CONTROL CLOUD DATA ACCESS WITH ATTRIBUTE BASED ENCRYPTION IN CLOUD COMPUTING

Ms.M.SUSHMITHA, Miss P.Mounika

Abstract Cloud computing is a computing concepts, which enables when required and low maintenance usage of resources, but the data is shares to some cloud servers and various privacy related concerns emerge from it. Various schemes like based on the attribute-based encryption have been developed to secure the cloud storage. Most work looking at the data privacy and the access control, while less attention is given to the privilege control and the privacy. In this paper, we present a privilege control scheme Anonymity Control to address and the user identity privacy in existing access control. Anonymity Control decentralizes the central authority to limit the identity leakage and thus achieves partial anonymity. It also generates the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a proper manner. We present the Anonymity Control-F, which prevents the identity and achieve the anonymity. Our security analysis shows that both Anonymity Control and Anonymity Control-F are secure under the Diffie–Hellman assumption and our performance evaluation exhibits the feasibility of our schemes.

I. INTRODUCTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a 'cloud'. It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data

manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the servers might illegally inspect users' data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.

II. LITERATURE SURVEY

The concept of ABE for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Secret-sharing schemes (SSS) are used to divide a secret among a number of parties. Matthew Pirretti and Brent Waters introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. A performance analysis of ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, demonstrates that the attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. Decryption decrypts a ciphertext encrypted by the Encryption. This process

begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key. John Bethencourt, AmitSahai, Brent Waters introduces Ciphertext-Policy Attribute-Based Encryption in 2008. They employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, 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 storing the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of the system and give performance measurements. The primary challenge in this line of work is to find new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010.

It illustrates the basic principles on which architecture for combining access control and cryptography can be built. Then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. It also described an approach for policy evolution that takes into account the main features of the scenario and is able to guarantee in most cases confidentiality of the information in the presence of significant policy updates, clearly identifying the exposure to collusion when this risk may arise. Other issues to be investigated include the integration with the Web paradigm, and the efficient execution of queries. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi introduced Anonymity-preserving PublicKey Encryption: A Constructive Approach where publickey cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). They use the constructive cryptography approach by Maurer and Renner and interpret cryptographic schemes

as constructions of a certain ideal resource (e.g. a confidential anonymous channel) from given real resources (e.g. a broadcast channel) and defined appropriate anonymous communication resources and show that a very natural resource can be constructed by using a PKE scheme which fulfills three properties that appear in cryptographic Literature. Results do not only support the trust in existing schemes and constructions; they also show that the simpler and more efficient weakly robust schemes can be used safely. Junbeom Hur, Dong Kun Noh introduces the concept of Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a reencryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it. R.Ranjith and D.Kayathri Devidescribes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous

Authentication in 2013. It is implemented with secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination.

Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches. Mr. ParjanyaC.A and Mr. Prasanna Kumar describe the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in March 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This

method claims required efficiency, scalability and most importantly reliability. Extensive analyses show that proposed scheme satisfies the desired security requirements and guarantees efficiency as well. Here it also show that how user gets extra time even after the time out this also one of the advantage of proposed schema. S DivyaBharathy and T Ramesh introduced the concept of privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control in April 2014. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks.

III PROPOSED SYSTEM

Propose anonymity Control to allow cloud servers to control users' access privileges without knowing their identity information.

1. The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in anonymity Control and no information is disclosed in anonymity Control-F.

2. The proposed schemes are tolerant against authority compromise, and compromising of up to $(N-2)$ authorities does not bring the whole system down.

3. Provided detailed analysis on security and performance to show feasibility of the scheme anonymity Control and anonymity Control-F.

4. First implement the real toolkit of a multi-authority based encryption scheme anonymity Control and anonymity Control-F.

In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. However, the scheme proposed by Chase considered the basic threshold-based KP-ABE, which lacks generality in the encryption policy expression. Many attribute based encryption schemes having multiple authorities have been proposed afterwards, but they either also employ a threshold-based ABE or have a semi-honest central authority, or cannot tolerate arbitrarily many users' collusion attack.
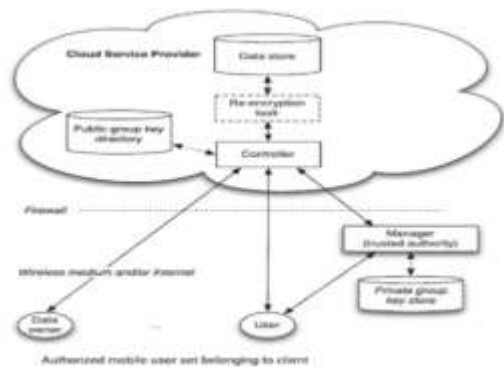
ARCHITECTURE

IVALGORITHMS IMPLEMENTATION

Algorithm 1 1-Out-of-2 Oblivious Transfer
1: Bob randomly picks a secret s and publishes gs to Alice. 2: Alice creates an encryption/decryption key pair:$\{gr, r\}$ 3: Alice chooses i and calculates $EK_i = gr$, $EK_i-1 = gs\ gr$ and sends EK_0 to Bob. 4: Bob calculates $EK_1 = gs\ EK_0$ and encrypts M_0 using EK_0 and M_1 using EK_1 and sends two cipher texts $EEK_0(M_0)$, $EEK_1(M_1)$ to Alice. 5: Alice can use r to decrypt the desired cipher text $EEK_i(M_i)$, but she cannot decrypt the other one. Meanwhile, Bob does not know which cipher text is decrypted.

Algorithm 2 1-Out-of-n Oblivious Transfer
1: Bob randomly picks n secrets s1, . . . , sn and calculates ti as follows: $\forall i \in \{1, \ldots, n\}$: $t_i = s_1 \oplus \cdots \oplus s_{i-1} \oplus M_i$ 2: For each $i \in \{1, \ldots, n\}$, Bob and Alice are engaged in a 1-out-of-2 OT where Bob's first message is ti and the second message is si . Alice picks ti to receive if she wants Mi and si otherwise. 3: After Alice receives n components, she has $t_i = s_1 \oplus \cdots \oplus s_{i-1} \oplus M_i$ for the i she wants and sk for $k \neq i$, she can recover the Mi by I. $M_i = t_i \oplus s_{i-1} \oplus s_{i-2} \oplus \cdots \oplus s_1$

V. RESULTS AND DISCUSSION

The system consists of modules Public Key: In this Module public key is generated for authentication for the user to provide the user specification logging. .

File Storage The File Storage module the file stored for the further usage of the consumer and the file is provided the option to view and Download based on the time period keys.

Encryption The files are encrypted in order to provide security to the documents or the contents of the provider

Data Access Control The Data Access control is provided to the consumer for the limited access to the cloud for the performance and usage of the cloud

Data Access The Data can be accessed by viewing the content of the file or downloaded

Fig 1. Login form

Fig 2. Show n-authorities database

Attribute based encryption is using data uploaded. This is each and every node encrypted data in store. Fine-Grain concept using encrypted data convert into binary value fully secure for database.

Fig 3. Database upload

Fig 4. Consumer database

Various techniques have been proposed to protect the data contents privacy via access control.

VI. CONCLUSIONS

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fullyanonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also

identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that Anony- Control both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer.

One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes [39]–[41] who support efficient user revocation is one of our future works.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO. Springer, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EURO-CRYPT. Springer, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributebased encryp-tion for fine-grained access control of encrypted data," in CCS. ACM, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in S&P. IEEE, 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in TCC. Springer, 2007, pp. 515–534.

[6] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS. ACM, 2009, pp. 121– 130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Bozovič, D. Socek, R. Steinwandt, and V. I. Villanyi, "Multi-authority attribute-based encryption with honest-butcurious central authority," IJCM, vol. 89, no. 3, pp. 268– 283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R.-W. Phan, "Low com-plexity multi-authority attribute based encryption scheme for mobile cloud computing," in SOSE. IEEE, 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "Dac-macs: Effective data access control for multi-authority cloud storage systems," in INFOCOM. IEEE, 2013, pp. 2895–2903.

Author's profile:

Ms. P.Mounika received M.Tech degree from Gokaraju Rangaraju Institute of Engineering & Technology affiliated to JNTUH, Hyderabad. He is currently working as Assistant professor, Department of CSE, in Nalgonda Institute of Technology &Sceince ,Nalgonda, Telangana, India. Her interests includes Web Technologies, Java Programming, Data Base Management Systems.

 Ms.SUSHMITHA received B.Tech Degree from Swamy Ramandhathirda Institute Of Technology and Science . She is currently pursuing M.tech Degree in Computer Science and Engineering specialization in Nalgonda Instituite of Technology & Science in Nalgonda, Telangana, India.