International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 8 (August '2016)

PRIVACY PRESERVING DATA ACCESS CONTROL PREVILIGES WITH FULLY ANONYMOUS ATTRIBUTE-BASED ENCRYPTION

Dr.G.Kesavaraj,
Professor &Head,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women, (Autonomous),
Elayampalayam, Namakkal, Tamilnadu

K.Anitha,
M.Phil Scholar,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women, (Autonomous),
Elayampalayam, Namakkal, Tamilnadu

Abstract: A data services in the cloud, users can easily modify and share data as a group. To ensure data integrity can be audited publicly, users need to compute signatures on all the blocks in shared data. Different blocks are signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks, which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud.

Key words: Anony control, Anony Control- F, DiffeHellman assumption,Data access control

I. INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. For that reason the Office of the Privacy Commissioner of Canada (OPC) has prepared some responses to Frequently Asked Questions (FAQs). To have also developed a Fact Sheet that provides detailed information on cloud computing and the privacy challenges it presents.

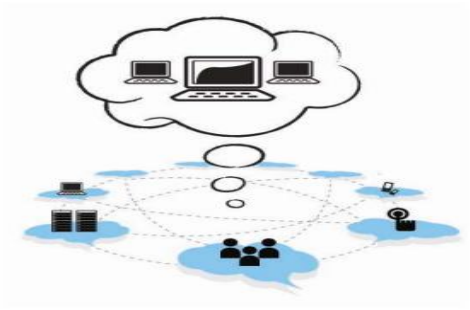

Figure 1: Cloud Computing

The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST).Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

II. SERVICE MODELS

The cloud computing service models are Software as a Service (Saas), Platform as a Service (Paas) and Infrastructure as a Service (Iaas). In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In Paas, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications.

DEPLOYMENT OF CLOUD SERVICES

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the

general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud. In a **private cloud**, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party. In a **community cloud**, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider. A **hybrid cloud** is a combination of different methods of resource pooling (for example, combining public and community clouds).

III. RELATED WORK

In cloud computing network, [1] in this paper, we propose a new identity-based identification (and signature) scheme based on error-correcting codes. . the scheme can also work in signature but leads to very large signature of size 1mo .[2] we introduce a new type of identity-based encryption (ibe) scheme that we call fuzzy identity-based encryption. in fuzzy ibe we view an identity as set of descriptive attributes. we prove the security of our schemes under the selective-id sec.[3]. as more sensitive data is shared and stored by third-party sites on the internet, there will be a need to encrypt data stored at these sites we demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes hierarchical identity-based encryption (hibe).[4]. In this paper, we propose dac-macs (data access control for multi-authority cloud storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority cp-abe scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security.

IV. EXISTING SYSTEM

Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns 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 semi-anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. 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. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear DiffeHellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

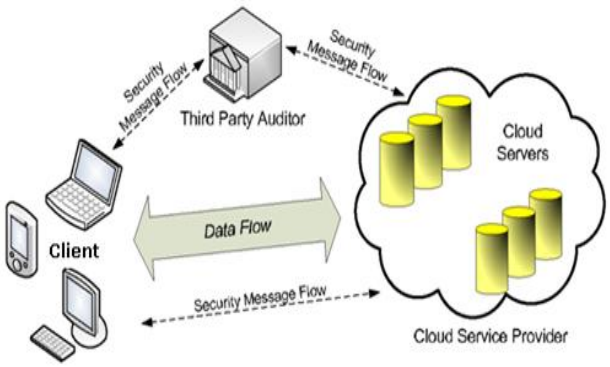

Figure 2 . System Architecture

IV. PROPOSED SYSTEM

In the proposed scheme, an authority Ak generates a set of random secret parameters and shares it with other authorities via secure channel, and xk is computed based on this parameters. It is believed that DDH problem is intractable in the group G0 of prime order p, therefore does not leak any statistical information about . This implies even if an adversary is able to compromise up to (N − 2) authorities, there are still two parameters kept unknown to the adversary. So, the adversary is not able to guess the valid g vk , and he fails to construct a valid secret key. Hence, the scheme achieves compromise tolerance to up to (N − 2) authorities compromise. But, if we reduce the time complexity of the setup phase by dividing authorities into several clusters having C authorities in each, attackers can compromise C − 1 authorities in a cluster to create valid master keys of that cluster. Therefore, there is a trade- off between tolerance and complexity. However, since the number of authorities is typically not very huge, and the setup is one-time operation at the very beginning of the system setup, we recommend using the original setup algorithm whose complexity is O (N 2).

The compromised authorities are able to issue valid attribute keys for which they are in charge of, so the cipher texts whose privilege trees have only those attributes might be illegally decrypted if the attacker issue all possible attribute keys to himself. But, since the authorities are well protected servers, it is hard to compromise even one authority, and the probability of compromising enough authorities to illegally decrypt cipher text is very low. We have defined the problem of minimizing the energy

consumption while meeting QoS requirements and stated the requirements for VM allocation policies. Moreover, we have proposed three stages of continuous optimization of VM placement and presented heuristics for a simplified version of the first stage.

a. Registration -Based Social Authentication

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),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.

b. Security Model

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 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 (i.e., Section VII), 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

C. Attribute-based encryption

Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. the attribute-based encryption have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the cipher text.

1. User revocation

User Revocation In this module, if any user wants to revoked from the cloud, that request for revocation is sends to TPA. After TPA verification that user must be revoked from the cloud. During revocation user details can be deleted from the database but Uploaded files of revoked user is maintained during user revocation.

2. Multi-authority model

A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

V. CONCLUSION

This paper proposes 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. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anon ymity 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.

VI. 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] B. 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] C. Bethencourt, A. Sahai, and B. Waters, " Ciphertext-policy attribute- based encryption," in Proc. IEEE SP , May 2007, pp. 321–334.

[5] C. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography . Berlin, Germany: Springer-Verlag, 2007, pp. 515–534

[6] C. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS , 2009, pp. 121–130.

[7] D.Lin,Z.Cao,X.Liang,andJ.Sha o, "Secure threshold multi authority attribute based encryption w ithout a central authority," Inf. Sci. , vol. 180, no. 13, pp. 2618–2632, 2010.

[8] E. Božovi´ c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with hone st-but-curious central authority," Int. J. Comput. Math. , vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribut e based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE , Mar. 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 Proc. IEEE INFOCOM , Apr. 2013, pp. 2895–2903