International Journal of Research
Available at
https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Authority Cloud Data Manage and Social Security Using Identity-Based Encryption

Ganipisetty Lakshmi Tirupatamma #1, Y Rajesh Babu #2
# P.G. Scholar in CSE, # Assistant Professor, Department of CSE
Priyadarshini Institute of Technology & Sciences for Women, Chintalpudi, Tenali, Andhra Pradesh, India

Abstract: Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand, and low-cost usage of computing resources, but the data is manage to some cloud servers, and number of privacy concerns emerge from it. New identity based encryption has been proposed to secure the cloud storage and targets the data contents privacy and the access control, while less attention is paid to the privilege control and the identity security. We present a semi anonymous privilege authority scheme to address not only the data privacy, but also the user identity privacy in existing access control schemes also generalizes the new file access control to the privilege authority, which privileges of all operations on the cloud data is managed in a compact structured manner. Subsequently, Anonymity control decentralizes the central authority to bind the identity leakage and so attains semi anonymity. In this model we have proposed an attribute based encryption technique is different from previously encryption techniques. Many of the previously proposed encryption techniques which are used in data sharing scenario have some models like varying size of cipher text, user revocation which are resolved in this model. The privileges of processes on the cloud data is accomplished in a fine-grained manner. Successively the AnonyControl-F is fully prevents the identity leakage and achieves the full anonymity is presented.

Index Terms: Anonymity, Multi-Authority, Attribute-Based Encryption. Cloud Computing, Access Control, Privilege Control, Semi Anonymity, Anonycontrol And Anonycontrol-F Scheme

1. INTRODUCTION

Today development of network is very speed which makes data destitution paradigm easier in services systems such as online social network or cloud computing where every wanted their data to be shared by only indent person which should have some access methods. So, for this purpose attribute based encryption system is provides a way of defining access policies based on different attributes of the requester the data object Attribute Based Encryption (ABE) is a generalization of identity-based cryptosystems which incorporates attributes as inputs to its cryptographic system[1].

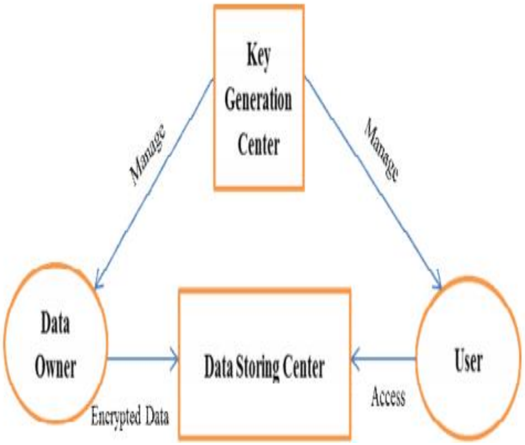

Fig. 1 Data Sharing System

Traditional data services systems are major issue of key escrow problem. Also, many of the existing techniques of attribute based encryption have some model related to security. The decrypt attributes the cipher text. Data owner would like to take their private data only to a indent users. Also applying CP-ABE in data sharing schema is problem of user revocation because the access methods is defined on the basis of attributes universe [2]. Security is consequently an extensive element in any cloud computing locations because it is crucial to security that only authorized access is sanctioned and protected behavior method is access. Any kind of security and services contravention is critical and data crucial results. As soon as the strict regulations and methods is taken against privacy in cloud, many personnel will feel save to new domain in cloud computing. A client may be different a big organization but all are having same concern data security so data security is dire consequence. Data security at many levels is the vital matter of this technology; it can be divided into two categories [3].

The data seclusion is not only about the data contents. Since the most new part of the cloud computing is the outsourcing of computation, it is far beyond enough to just oversee an access control. More likely, users want to control the right of data modify over other users or cloud servers. [4] [5]

2. RELATED WORK

We discuss new access control systems are provide a facility like availing of data to the user even during the fault occurrence situation in the cloud. To take flexibility and fine-grained access control, many access control method is projected a new system called as Attribute-Based Encryption [ABE] projected by Yu [6]. Expressibility lacking is the main disadvantage of ABE system to distributed data user can able to access data if a user posses a certain set of credentials or attributes. Presently the one method for enforcing such methods is to employ a trusted server to store the data and mediate access control. We present model is realizing complex access control on encrypted data to say Cipher text-Policy Attribute-Based Encryption. By using our security encrypted data can be kept confidential even if the storage server is untrusted; [8] Our systems is secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to explain the security data and built policies into user's keys our systems is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). We implementation our system and give performance measurements [7]. Ethencourt, Sahai and Waters [9] came up with a system for cipher text-Policy Attribute Based Encryption is a new type of encrypted access control indent user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. This system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Ostrovsky, Sahai and Waters [10] presented the first Attribute Based Encryption system that supports the expression is formulas in key policies. They achieved this through a many application of revocation system into existing ABE schemes Sun and Liu [11] The proposed scheme has less overhead associated with key management system. Cheung, Cooley, Khazan and Newport [12] proposed a new scheme called group key management scheme which is based on cipher text-policy attribute-based encryption model.

3. CLOUD SERVICE COMPOSITION MODEL

The Architecture is different users in the cloud envelopment and secure server Plus application is mainly double login security. That is, after logging into the application user take a secret key on his registered mail id. This secret key is entered in the pop-up box displayed after logging into SSP Application. This application uses two functionalities, Encryption and Decryption [13]. Encryption is the functionality in which the file and sent over mail in firstly divided into 4 equal levels in byte format and then encrypted using many security algorithms .After Encryption files would be sent to recipient through mail At the recipient end, He will download the files and using SSP Application data in files would be decrypted and combined [14]. Control indent authority is in control of a subset of attributes set and for the attributes that it is in modify of exact information of the key requester. If the information from all authorities is collected totally complete attribute set of the key requester is recovered and thus his identity is disclosed to the authorities [15].

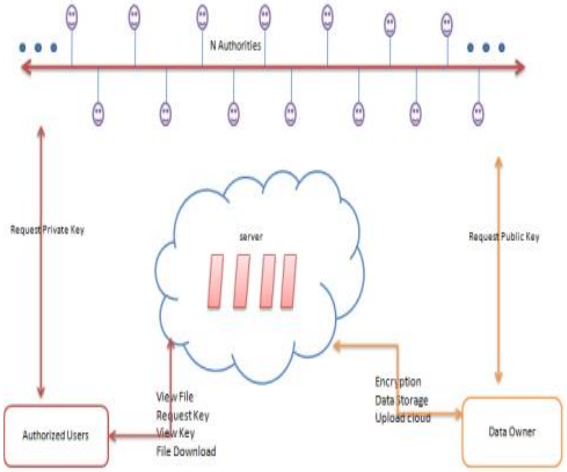

Fig.2. System Architecture

4. METHODOLOGY

Step 1: In this project we are not only providing data content privacy we are also providing identity privacy by using anonycontrol.

- We present the AnonyControl-F, is fully prevents the identity leakage data and full anonymity.

Step 2: In our system Attribute Encryption Standard (AES) model. This algorithm is used to security classified information and is used by the total world to encrypt and decrypt sensitive data.

AES consists of three block ciphers. AES-128, AES-192, AES-256 and every cipher uses 128 bits of blocks using cryptographic keys 128,192 and 256 bits to encrypt and decrypt delicate data. [16].

Step 3: In our system, there are four types of systems: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and Data Consumer simultaneously.

- Data owner security and uploads the files in to the cloud server. Data customers decrypt and downloads the files from the cloud server.

Step 4: To access and perform any operations on files the data owner and data customer should first register in to the system.

- When they registered at a time password and unique id will send to their registered mail id.

Step 5: To upload and download data by the user. The user may be a data owner and data customer request the identify for permission.

- The authority take public key to data owner and private key to customer. Issuing keys by authority and identify in our system is succeeding using attribute based encryption. [1] [15]

Step 6: Attribute-based encryption is new public-key encryption in which the secret key of a user and the cipher text is dependent upon the decryption of a cipher text is modify only if the set of attributes of the user key matches the attributes of the cipher text [17].

Step 7: Using the keys provided by authority the users access the files in to and from the cloud serve

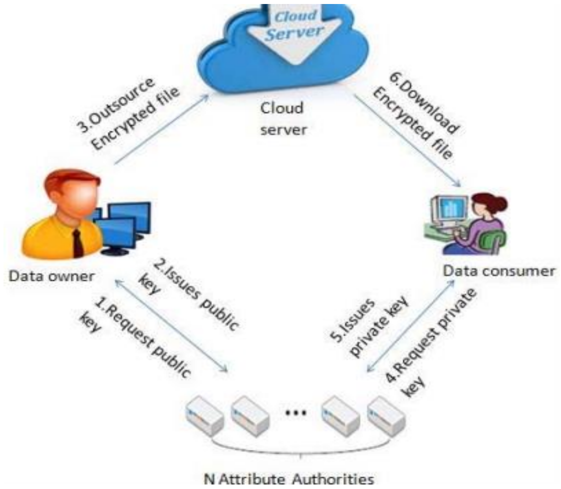

Fig. 3 Architectural Flow

1. Key Generation:

The keys for the RSA algorithm are generated the following way:

1.Take two distinct prime numbers p and q. For portions purposes, the integers p and q should be chosen at random, and should be same in magnitude.

2.Compute n = pq. n is used as the modulus for both the public and private keys. Its size, usually expressed in bits, is the key length [18].

3.Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n − (p + q − 1), where φ is Euler's totient function. This value is kept security.

4.Choose an integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1; i.e., e and φ(n) are customers

5.Determine d as d ≡ e −1 (mod φ(n)); i.e., d is the modular multiplicative inverse of e (modulo φ(n)) This is more clearly stated as: solve for d given d·e ≡ 1 (mod φ(n)) e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 2 16 + 1 = 65,537 much smaller values of e (such as 3) have been shown to be less secure in some settings. e is released as the public key exponent. d is kept as the private key exponent.

5. PERFORMANCE EVALUATION

It presents, here regarding results evaluation based on the assessment about executing prototype system of AnonyControl-F. This is the first implementation of a multi-authority attribute based encryption system. This prototype system offers five command line tools [12].

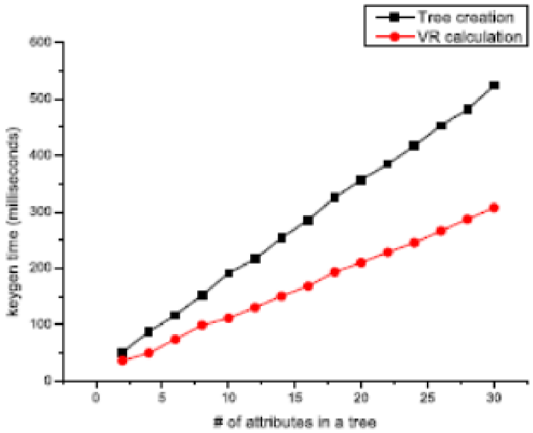

Fig 4 Time to create a privilege tree and decrypt a verification parameter from it

This toolkit is based on the CP-ABE toolkit which is take online and total system is implemented on a Linux system with Intel i7 2nd Gen @ 2.7GHz and 2GB RAM. It is furthermore [17] employed two similar works under the same condition for the comparison purpose. Particularly, it is set only one privilege for the data access, and measured the time to create one security tree and calculate its verification parameter. In general the computation overhead of is much higher system involves number of exponentiations and bilinear mappings in the accountability [15] and [18]. Finally, only run times are plotted because the security creation is the same process in the system

6. CONCLUSION

A semi-anonymous attribute-based security control scheme is Anony Control and a fully anonymous attribute-based privilege control scheme Anony Control-F to address the user security multiple authorities in the cloud computing environment. Our proposed schemes is identity anonymity security control based on users' identity file Our system is consider up to N − 2 authority compromise which is highly security especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis is shows that AnonyControl both secure and efficient for cloud storage system Building the systems well-suited with present ABE systems who sustain resourceful user revocation. Future work we additionally direct the security and execution dections which demonstrates that AnonyControl both secure and proficient for distributed storage framework.

7. FUATURE WORK:

In future implemented model is deployed on cloud and used many companies. For implementation new considered file as document data, text file which can be modify to sound file, video file, image file etc. Also the set of attributes can be increased in order to provide high security to the modern cloud computing system.

REFERENCES

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

[2] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing", IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, 2013

[3] a. Shamir, "identity-based cryptosystems and signature schemes," In advances in cryptology. Berlin, germany: springer-verlag, 1985, Pp. 47–53.

[4] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan," Cipher textPolicy Attribute-Based Encryption", T Jung - 2015.

[5] 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings.

[6] 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

[7] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan," Cipher textPolicy Attribute-Based Encryption", T Jung - 2015.

[8] 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[10]R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures", Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.

[11]Y. Sun and K. Liu, "Scalable hierarchical access control in secure group communications", In Proc. of the IEEE Infocom, Hong Kong, China, March 2004.

[12] L. Cheung, J. Cooley, R. Khazan, and C. Newport, "Collusion-resistant group key management using attribute-based encryption", Cryptology ePrint Archive Report 2007/161, 2007.

[13] j. Li, q. Huang, x. Chen, s. S. Chow, d. S. Wong, and d. Xie, "multiauthority Ciphertext-policy attribute-based encryption with accountability," In proc. 6th asiaccs, 2011, pp. 386–390.

[14] h. Ma, g. Zeng, z. Wang, and j. Xu, "fully secure multi-authority Attribute-based traitor tracing," j. Comput. Inf. Syst., vol. 9, no. 7, Pp. 2793– 2800, 2013.

[15] Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi. "Multi-authority attributes based encryption with honest-butcurious central authority".

[16] S. G. Akl and P. D. Taylor. Cryptographic Solution to a Multi Level Security Problem in Advances in Cryptology -- CRYPTO 1982.

[17] M.R.KAVITHA RANI,M.E, S.BRINDHA, M.E., "A Survey on Data Stored in Clouds" ISSN: 2350-0328 International Journal of Advanced

Research in Science, Engineering and Technology Vol. 2, Issue 11 , Novem

[18] X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attribute based encryption supporting efficient decryption test," in Proc. 8th ASIACCS, 2013, pp. 511–516.

AUTHOR DETAILS

Ganipisetty Lakshmi Tirupatamma born in Chimatavaripalem, Munnigavaripalem, Yaddanapudi, Prakasam Dt, AP. I received B.Tech in CSE from Chintalapudi Engineering College, Chintalapudi,Gunturdt, AP.JNTU Kakinada in the year 2013. Presently Iam pursuing M.TECH in CSE from Priyadarshini Instiiute of Technology& Science for Women, Chintalapudi near Tenali, GunturDt, Andhrapradesh, India .

Y.Rajesh Babu received B.Tech (CSE) Degree from Vignan's Lara Institute of Technology & Science in 2012 and M.Tech (CSE) Degree from Priyadarshini Institute of Technology & Science, Chintalapudi in 2015. He has 4 years of teaching experience. He joined as Assistant Professor in Priyadarshini Institute of Technology & Science for Women, Chintalapudi, Guntur dt, AP. Presently he is working as Assistant Professor in CSE department. He published international journal on Enhanced dynamic secured group sharing using OTP in public cloud. He attended Various National and International Workshops and Conferences on Cloud Computing.