribute-based encryption (CP- ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. However, the advantage comes with a majordrawback which is known as a key escrow problem. The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner wouldlike to make their private data only accessible to designated users. In addition, applying CP-ABE in the data sharing system introduces another challenge with regard to the user revocation since the access policies are defined only over the attribute universe. Therefore, in this study, we propose a novel CP- ABE scheme for a data sharing system by exploiting the characteristic of the system architecture. 1)The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data-storing center. 2) Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selec- tive attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

C. Anonymous authentication mechanisms for data stored in clouds:
This paper gives details about various methods prevailing inliterature of anonymous authentication mechanisms for data stored in clouds. It is a Decentralized access of system inwhich every system have the access control of data. The Cloud which is a Secured storage area where the anonymous authentication is used, so that only the permitted users can be accessed. Decrypting of data can be viewed only by a valid users and can also store information only by valid users. This Scheme prevents Replay attack which mean Eaves Dropping can be avoided, Support Creation of data inside storage, modifying the data by Unknown users, and Reading data stored in Cloud.

III. SYSTEM ARCHITECTURE

There are three users, a creator, a reader, and writer. Creator Alice receives a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token . There are multiple KDCs, which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.

Write proceeds in the same way as file creation. By designating the verification process to thecloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

IV. SYSTEM A NALYSIS

A. Proposed System
The main contributions of this paper are the following: Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and write on the data stored in the cloud. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud. Manages social insurance numbers etc. On presenting her id the trustee gives her a token. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. The creator decides on a claim policy Y, to proveher authenticity and signs the message under this claim. The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C.
If the user has attributes matching with access policy, it can decrypt and get back original message. Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from

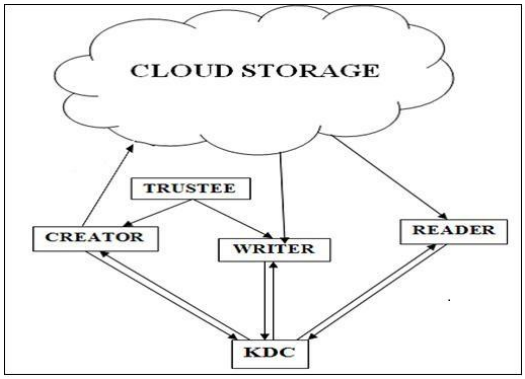
IJARCCE

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

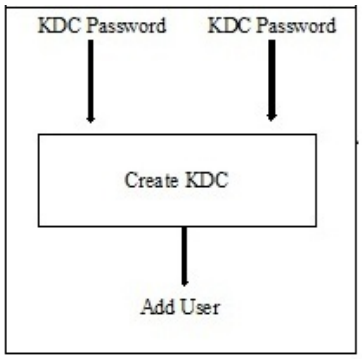
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

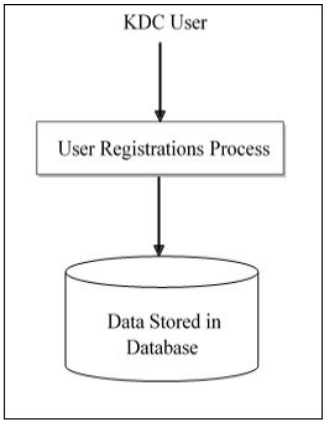
1) Creation of KDC system: Different number of KDC's are created and to register a user details. KDC name, KDC id and KDC password are given as input to create KDC. Inputs will save in a database and to register a user details given a input as username and user id.



2) KDC Authentication: After KDC given a user id to a user, the user will enrolled the personal details to KDC's given a input as user name, user id, password etc. The KDC will be verify the user details and it will insert it in a Database.



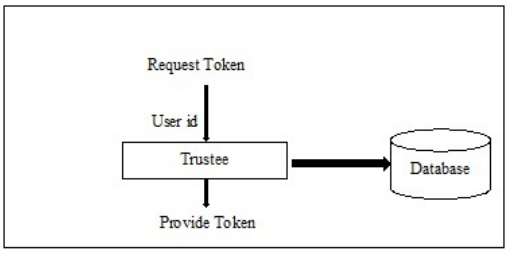
3) Trustee and User Accessibility: Users can get the token from trustee for the file upload. After trustee was issuing a token, trustee can view the logs. User can login with their credentials and request the token from trustee for the file upload using the user id. After the user id received by the trustee, trustee will be create token using user id, key and user signature (SHA).



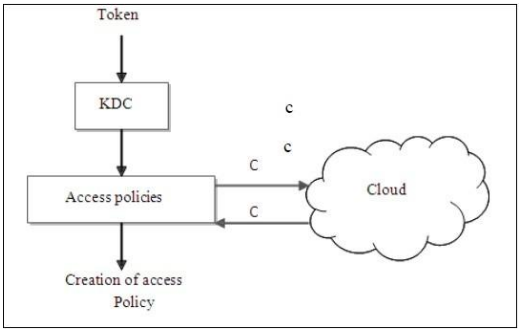
4) Creation of access policy : After the key was received by the User, the message MSG is encrypted under the access policies. The access policies decide who can access the data stored in the cloud. The cipher text C with signature is c,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

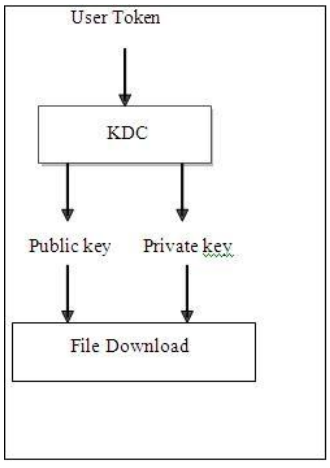
and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message and user can upload the file after user get key from the KDC.



5) File accessing : Using their access policies the users can download their files by the help of kdcs to issue the private keys for the particular users. After trustee token issuance for the users, the users produce the token to the KDC then the token verify by the KDC if it is valid then KDC will provide the public and Private key to the user. After users received the keys the files are encrypt with the public keys and set their Access policies (privileges).



6) Decentralized Access Control Mechanism : Attribute based encryption is used to secure the data and to make only authorized user to get access to the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Each user has set of attributes and their corresponding keys. For decrypting the information stored in cloud, users set of attributes should match with access policy.



B. Attribute Based Signature

It is used to secure the identity of user against the authenticity and privacy, who creates the data. Users have a claim predicate associated with a message, that makes easier to recognize the user as an authorized one, without revealing its identity. Similarly other users can verify authorization and validity of information stored. Usage of ABS with ABE helps to achieve authenticated access control without disclosing the identity of user to the cloud.

1) Algorithm of ABS:

• ABS is also uses the hash function for data encryption, Private Key and public key for message sign and verification.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

• KDC is used to generate token as signing key and signature.
• Token verification algorithm utilized for signature verification.
ABS.sign = for message signing
ABS.verify = for message authentication without revealing the identity of the user
• Encryption Process Encryption function is modeled as sender decides the access tree through Boolean access structure.
• Decryption process Decryption function takes cipher text, group; secret key, access matrix. Access matrix compares the attributes for similarity.

2) Attribute Based Ecryption: KP-ABE, the sender has an access policy to encrypt data. Here, once a writer having attributes and keys have been revoked cannot write back stale information. The attribute authority distributes attributes and secret keys to the receiver and can decrypt the message if it matches with access policy.

V. CONCLUSION

A decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks, is achieved. The cloud does not know the identity of the user who stores information, but only verifies the users credentials. Key distribution is done in a decentralized way and also hide the attributes and access policy of a user. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, using SQL queries for hide the attributes and access policy of a user. Files stored in cloudcan be corrupted. So for this issue using the file recovery technique to recover the corrupted file successfully and to hide the access policy and the user attributes.

REFERENCES

[1] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu,SPICE Simple Privacy-Preserving Identity-Managementfor Cloud Environment, Proc. 10th Intl Conf. Applied toCryptography and Network Security, 2012
[2] Y. Sun and K.J.R. Liu, Scalable Hierarchical Access Control in Secure Group Communications, Proc. IEEEINFOCOM 04, 2004.
[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham,Aggregate and Verifiably Encrypted Signatures from BilinearMaps,Proc. 22nd Intl Conf. Theory and Applications ofCryptographic Techniques,2003.
[4] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter,Patient Controlled Encryption: Ensuring Privacy of ElectronicMedical Records, Proc. ACM Workshop Cloud ComputingSecurity(CCSW09),2009.
[5] M.J. Atallah, M. Blanton, N. Fazio, and K.B.Frikken, Dynamic and Efficient Key Management for AccessHierarchies, ACM Trans. Information and System Security,vol.12, no. 3, pp. 18:1-18:43, 2009.
[6] L. Hardesty,Secure Computers Arent so Secure.MITpress, http://www.physorg.com/news176107396.html, 2009. [7]] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W.Lou, Privacy Preserving Public Auditing for Secure CloudStorage,IEEE Trans. Computers,Feb.2013
[8] F. Guo, Y. Mu, Z. Chen, and L. Xu, Multi-Identity Single-Key Decryption without Random Oracles,Proc.Information Security and Cryptology, 2007.
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters on ,Attribute-Based Encryption for Fine-Grained Access Controlof Encrypted Data, Proc. 13th ACM Conf. Computer andComm. Security, 2006.
[10] S.G. Akl and P.D. Taylor, Cryptographic Solutionto a Problem of Access Control in a Hierarchy,ACMTrans.Computer Systems, 1983.
[11] G.C. Chick and S.E. Tavares, Flexible Access Controlwith Master Keys,Proc. Advances in Cryptology (CRYPTO89, 1989.
[12] W.-G. Tzeng, A Time-Bound Cryptographic KeyAssignment Scheme for Access Control in a Hierarchy,IEEETrans. Knowledge and Data,Jan./Feb. 2002.
[13] G. Ateniese, A.D. Santis, A.L. Ferrara, and B.Masucci, Provably Secure Time-Bound Hierarchical KeyAssignment Schemes, J. Cryptology, 2012.
[14] R.S. Sandhu, Cryptographic Implementation of a Tree Hierarchy for Access Control, Information Processing Letters, 1988.
[15] Q. Zhang and Y. Wang, A Centralized Key Management Scheme for Hierarchical Access Control,Proc.IEEE Global Telecomm. Conf., 2004.
[16] A. Sahai and B. Waters, Fuzzy Identity-Based Encryption,Proc. 22nd Intl Conf. Theory and Applications of Cryptographic Techniques, 2005
[17] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou,and R.H. Deng, Dynamic Secure Cloud Storage with Provenance, Cryptography and Security, 2012.
[18] S. Ruj, M. Stojmenovic and A. Nayak, Privacy Preserving Access Control with Authentication for Securing Data in Clouds IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556563, 2012.
[19] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, Toward Secure and Dependable Storage Services in Cloud Computing, IEEE T. Services Computing, vol.5, no. 2, pp. 220232, 2012
[20] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, Fuzzy keyword search over encrypted data in cloud computing, in IEEE INFOCOM. , pp.44145, 2010
[21] S. Kamara and K. Lauter, Cryptographic cloud storage, in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol.6054. Springer, pp. 136149, 2010.
[22] H. Li, Y. Dai, L. Tian, and H. Yang, Identity-based authentication for cloud computing, in Cloud Com, ser. Lecture Notes in Computer Science, vol.5931. Springer, pp. 157166, 2009