International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016
ISSN 2091-2730

Anonymous Validation of Cloud Data and Distributed Entry Management

[1]K.V.G.N.NAIDU , [2]P..SIREESHA

[12]Assistant professor,[12]Department of Computer Science and Engineering,[12]NIST,Rajampet

[1]venkataguru2003@gmail.com,[2]sireeshapolicherla@gmail.com

Abstract— We propose a new localised access management theme for secure knowledge storage in clouds that supports anonymous authentication. In the proposed theme, the cloud verifies the authenticity of the series while not knowing the users identity before storing data. Our scheme additionally has the additional feature of access management in that solely valid users are able to decode the keep info. The scheme prevents replay attacks and supports creation, modification, and reading data keep in the cloud. We additionally address user revocation. Moreover, our authentication and access control theme is localised and sturdy, unlike alternative access management schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

Keywords— Access control, authentication, attribute-based sig- natures, attribute-based encryption, cloud storage

INTRODUCTION

Research in cloud computing is receiving a lot of attention from both tutorial and industrial worlds. In cloud computing, users can source their computation and storage to servers (also called clouds) victimisation net. This frees users from the hassles of maintaining resources on-site. Clouds can offer many varieties of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazons EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazons S3, Windows Azure). Much of the information hold on in clouds is extremely sensitive, for example, medical records and social networks. Security and privacy are, thus, very vital problems in cloud computing. In one hand, the user should attest itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the info that's outsourced. User privacy is also needed in order that the cloud or other users do not recognize the identity of the user. The cloud can hold the user account able for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is additionally verified. Apart from the technical solutions to ensure security and privacy, there is also a requirement for law enforcement. Recently, Wang et al. [2] addressed secure and dependable cloud storage. Cloud servers prone to Byzantine failure, where a storage server will fail in absolute ways in which [2]. The cloud is also susceptible to information modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it will modify information files as long as they are internally consistent. To provide secure data storage, the data must be en- crypted. However, the data is usually changed and this dynamic property needs to be taken into consideration whereas coming up with efficient secure storage techniques. Efficient search on encrypted information is additionally a crucial concern in clouds. The clouds should not recognize the question but ought to be ready to come the records that satisfy the query. This is achieved by means of searchable encoding [3], [4]. The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the info records should have keywords associated with them to enable the search. The correct records are came solely when searched with the actual keywords. Security and privacy protection in clouds are being explored by many researchers. Wang et al. [2] addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptologic techniques has been studied in [5]. Many homomorphic encryption techniques have been prompt [6], [7] to ensure that the cloud isn't able to browse the info whereas performing computations on them. Using homomorphic encryption, the cloud receives ciphertext of the data and performs computations on the ciphertext and returns the encoded value of the result. The user is able to decipher the result, but the cloud will not recognize what information it's operated on. In such circumstances, it must be attainable for the user to verify that the cloud returns correct results. Accountability of clouds is a terribly difficult task and involves technical issues and law social control. Neither clouds nor users should deny any operations performed or requested. It is important to possess log of the transactions performed; however, it is a crucial concern to determine how a lot of data to stay within the log. Accountability has been addressed in TrustCloud [8]. Secure provenance has been studied in [9]. Considering the following situation: A pupil, Alice, wants to send a series of reports regarding some malpractices by authorities of University X. to all the professors of University X, research chairs of

universities in the country, and students belonging to Law department in all universities in the province. She wants to stay anonymous while publication all proof of malpractice. She stores the information within the cloud. Access control is important in such case, so that solely licensed users will access the data. It is also vital to verify that the information comes from a reliable supply. The problems of access control, authentication, and privacy protection should be resolved at the same time. We address this drawback in its entirety in this paper. Access control in clouds is gaining attention as a result of it is important that solely licensed users have access to valid service. A huge quantity of data is being hold on within the cloud, and much of this can be sensitive data. Care should be taken to guarantee access management of this sensitive information that will typically be associated with health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking). There are broadly 3 varieties of access management: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list contains the list of users who ar licensed to access information. This is not feasible in clouds wherever there are several users. In RBAC (introduced by Ferraiolo and Kuhn [10]), users are classified based on their individual roles. Data will be accessed by users who have matching roles. The roles are defined by the system. For example, only school members and senior secretaries might have access to information however not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has hooked up access policy. Only users with valid set of attributes, satisfying the access policy, can access the information. For instance, in the above example bound records could be accessible by faculty members with a lot of than ten years of research expertise or by senior secretaries with a lot of than 8 years expertise. The pros and cons of RBAC and ABAC are mentioned in [11]. There has been some work on ABAC in clouds (for example, [12], [13], [14], [15], [16]). All these work use a cryptographic primitive famed as attributebased encryption (ABE). The eXtensible access management markup language [17] has been proposed for ABAC in clouds [18]. An space wherever access management is wide being employed is health care. Clouds are being used to store sensitive information regarding patients to change access to medical professionals, hospital staff, researchers, and policy makers. It is important to regulate the access of knowledge in order that solely authorized users will access the information. Using ABE, the records are encrypted underneath some access policy and hold on in the cloud. Users are given sets of attributes and corresponding keys. Only once the users have matching set of attributes, can they rewrite the data hold on in the cloud. Access control in health care has been studied in [12] and [13]. Access control is additionally gaining importance in on-line social networking where users (members) store their personal information, pictures, videos and 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 data are being hold on in clouds. It is vital that only the licensed users are given access to those information. A similar situation arises once information is hold on in clouds, for example, in Dropbox, and shared with certain groups of individuals. It is just not enough to store the contents firmly within the cloud but it would possibly even be necessary to confirm obscurity of the user. For example, a user would like to store some sensitive information however will not need to be recognized. The user might need to post a comment on a piece, but does not need his/her identity to be disclosed. However, the user should be ready to persuade the opposite users that he/ she is a valid user who hold on the data while not revealing the identity. There are cryptologic protocols like ring signatures[20], mesh signatures [21], group signatures [22], which will be employed in these things. Ring signature is not a feasible choice for clouds wherever there are a large range of users. Group signatures assume the existence of a group which could not be attainable in clouds. Mesh signatures do not ensure if the message is from a single user or many users colluding along. For these reasons, a new protocol referred to as attribute-based signature (ABS) has been applied. ABS was proposed by Maji et al. [23]. In ABS, users have a claim predicate associated with a message. The claim predicate helps to identify the user as an licensed 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 attain authenticated access management while not revealing the identity of the user to the cloud. Existing work [12], [13], [14], 15], [16], [18], [38] on access control in cloud are centralized in nature. Except [38] and [18], all other schemes use ABE. The scheme in [38] uses a symmetric key approach and will not support authentication. The schemes [12], [13], [16] do not support authentication as well. Earlier work by Zhao et al. [15] provides privacy preserving attested access management in cloud. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single purpose of failure however tough to keep up because of the big range of users that are supported in an exceedingly cloud environment. We, therefore, emphasize that clouds should take a localised approach whereas distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in numerous locations within the world. Although rule et al. [34] proposed a localised approach, their technique does not attest users, who want to stay anonymous whereas accessing the cloud. In an earlier work, Ruj et al. [16] proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other disadvantage was that a user will produce and store a file and different users can solely browse the file. Write access was not permitted to users apart from the creator. In the preliminary version of this paper [1], we extend our previous work with added options that allows to authenticate the validity of the message while not revealing the identity of the user who has

hold on data in the cloud. In this version we additionally address user revocation, that was not addressed in [1]. We use ABS scheme [24] to attain believability and privacy. Unlike [24], our scheme is resistant to replay attacks, in which a user can replace contemporary information with stale information from a previous write, even if it now not has valid claim policy. This is an important property as a result of a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our theme and modify [24] appropriately. Our scheme additionally permits writing multiple times which was not allowable in our earlier work [16].

Our Contributions

The main contributions of this paper are the following:

1. Distributed access control of information hold on in cloud therefore that only licensed users with valid attributes will access them.
2. Authentication of users who store and modify their data on the cloud.
3. The identity of the user is protected from the cloud during authentication.
4. The architecture is localised, meaning that there can be many KDCs for key management.
5. The access control and authentication are each collusion resistant, meaning that no 2 users will collude and access information or attest themselves, if they are on an individual basis not licensed.
6. Revoked users cannot access data once they have been revoked.
7. The proposed theme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.
8. The protocol supports multiple read and write on the data hold on within the cloud.
9. The costs are cherish the present centralized approaches, and the expensive operations are largely done by the cloud

RELATED WORK

Related work ABE was proposed by Sahai and Waters [26]. In ABE, a user has a set of attributes additionally to its unique ID. There are two categories of ABEs. In key- policy ABE or KP-ABE (Goyal et al. [27]), the sender has an access policy to write in code knowledge. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt info if it has matching attributes.In Ciphertext-policy, CP-ABE ([28], [29]), the receiver has the access policy in the type of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates. All the approaches take a centralized approach and allow solely one KDC, which is a single purpose of failure. Chase [30] proposed a multi authority ABE, in which there are many KDC authorities (coordinated by a sure authority) which distribute attributes and secret keys to users. Multi authority ABE protocol was studied in [31] and [32], that needed no sure authority which needs every user to have attributes from in any respect the KDCs. Recently, Lewko and Waters [35] proposed a totally sub urbanised ABE where users might have zero or additional attributes from every authority and did not require a sure server. In all these cases, decryption at users finish is computation intensive. So, this technique can be inefficient when users access victimization their mobile devices. To get over this problem, Green et al. [33] proposed to source the decipherment task to a proxy server, so that the user will cipher with minimum resources (for example, hand held devices). However, the presence of one proxy and one KDC makes it less robust than decentralized approaches. Both these approaches had no way to manifest users, anonymously. Yang et al. [34] presented a modification of [33], authenticate users, who want to stay anonymous whereas accessing the cloud. To ensure anonymous user authentication ABSs were introduced by Maji et al. [23]. This was also a centralized approach. A recent scheme by Maji et al. [24] takes a decentralized approach and provides authentication while not disclosing the identity of the users. However, as mentioned earlier in the previous section it's at risk of replay attack.

PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME

In this section, we propose our privacy preserving authen- ticated access control scheme. According to our scheme a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS. We will first discuss our scheme in details and then provide a concrete example to demonstrate how it works. We refer to the Fig. 1. 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 (here 2), 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, K 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 the cloud, 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.

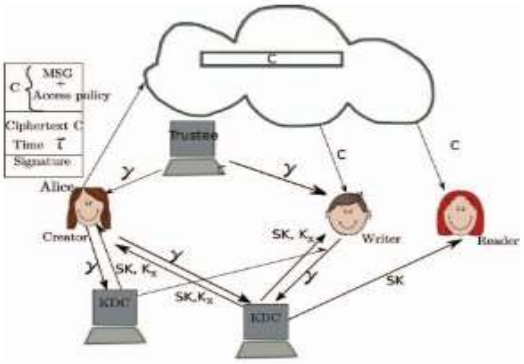

Fig. 1. Our secure cloud storage model

COMPARISON WITH OTHER ACCESS CONTROL SCHEMES IN CLOUD

We compare our theme with different access management schemes and show that our scheme supports several features that the different schemes didn't support. 1-W-M-R means that just one user will write whereas several users will read. M-W-M-R means that several users will write and browse. We see that most schemes don't support several writes which is supported by our theme. Our scheme is strong and de- centralized ,most of the others are centralized. Our scheme additionally supports privacy protective authentication, which is not supported by others. Most of the schemes do not support user revocation, which our theme will. We compare the computation and communication costs incurred by the users and clouds and show that our distributed approach has comparable costs to centralized approaches. The most expensive operations involving pairings and is done by the cloud. If we compare the computation load of user during scan we have a tendency to see that our scheme has comparable prices. Our scheme additionally compares well with the other echt theme of [15].

CONCLUSION

We have bestowed a decentralized access management technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user United Nations agency stores info, but solely verifies the users credentials. Key distribution is done in a decentralized manner. One limitation is that the cloud knows the access policy for every record keep within the cloud. In future, we would wish to hide the attributes and access policy of a user.

REFERENCES:

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563-2012
[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,vol. 5, no. 2, pp. 220-232, Apr.- June 2012.
[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.
[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.
[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.
[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.
[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.
[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.
[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.
[10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.
[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role- Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.
[12] 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'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.
[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.
[16] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
[17] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs- 01-en.pdf, 2013.
[18] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud, 2013.
[19] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,"Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.
[20] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.
[21] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.
[22] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.
[23] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
[24] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
[25] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.
[26] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473,2005.
[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[29] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.
[30] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[31] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority," Proc. Progress in ryptology Conf. (INDOCRYPT), pp. 426-436, 2008.

[32] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

[33] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp., 2011