 ISSN: 2321-8169
84 – 86

Organize Cloud Data Access Privilege and Anonymity with Fully Nameless Attribute-Based Encryption

[1] R. Ravikumar, [2] C. Sivasamy
[1]Asst.professor, Dept.of.Computer Science, Tamil University, Thanjavur-613010
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010

Abstract: Cloud computing may be a computing ideas that allows once needed and low maintenance usage of resources, however the info is shares to some cloud servers and varied privacy connected issues emerge from it. Various schemes based on the Attribute-Based Encryption have been proposed to secure the cloud storage. However, most work focuses 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, we present a semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

Keywords: *Anonymity, multi-authority, attribute-based encryption.*

*****

I. INTRODUCTION

Cloud computing could be a revolutionary computing technique, by that computing resources are provided dynamically via web and therefore the knowledge storage and computation are outsourced to somebody or some party in an exceedingly cloud. In cloud storage systems, there are multiple authorities co-exist and every authority is ready to issue attributes severally [9].Cloud computing provides a ascendable, location-independent and high performance resolution by relegation computation tasks and storage into the resource-rich clouds.

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. Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it.

II. REIMBURSEMENT OF CLOUD COMPUTING:

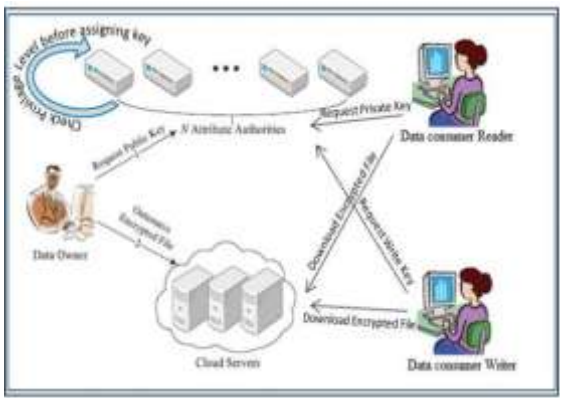
1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.

2. **Reduce spending on technology infrastructure** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.

3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.

4. **Streamline processes.** Get more work done in less time with less people.

5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.



III. DESCRIPTION SYSTEM

1. Attribute Authorities:

Every AttributeAuthority is a self-sufficient trademark master that is accountable for entitling and

 ISSN: 2321-8169
84 – 86

renouncing customer's credits according to their part or identity in its territory. In our arrangement, every characteristic is connected with a single Attribute Athourity, however every AttributeAuthority can manage a subjective number of characteristics. Every AttributeAuthority has full control over the structure and semantics of its qualities. Each AttributeAuthority is responsible for making an open quality key for every trademark it administers and a puzzle key for each customer reflecting his/her properties.

2. Data Consumers:

Every client has a worldwide character in the framework. A client might be entitled an arrangement of characteristics which may originate from various property specialists. The client will get a mystery key related with its qualities entitled by the comparing property specialists.

3. Data Owners:

Every proprietor first partitions the information into a few segments as indicated by the rationale granularities and encodes every information segment with various substance keys by utilizing symmetric encryption systems. At that point, the proprietor characterizes the get to approaches over properties from numerous property experts and scrambles the substance keys under the strategies.

4. Cloud Server:

At that point, the proprietor sends the scrambled information to the cloud server together with the figure writings. They don't depend on the server to do information get to control. Be that as it may, the get to control occurs inside the cryptography. That is just when the client's qualities fulfill the get to strategy characterized in the figure message; the client can decode the ciphertext. Along these lines, clients with various characteristics can decode diverse number of substance keys and in this way get distinctive granularities of data from similar information.

IV. THREATS MODEL

We assume the Cloud Servers are semi-honest, who behave properly in most of time but may collude with malicious Data Consumers or Data Owners to harvest others' file contents to gain illegal profits. But they are also assumed to gain legal benefit when users' requests are correctly processed, which means they will follow the protocol in general. N authorities are assumed to be untrusted. That is, they will follow our proposed protocol in general, but try to find out as much information as possible individually. More specifically, we assume they are interested in users' attributes to achieve the identities, but they will not collude with users or other authorities. This assumption is similar to many previous researches on security issue in cloud computing, and it is also reasonable since these authorities will be audited by government offices.

V. METHODOLOGY

Step 1: In this project we are not only providing data content privacy, we are also providing identity privacy by using anonycontrol. AnonyControl decentralizes the focal specialist to constrain the character starting point and subsequently accomplishes emianonymity. Subsequently, we introduce the AnonyControl-F, which completely keeps the personality spillage and accomplish the full obscurity.

Step 2: In our framework we utilize Attribute Encryption Standard (AES) calculation. This calculation is utilized to secure characterized data and is utilized by the aggregate world to scramble and decode delicate data.AES comprises of three piece figures. AES-128, AES-192,AES-256 and this each figure utilizes 128 bits of pieces utilizing cryptographic keys 128,192 and 256 bits to scramble and decode sensitive information. So the figures utilizes same mystery key for encoding and decoding. There are distinctive rounds for keys.Each round comprises of various strides incorporate substitution,transposition and blending of plain content. At long last the plain content is changed into figure content.

Step 3: In our system, there are four types of systems: A client can be a Data Owner and Data Consumer simultaneously.Data proprietor scramble and transfers the records into the cloud server. Information buyer decodes and downloads the documents from the cloud server.

Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it‟s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. Module description: Number of Modules After careful analysis the system has been identified to have the following modules:

1. Registration based Social Authentication Module 2. Security Module Attribute-based encryption module.
3. Multi-authority module. 1. Registration -Based Social Authentication Module: The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator, and then a few friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's Registration. 2. Security Module: Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your

 ISSN: 2321-8169
84 – 86

information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. Trustee based social authentication systems ask users to select their own trustees without any constraint. In our experiments, we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees.

VI. CONCLUDION

This paper proposes a semi-anonymous attribute-based privilege management theme AnonyControl and a completely anonymous attribute-based privilege management theme AnonyControl-F to deal with the user privacy drawback in a very 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. 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.

REFERENCE

[1] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan,‖ Cipher text-Policy Attribute-Based Encryption‖, T Jung - 2015.

[2] 7th Theory of Cryptography Conference, TCC 2010, Zurich,Switzerland, February 9-11, 2010, Proceedings.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in Proc. 13thCCS, 2006, pp. 89–98.

[4] aters, "Ciphertext-policy attributebased encryption," in Proc. IEEE SP, May 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] J. Horwitz and B. Lynn, "Toward hierarchical identity-b ased encryption," in Advances in Cryptology–EUROCRYPT 2002 , Springer, 2002, pp. 466–481.

[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based en cryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, 2008, pp. 417– 426.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R.-W. Phan, "Low complexity 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.