

Attribute-Predicated Encryption on Users Data Stored In Cloud

Sowmya Reddy Kambam

PG Scholar

Department of CSE
SVR Engineering College,
Ayyaluru, Nandyal.

M Subba Reddy

Associate Professor
Department of CSE
SVR Engineering College,
Ayyaluru, Nandyal.

Abstract

Cloud computing is the furthestmost topical evolving archetype capable to turn the revelation of “computing utilities” into certainty. Several systems predicated on the attribute-predicated encryption have been projected to secure the cloud storage. Conversely, much work accentuations on the data contents privacy and the access control, while less consideration is compensated to the identity privacy. In this Manage cloud data access opportunity and anonymity with plenary incognito with secure status, a semi incognito privilege control system Anony Control to address not only the data privacy, but withal the utilizer identity privacy in prevailing access control systems are accessible. Anony Control decentralizes the central ascendancy to bound the identity leakage and so procures semi anonymity. Here, the privileges of all processes on the cloud data can be accomplished in a fine-grained manner. Successively, the Anony Control-F, which plenary obviates the identity leakage and achieves the full anonymity, is presented.

Keywords: Anonymity, multi-ascendancy, attribute-predicated encryption

INTRODUCTION

Computing is being transformed to a model consisting of accommodations that are commoditized and distributed in a manner kindred to utilities such as dihydrogen monoxide, electricity, gas, and telephony. In such a model, users access accommodations predicated on their requisites regardless of where the accommodations are hosted. Several computing paradigms have promised to distribute this utility computing vision. Cloud computing is a radical

computing paradigm, that enables on-demand, and low-cost utilization of computing resources, but the data is outsourced to some cloud servers, and sundry privacy concerns emerge from it. An accommodation offering computation resources is frequently referred to as Infrastructure as a Accommodation (IaaS) and the applications as Software as a Accommodation (SaaS)[1]. An environment utilized for construction, deployment, and management of applications is called PaaS (Platform as an Accommodation). Cloud storage has been most popular since last few years. It is utilized as the core technology. Cloud has at least two challenges that must be handled. First is, data confidentiality should be assured. Most of the work fixates on the data content privacy and access control, and there is less fixate on the privilege control, so other users might be able to infer sensitive information. Consequently, not only the data content privacy or access, but additionally the operation should be controlled. The second is, personal information (set of utilizer attribute) is in jeopardy because there is no privacy of the utilizer identity. Nowadays, most people are more concerned about privacy of their identity, so there is a desideratum to forfend identity privacy. In anterior system only concern was regarded data content privacy as Identity-predicated encryption (IBE) [2], Fuzzy Identity-Predicated Encryption [3]. Most work fixate on the data content privacy and access control, and less fixate on the privilege control and the identity privacy. User’s identity with their attributes is revealed to key issuers, and it issue private keys according to their attributes get their private keys. But at present, users are more concerned to keep their identities secret. Ergo, we propose the Anony Control and Anony Control-F [1] with Attribute Predicated Encryption for cloud servers for users to access data

without knowing their identity information. Attribute-Predicated-Encryption is a technique for Encryption data by utilizing attributes and keys. Security is main issue in cloud storage system because data is more sensitive so, anyone hack data so utilized the encryption data with ABE for secure data. Anony Control and Anony Control-F [1] use to provide access privilege with identity auspice.

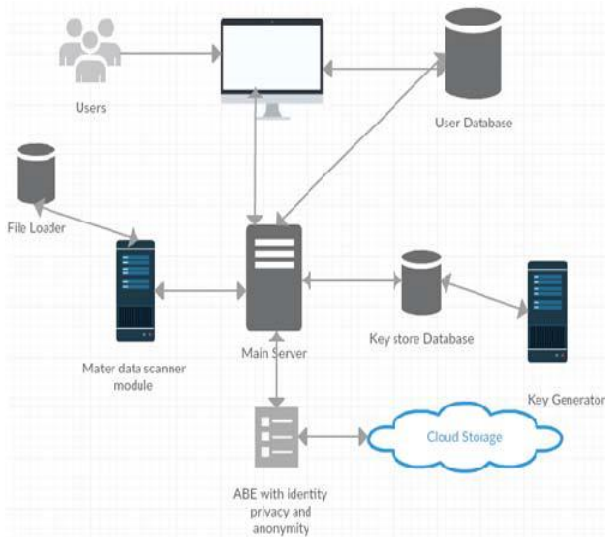


Fig - 1 Overview of proposed system

RELATED WORK

Existing system

We present a semi innominate privilege control scheme AnonyControl to address not only the data privacy, but additionally the utilizer identity privacy in subsisting access control schemes. Besides the fact that we can express arbitrarily general encryption policy, our system additionally abides the compromise attack towards attributes ascendant entities, which is not covered in many subsisting works. We elongate subsisting schemes by generalizing the access tree to a privilege tree. We elongate subsisting schemes by generalizing the access tree to a privilege tree. The key point of the identity information leakage we had in our antecedent scheme as well as every subsisting attribute predicated encryption schemes is that key engenderer issues attribute key predicated on the reported attribute, and the engenderer has to ken the user's attribute to do so.

Propose system

Sundry schemes predicated on the attribute-predicated encryption have been proposed to secure the cloud storage. Various techniques have been proposed to bulwark the data contents privacy via access control. We propose AnonyControl and Anony Control- to sanction cloud servers to control users' access privileges without knowing their identity information. They will follow our proposed protocol in general, but endeavor to ascertain as much information as possible individually. The proposed schemes are able to bulwark user's privacy against each single ascendancy. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. We firstly implement the authentic toolkit of a multiauthority predicated encryption scheme AnonyControl and AnonyControl-F.

IMPLEMENTATION

Registration -Predicated Convivial Authentication Module:

The system prepares trustees for a utilizer Alice in this phase. Concretely, Alice is first authenticated with her main authenticator (i.e., password), and then a few (e.g., 5) friends, who withal have accounts in the system, are culled by either Alice herself or the accommodation provider from Alice's friend list and are appointed as Alice's Registration.

Security Module:

Authentication is essential for securing your account and obviating spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Irate recipients and spam complaints resulting from it become your mess to emaculate, in order to rehabilitate your reputation. trustee-predicated convivial authentication systems ask users to cull their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the accommodation provider can constrain trustee culls via imposing that no users are culled as trustees by an inordinate quantity of other users, which can achieve better security guarantees.

Attribute Ascendant entities:

They are surmised to have potent computation facilities on some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each ascendancy, ergo each ascendancy is vigilant of only part of attributes.

Data Owner: A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers.

Cloud Server: The Cloud Server, who is postulated to have adequate storage capacity, does nothing but store them.

Data Consumers:

All Data Consumers are able to download any of the encrypted data files, but only those whose private keys slake the privilege tree T_p can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree T_p . Incipiently joined Data Consumers request private keys from all of the ascendancy entities, and they do not ken which attributes are controlled by which ascendancy entities. When the Data Consumers request their private keys from the ascendancy entities,

Multi-ascendancy module:

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

CP-ABE Algorithm:

In the CP-ABE, ciphertexts are engendered with an access structure, which designates the encryption policy, and private keys are engendered according to

users' attributes. A utilizer can decrypt the ciphertext if and only if his attributes in the private key slake the access tree designated in the ciphertext. By doing so, the encrypter holds the ultimate ascendancy about the encryption policy. Additionally, the already issued private keys will never be modified unless the whole system reboots.

Privilege Trees T_p :

A data file has several operations executable on itself, and each of them is sanctioned only to sanction users with different caliber of qualifications. For example, {Read_mine, Read_all, Efface, Modify, Engender} is a privileges set of students' grades. Then, reading Alice's grades is sanctioned to her and her edifiers, but all other privileges should be sanctioned only to the edifiers, so we require to grant the "Read_mine" to Alice and all other to the edifiers. Every operation is associated with one privilege p, which is described by a privilege tree T_p . If a user's attributes satiate T_p , he is granted the privilege p. By doing so, we not only control the file access but additionally control other executable operations, which makes the file controlling fine-grained and thus congruous for cloud storage accommodation.

EXPERIMENTAL RESULTS

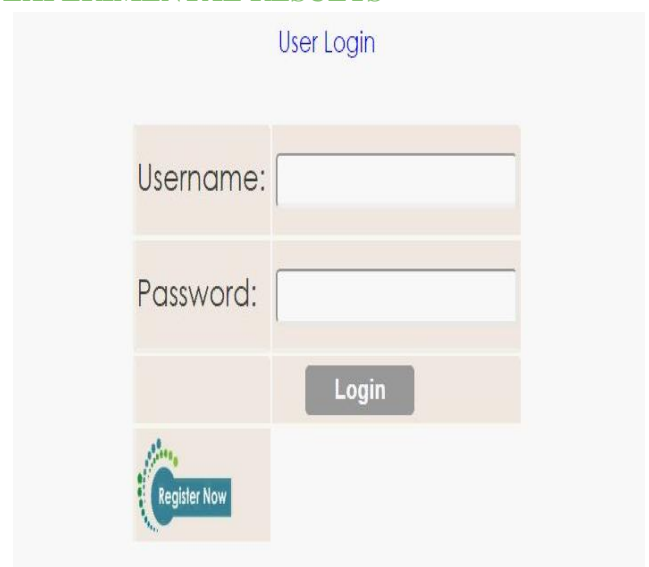


Fig:-2 authentication and authorization



Fig:-3 Data Upload Screen



Fig:-4 Key Generation & CPABE

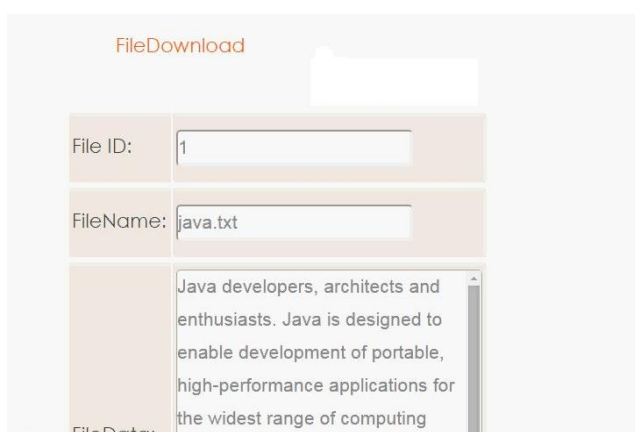


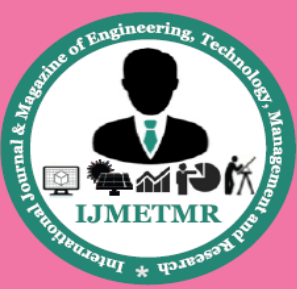
Fig:-5 File Download

CONCLUSION

To bulwark utilizer data privacy is a central question of cloud storage. So, we can develop a Secure and scalable file sharing model on the cloud platform utilizing unique Attribute Predicated Encryption method. The utilizer identity and privacy is much more paramount and we can apportion data among users without revealing utilizer identity. The cloud is very costly. A system must astutely utilize cloud platform while storing data in it. We developed a system where data duplication can be obviated in the cloud. This system can be installed on top of any cloud server by any utilizer. Whenever a company or organization want to utilize cloud storage for their organization uses than they can install our system as a gateway so that the sharing of data will be secure and additionally cloud storage will be optimized. This will preserve cost withal. In current scope, we considered only one cloud for reference. But in future we can amalgamate multiple clouds additionally and utilize them as an optimized and secure storage system.

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



- [6] M. 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] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," *Inf. Sci.*, vol. 180, no. 13, pp. 2618–2632, 2010.
- [8] V. Božović, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-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 attribute 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.<http://www.sourcefordgde.com>