International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Attribute-Based Access Control with Fixed-Size Cipher text

1 B.VINEELA U.SANDHYA

Abstract— Cloud computing is a radically new computing paradigm, which enables flexible, on demand, and low cost usage of computing resources , but the data is deployed to some cloud servers, and various privacy concerns emerge from it. Various layouts based on the attribute based encryption have been proposed to secure the cloud sto rage. However, most work targets on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, a semi anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in current access control schemes. AnonyControl decentralizes the central authority to limit the identity origin and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, which privileges of all operations on the cloud data can be managed in a compact structured manner. Subsequently, we present the AnonyControl F, which fully prevents the identity leakage and achieve the full anonymity. Our security presentation shows that both AnonyControl and AnonyControl F are secure under the Diffie Hellman assumption, and our performance estimation exhibits the feasibility of our schemes.

.

I. INTRODUCTION

Cloud computing is a complete computing technique, by which computing resources are provided dynamically via Internet and the data storage is outsourced to someone or some party in a „cloud". It greatly attracts attention and interest from both academia and industry due to the profit making, but it also has at least three challenges that must be handled before coming to our reality to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data seclusion is not only about the data contents. Since the most attractive part of the cloud computing is the outsourcing of computation, it is far beyond enough to just oversee an access control. More likely, users want to control the right of data manipulation over other users or cloud servers. [1] [2] This is because when sensitive information or computation is outsourced to the cloud servers or user,

which is out of users‟ control in most cases, privacy risks would raise constantly because the servers might illegally inspect users‟ data and access sensitive information, or other users might be able to infer careful information from the outsourced computation. Therefore, not only the access but also the operation should be managed. S econdly, personal information (defined by each user‟s attributes set) is at risk because user's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As everyone is becoming more concerned about their identity privacy these days, the identity privacy also has to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client‟s personal data. Last but not least, the cloud computing system should be resilient in the case of security breach in which

half part of the system is compromised by attackers. [1]

II. LITERATURE SURVEY

A.Cipher text Policy Attribute Based Encryption

AUTHORS:Taeho Jung, Xiang Yang Li, Zhiguo Wan, Meng Wan

In several distributed systems a user can able to access data if a user posses a certain set of credentials or attributes. Presently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server stores the data, which is compromised, then the confidentiality of the data will be compromised. In this paper, we present a process for realizing complex access control on encrypted data that we say Cipher text Policy Attribute Based En cryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; [2] moreover, our systems are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to explain the encrypted data and built policies into user‟s keys; while in our system attributes are used to explain a user‟s credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our systems are conceptually closer to traditional access control methods such as Role Based Access Control (RBAC). In addition, we ensure an implementation of our system and give performance measurements. [1]

B. **Multi Authority Attribute Based Encryption With Honest But Curious Central Authority**

AUTHORS: Vladim ir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi

An attribute based encryption scheme capable of handling multiple authorities were recently proposed by Chase. The scheme is built upon a single authority attribute based encryption technique presented earlier by Sahai and Waters. Chase‟s construction uses a trusted central authority that is inherently able to do decrypting arbitrary cipher texts created within the system. We present a multi authority attribute based encryption technique in which only the set of recipients defined by the encrypting party can decrypt a corresponding cipher text. The central authority is shown as "honest but curious": on the one hand it honestly follows the protocol, and on the other it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. The advance scheme, which like its predecessors relies on the Bilinear DiffieHellman assumption, has a complexity comparable to that of Chase‟s technique. We prove that our scheme is secure in the selective ID model and can tolerate an honest but curious central authority. Building on the proposal for multi authority based attribute based encryption from; we constructed a scheme where the central authority is no longer capable of decrypting arbitrary cipher texts created within the system. In addition to viewing security in the selective ID model, we showed that the proposed system can able to tolerate an honest but curious central authority. Since both Chase‟s scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chase‟s construction. However, since the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is suggested in applications where security against such a central authority is required. [9]

III. METHODOLOGY

Step 1:

In this project we are not only providing data content privacy, we are also providing identity privacy by using anony control.

•AnonyControl decentralizes the central authority to limit the identity origin and thus achieves semianonymity. Flexible and Fine Grained Attribute Based Data Storage

in Cloud Computing International Journal of Advanced Technology and Innovative Research Subsequently, we present the AnonyControl F, which fully prevents the identity leakage and achieve the full anonymity.

Step 2:

In our system we use Attribute Encryption Standard (AES) algorithm. This algorithm is used to protect classified information and is used by the total world to encrypt and decrypt sensitive data. AES consists of three block ciphers. AES 256 and this each cipher uses 128 bits of blocks using cryptographic keys 128,192 and 256 bits to encrypt and decrypt delicate data. So the ciphers uses same secret key for encrypting and decrypting. There are different rounds for keys. Each round consists of different steps include substitution, transposition and mixing of plain text. Finally the plain text is transformed into cipher text.

Step 3:

In our system, there are four types of systems: N Attribute Authorities (denoted as A), Cloud Server, D ata Owners and Data Consumers.

•A user can be a Data Owner and Data Consumer simultaneously.

•Data owner encrypt and uploads the files in to the cloud server. Data consumer decrypts and downloads the files from the cloud server.

Step 4:

To access and perform any operations on files the data owner and data consumer should first register in to the system.

• When they registered at a time password and unique id will send to their registered mail id.

Step 5:

To upload and download files by the user. The user may be a data owner and data consumer request the authority for permission.

• The authority provides public key to data owner and private key to consumer. Issuing keys by authority and authentication in our system is succeeding using attribute based encryption. [1] [5]

Step 6:

Attribute based encryption is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is conceivable only if the set of attributes of the user key matches the attributes of the

cipher text. A critical security aspect of Attribute Based Encryption is collusion resistance. An adversary that holds multiple keys should be able to access data if at least one individual key grants access.

Step 7:Using the keys provided by authority the users (data owner and data consumer) access the files in to and from the cloud server.

IV. IMPLEMENTATION

Implementation is the status of the project when the theoretical design is turned out into a working system. Thus it can be designed to be the most critical stage in achieving a successful new system and in giving the user, assurance that the new system will work and be effecti

ve. [4]

The

implementation stage involves accurate planning, analysis of

the existing system and it‟s constraints on implementation,

designing of methods to attain changeover and estimation of

changeover methods. [10]

A. Module Description

After

careful analysis the system has been classified to have the following modules:

- Registration based Social Authentication Module
- Security Module
- Attribute

-

based encryption module.

- Multi

-

authority module.

Fig.

1 represents the architectural flow of th

e modules

which we have used.

Fig

.

1

.

Architectural Flow Diagram

.

CONCLUSION

This paper introduces a semi anonymous attribute based privilege control scheme AnonyControl and a fully anonymous attribute based privilege control scheme AnonyControl F to address the user privacy

problem in a cloud storage server. By using the multiple authorities in the cloud computing system, our proposed schemes achieve not only fine grained privilege control but also identity anonymity while controlling privilege control based on users‟ identity information. More importa ntly, our system can accept up to N −2 authority compromise, which is highly preferable especially in Internet based cloud computing environment. We also direct detailed security and performance analysis which shows that AnonyControl both efficient and sec ure for cloud storage system. The AnonyControl F directly inherits the security of the AnonyControl and thus is equivalently secure as it. One of the upcoming future works is to introduce the efficient user repudiation mechanism on top of our anonymous ABE.Supporting user repudiation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes adaptable with existing ABE schemes support efficient user revocation is one of our futuree works.

REFERENCES

[1] A. Sahai and B. Waters,“Fuzzy Identity-Based Encryption,”*EUROCRYPT’05*, LNCS, vol. 3494, pp. 457-473,2005.

[2] J.Bethencourt,A.Sahai and B.Waters,“Ciphertext-PolicyAttribute-BasedEncryption,”*Proc. IEEE Symposium on Security and Privacy*,

[3]V. Goyal, O. Pandey, A. Sahai, andB. Waters, “Attribute-Based En-cryption for Fine-Grained [Access Control of Encrypted Data,”*Proc.13th ACM Conference on Computer and Communications Security(CCS ’06)*, pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] D. Boneh and M.K. Franklin,“Identity-Based Encryption from the Weil Pairing,” *SIAM Journal of Computing*, vol. 32, no. 3,pp. 586-615,2003.

[5] A. Boldyreva, V. Goyal, and V. Kumar,“Identity-Based En-cryption with Efficient Revocation,”*Proc.15th ACM conference on Computer and communications security(CCS ’ 08)*,pp. 417-426,2008.

[6] S. Yu, C. Wang, K. Ren, and W. Lou,“Attribute Based Data Sharing with Attribute Revocation,”*Proc.5th ACM Symposium on Information, Computer and Communications Security (ASIACCS ’ 10)*, pp. 261-270,2010.

[7] M. Yang, F. Liu, J. Han, and Z. Wang,“An Efficient Attribute based

Encryption Scheme with Revocation for Outsourced Data Sharing Control," *Proc.2011International Conference on Instru-mentation, Measurement, Computer, Communication and Control*,pp. 516-520,2011.

[8] P.K. Tysowski and M.A. Hasan,"Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applica-tions in Clouds," *IEEE Transactions onCloudComputing*, pp. 172-186, 2013.

[9] J. Hur and D. K. Noh,"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,"*IEEE Transactions onParallel and Distributed Systems*, pp. 1214-1221,2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou,"Achieving Secure, Scal-able, and Fine-Grained Data Access Control in Cloud Compu-ting,"*Proc. of IEEE INFOCOM'10*,pp. 1-9,2010.

[11] M. Green, S. Hohenbergerand B. Waters, "Outsourcing the decryp-tion of ABE ciphertexts,"*Proc.20th USENIX Conference on Security(SEC '11),* pp. 34, 2011.

[12] J. Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Maand W.J. Lou, "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryp-tion,"*Proc.18th European Symposium on Research in Computer Security(ESORICS '13)*,LNCS8134,Berlin: Springer-Verlag, pp. 592-609, 2013.

[13] J.W. Li, C.F. Jia, J. Liand X.F. Chen, "Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce,"*Proc.14th International ConferenceonInformation and Communications Security(ICICS '12),*LNCS7618,Berlin:Springer-Verlag, pp. 191-201, 2012.doi:10.1007/978-3-642-34129-8_17

[14] M.Chase, "Multi-authority Attribute Based Encryption,"*Proc.4th Theory of Cryptography Conference(TCC '07)*, LNCS4392,Berlin:Springer-Verlag, pp. 515-534, 2007.

[15] Z. Liu, Z. Cao, Q. Huang, D. S. Wongand T. H. Yuen, "Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles,"*Proc.16th European Symposium on Research in Computer Security(ESORICS '11)*, LNCS6879, Berlin:Springer-Verlag, pp. 278-297, 2011.

[16] J.G. Han, W. Susilo, Y. Mu andJ. Yan, "Privacy-Preserving Decentral-ized Key-

Policy Attribute-Based Encryption,"*IEEETransactions on Parallel and Distributed Systems*,vol.23, no.11, pp. 2150-2162, Nov 2012, doi: 10.1109/TPDS.2012.50.

[17] H.L. Qian, J.G. Liand Y.C. Zhang, "Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Ac-cess Structure,"*Proc.15th International ConferenceonInformation and Communications Security(ICICS '13)*,LNCS8233,Berlin:Springer-Verlag,pp. 363-372, 2013.

[18] H.L. Qian, J.G. Li, Y.C. Zhangand J.G. Han, "PrivacyPreserv-ingPersonalHealthRecordUsingMulti-AuthorityAttribute-BasedEncryption withRevocation,"*InternationalJournalofInfo rmation Security*,doi:10.1007/s10207-014-0270-9.

[19] Z.Liu, Z.F.Caoand Duncan S. Wong, "Black-Box Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay,"*Proc.2013 ACM SIGSAC Conference on Computer andCommunications Security(CCS '13)*,pp. 475-486, 2013, doi: 10.1145/2508859.2516683.

AUTHOR'S DETAILS:

1.B.VINEELA

vineelabjr@gmail.com

2.U.SANDHYA

ummadisettysandhya@gmail.com

ASSISTANT PROFESSOR