International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

A Fully Anonymous Attribute-Based Encryption to Control Cloud Data Access and Anonymity

Chanda Gurnule[*1], Prof. Bhagyashree Madan[2]

[*1]M.Tech Student, Department of Computer Science and Engineering, W.C.E.M, Nagpur, Maharashtra, India
[2]Assistant Professor, Department of Computer Science and Engineering, W.C.E.M, Nagpur, Maharashtra, India

ABSTRACT

Cloud computing is a processing ideas, which empowers when required and low support use of assets, yet the information is offers to some cloud servers and different security related concerns rise up out of it. Different plans like based on the attribute-based encryption have been produced to secure the distributed storage. Most work taking a gander at the information protection and the access control, while less consideration is given to the benefit control and the security. In this paper, we display a benefit control plot Anonymity Control to address and the client character protection in existing access control. Anonymity Control decentralizes the focal authority to constrain the character spillage and subsequently accomplishes incomplete anonymity. It additionally produces the file access control to the benefit control, by which benefits of all operations on the cloud information can be overseen in an appropriate way. We exhibit the Anonymity Control-F, which keeps the personality and accomplish the anonymity. Our security examination demonstrates that both Anonymity Control and Anonymity Control-F are secure under the Diffie–Hellman supposition and our performance assessment shows the feasibility of our plans.

Keywords: Anonymity, Multi-Authority, Attribute-Based Encryption

I. INTRODUCTION

Cloud processing is a progressive registering method, by which figuring assets are given powerfully by means of Internet and the information stockpiling and calculation are outsourced to somebody or some gathering in a 'cloud'. It significantly pulls in consideration and enthusiasm from both scholarly community and industry because of the profitability, however it likewise has no less than three difficulties that must be taken care of before going to our genuine to the best of our insight. First, information confidentiality ought to be ensured. The information security is not just about the information substance. Since the most alluring piece of the cloud, registering is the calculation outsourcing; it is far sufficiently past to simply lead an access control. More probable, clients need to control the benefits of information control over different clients or cloud servers. This is on the grounds that when touchy information or calculation is outsourced to the cloud servers or another client, which is out of clients' control as a rule, security dangers would rise significantly on the grounds that the servers may wrongfully investigate clients' information and access delicate information, or different clients may have the capacity to infer delicate information from the outsourced calculation. Therefore, the access as well as the operation ought to be controlled.

In addition, individual information (defined by every client's attributes set) is at hazard since one's personality is validated based on his information for the reason for access control (or benefit control in this paper). As individuals are winding up noticeably more worried about their character security nowadays, the personality protection additionally should be ensured before the cloud enters our life. Preferably, any authority or server alone ought not to know any customer's close to home information. To wrap things up, the cloud-figuring framework ought to be flexible because of security rupture in which aggressors bargain some piece of the framework.

Different procedures have been proposed to secure the information substance protection by means of access control. Shamir [1], in which the sender of a message can specify a personality to such an extent that exclusive a collector with coordinating personality can decode it, first presented character based encryption (IBE). After few years, Fuzzy Identity-Based Encryption [2] is proposed, which is otherwise called Attribute-Based Encryption (ABE). In such encryption conspire, a personality is seen as an arrangement of illustrative attributes, and decoding is conceivable if a decrypt's character has a few covers with the one specified in the ciphertext. Before long, more broad tree-based ABE plans, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4], are introduced to express more broad condition than straightforward 'cover'. They are partners to each other as in the choice of encryption strategy (who can or cannot decode the message) is made by different gatherings.

In the KP-ABE [3], a ciphertext is related with an arrangement of attributes, and a private key is related with a monotonic access structure like a tree, which portrays this current client's character (e.g. IIT AND (Ph.D OR Master)). A client can unscramble the ciphertext if and just if the access tree in his private key is satisfied by the attributes in the ciphertext. Notwithstanding, the encryption approach is portrayed in the keys, so the encryptor does not have whole control over the encryption strategy. He needs to trust that the key generators issue keys with right structures to right clients. Furthermore, when a re-encryption happens, the majority of the clients in a similar framework must have their private keys re-issued in order to access the re-encoded files, and this procedure causes significant issues in usage. Then again, those issues and overhead are altogether explained in the CP-ABE [4]. In the CP-ABE, ciphertexts are made with an access structure, which specifies the encryption approach, and private keys are created by clients' attributes. A client can unscramble the ciphertext if and just if his attributes in the private key satisfy the access tree specified in the ciphertext. Thusly, the encryptor holds a definitive authority about the encryption strategy. Additionally, the as of now issued private keys will never be modified unless the entire framework reboots.

Not at all like the information confidentiality, is less effort paid to secure clients' personality protection amid those intuitive conventions. Clients' characters, which are depicted with their attributes, are largely revealed to key backers, and the guarantors issue private keys as per their attributes. However, it appears to be characteristic that clients will keep their personalities mystery while despite everything they get their private keys. Therefore, we propose AnonyControl and AnonyControl-F (Fig. 1) to permit cloud servers to control clients' access benefits without knowing their character information.

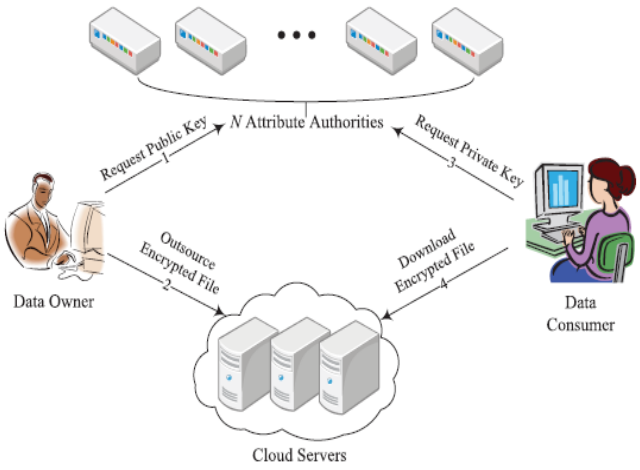

Figure 1: General Flow of System

Their primary benefits are:

1) The proposed plans can ensure client's protection against each single authority. Fractional information is revealed in AnonyControl and no information is uncovered in AnonyControl-F.
2) The proposed plans are tolerant against authority trade off, and bargaining of up to (N −2) experts does not cut the entire framework down.
3) We give nitty gritty investigation on security and performance to show feasibility of the plan AnonyControl and AnonyControl-F.
4) We firstly actualize the genuine toolbox of a multi-authority based encryption conspire AnonyControl and AnonyControl-F.

II. RELATED WORK

The concept of ABE for Fine Grained Access Control of Encrypted Data in 2006 [5]. 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 labelled 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 [6]. 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 Bethen court, Amit Sahai, Brent Waters introduces Ciphertext-Policy Attribute-Based Encryption in 2008 [6]. 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 [7]. 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 [8] Anonymity-preserving Public-Key Encryption: A Constructive Approach where public-key cryptosystems with enhanced security properties have been proposed. It investigates 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 fulfils 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 [9]. 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 re-encryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it. R.Ranjith and D.Kayathri Devi describes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013 [10]. 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[11]. 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 shows that how user gets extra time even after the time out this also one of the advantage of proposed schema. S Divya Bharathy 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 [12]. 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 permit cloud servers to control clients' access benefits without knowing their personality information.

1. The proposed plans can ensure client's protection against each single authority. Fractional information is revealed in anonymity Control and no information is unveiled in anonymity Control-F.
2. The proposed plans are tolerant against authority bargain, and trading off up to (N −2) experts does not cut the entire framework down.
3. Given nitty gritty investigation on security and performance to show feasibility of the plan anonymity Control and anonymity Control-F.
4. First execute the genuine toolbox of a multi-authority based encryption plot anonymity Control and anonymity Control-F.

In this setting, every authority knows just a piece of any client's attributes, which are insufficient to figure out the client's personality. Be that as it may, the plan proposed by Chase considered the essential limit based KP-ABE, which needs all inclusive statement in the encryption arrangement expression. Many attribute based encryption plans having multiple experts have been proposed afterwards, yet they either additionally utilize a limit based ABE or have a semi-genuine focal authority, or cannot endure self-assertively many clients' intrigue assault.

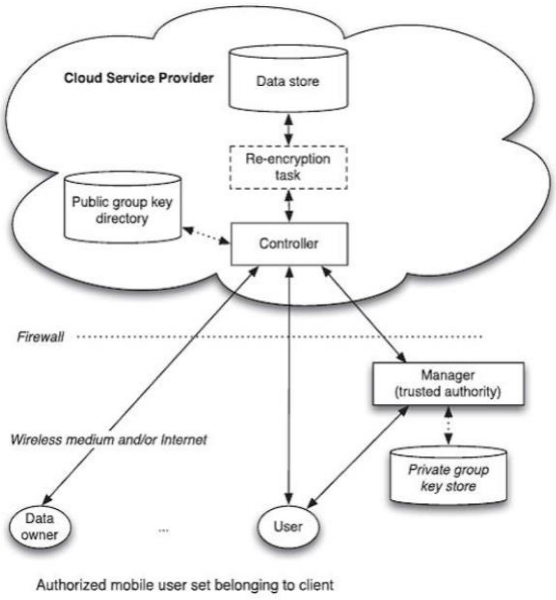

Figure 2: System Architecture

IV. ALGORITHMS 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 *EKi* = *gr* , *EKi*−1 = *gs*
4. *gr* And sends *EK*0 to Bob.
5. Bob calculates *EK*1 = *gs*

EK0

And encrypts *M*0 using

EK_0 and M_1 using EK_1 and sends two cipher texts $E_{EK_0}(M_0)$, $E_{EK_1}(M_1)$ to Alice.
5: Alice can use *r* to decrypt the desired cipher text *EEKi (Mi), but she cannot decrypt the other one. Meanwhile,*
Bob does not know which cipher text is decrypted.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

V. RESULTS AND DISCUSSION

We introduce the performance assessment based on our estimation on the actualized model arrangement of AnonyControl-F. To the best of our insight, this is the first execution of a multi-authority attribute based encryption conspire. Our model framework gives five order line instruments.

- anonycontrol-setup: Jointly creates an open key and N ace keys.
- anonycontrol-keygen: Generates a piece of private key for the attribute set it is in charge of.
- anonycontrol-enc: Encrypts a file under r benefit trees.
- anonycontrol-dec: Decrypts a file if conceivable.
- anonycontrol-rec: Decrypts a file and re-encodes it under different benefit trees.

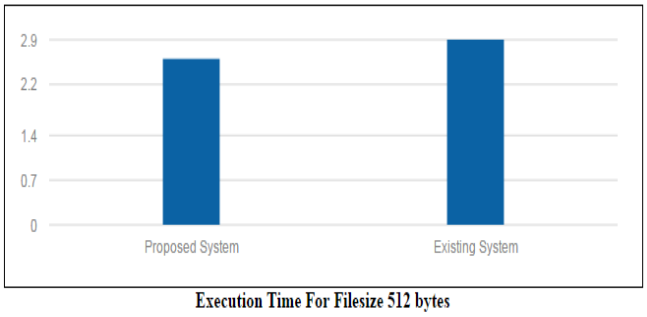

Figure 3: Execution Time comparison for encryption of 512 Bytes of Data

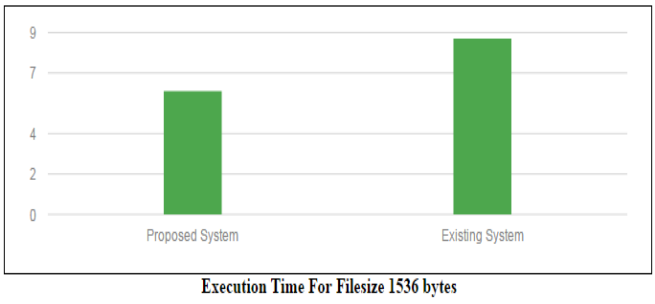

Figure 4: Execution Time comparison for encryption of 1536 Bytes of Data

Figure 3 and 4 demonstrates the consequences of the encryption efficiency for different file measure. We have considered two-file measure one is 512 bytes and second 1536 bytes. Result demonstrates the efficiency examination of the current framework and proposed framework. From the outcomes, we can reason that our framework is more efficient as that of existing instrument.

VI.CONCLUSION

This paper proposes a semi-unknown attribute-based benefit control plot AnonyControl and a fully-mysterious attribute-based benefit control conspire AnonyControl-F to address the client protection issue in a cloud stockpiling server. Utilizing multiple experts in the cloud registering framework, our proposed plans accomplish fine-grained benefit control as well as character anonymity while directing benefit control based on clients' personality information. All the more imperatively, our framework can endure up to N − 2 authority trade off, which is profoundly preferable particularly in Internet-based cloud figuring condition. We additionally directed itemized security and performance investigation which demonstrates that Anony-Control both secure and efficient for cloud stockpiling framework. The AnonyControl-F straightforwardly acquires the security of the AnonyControl and in this way is proportionately secure as it, however additional correspondence overhead is caused amid the 1-out-of-n negligent transfer.

One of the promising future works is to present the efficient client disavowal component on top of our unknown ABE. Supporting client denial is an essential issue in the genuine application, and this is an incredible test in the utilization of ABE plans. Making our plans good with existing ABE plans [39]–[41] who bolster efficient client denial is one of our future works.

VII. REFERENCES

[1] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEE SP, May 2007, pp. 321–334.
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryp-tion for fine-grained access control of encrypted data,” in CCS. ACM, 2006, pp. 89–98.
[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in S&P. IEEE, 2007, pp. 321–334.
[7] M. Chase, “Multi-authority attribute based encryption,” in TCC. Springer, 2007, pp. 515–534.
[8] M. Chase and S. S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in CCS. ACM, 2009, pp. 121– 130.
[9] 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.
[10] V. Bozovi˘c,´ D. Socek, R. Steinwandt, and V. I. Villanyi,´ “Multi-authority attribute-based encryption with honest-but-curious central authority,” IJCM, vol. 89, no. 3, pp. 268–283, 2012.
[11] 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.
[12] 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.