International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 05
April 2017

An Proficient Presentation of Attribute Based EncryptionScheme in CloudComputing

Mrs. D.SRILATHA[1]; K.Dinesh Reddy[2]; B. Vinay Kumar[3]; M. Masthan Reddy[4]& K. Ankitha[5]

[1]Assistant professor,CSE, Mahaveer Institute of Science & Tech., Bandlaguda,Hyderabad,India
[2,3,4,5]B.Tech student,CSE, Mahaveer Institute of Science & Tech., Bandlaguda,Hyderabad,India

ABSTRACT:*Cloud computing is oneof the up-coming technologies used for handling voluminous data and its storage.In this paper, we present a semianonymous privilegecontrol scheme AnonyControl to address not only the dataprivacy, but also the user identity privacy in existing accesscontrol schemes. AnonyControl decentralizes the centralauthority to bound the identity leakage and thus achievessemianonymity. In addition, it also generalizes the file access controlto the privilege control, by which privileges of all operations onthe cloud data can be managed in a fine-grained manner.Consequently, we present the AnonyControl-F, which fullyprevents the identity leakage and achieve the full anonymity.*

KEYWORDS-Anonymity, multi-authority, attribute-basedencryption.

I. INTRODUCTION

Cloud computing is one of important sourcing that enablesorganizations to move from traditional data storage andmaintain within organization boundaries with costeffectiveness. Nowadays most of IT industry/ organizationuses cloud infrastructure widely and provide shared access tonetwork resources and data to users. Cloud implementationhas proved rapid growth as it operates at fast speed andrequires very less maintenance. The cloud service modelprovides services to users as per their requirement. So anyOrganization can select service as their need to meet itsrequirement. Virtualization of hardware and its availabilityreduces dependency and investment on required hardware.Cloud application programming interface (API) allowsdevelopers and users to access cloud services efficiently.Users can connect to cloud services through a web servicesusing web browsers so access to cloud services are notdependent on a particular location and device. Sharing of dataand require resources on cloud computing allows to increaseuser productivity by reducing system response time. As datasecurity is an important aspect of the organization datasharing and deployment model of cloud computing can beeffectively used to increase the complexity level of security.Now days in market cloud computing provide differentservice oriented models have been available, models like 1)IaaS-Infrastructure as a Service, 2) PaaS-Platform as aService, and 3) SaaS-Software as a Service. Many commercialcloud computing systems have been built at different levels,e.g., Amazon's S3 [3], Amazon's EC2 [2], and IBM's BlueCloud [4] are IaaS systems, while Engine Yard[3], GoogleApp Engine [5] and Yahoo Pig are representative PaaSsystems, and Google's Apps [6] and Salesforce's CustomerRelation Management (CRM) System [7] belong to SaaSsystems. With these cloud computing services, the enterpriseusers no longer need to empower in hardware or softwaresystems or hire professionals to maintain these systems, thusthey save cost on IT infrastructure and human resources; andalso different computing utilities provided by cloudcomputing are being provide at a comparatively low price in apay-as-you-use manner[1].

In spite of the fact that the great benefits introduce by cloudcomputing paradigm are exciting for organization, academicresearchers, and widely cloud users, security problems incloud computing become serious barrier which, withoutconsidering, will put a stop to cloud computing largeapplications and usage in the future. One of the importantsecurity concerns is data privacy and data security in cloudcomputing because of its Internet-based data storage andmanagement. In cloud computing, data users have to providedata to the cloud service provider for storage and variousbusiness operations, while the cloud service provider isusually a third party which cannot be totally trusted. Data isvery important property for any organization, and users

willface serious problems if its confidential data is reveal to theircompetitors or the public. Thus, cloud users initially want tomake sure that their data are kept secret and confidential tothe cloud provider and their potential competitors. This is thefirst data security requirement.

II. RELATED WORKS

In cloud computing, the data owner wants to share the data from the cloud in the sense owner encrypt the datathen uploaded into the cloud storage. All the sensitive cloud data's are encrypted to avoid the unauthorized user accessof the cloud data. The different schemes exist that provide security, data confidentiality and access control. Theencryption scheme provides security to the cloud data, and one of the schemes is attribute based encryption scheme. Oneof the encryption schemes is Attribute-Based Encryption (ABE) which is a new paradigm where such policies arespecified and cryptographically enforced in the encryption algorithm itself. The existing ABE schemes are of two types.

They are Key-Policy ABE (KP-ABE) scheme and Cipher text-Policy ABE (CP-ABE) scheme. In KP-ABE scheme,attribute policies are associated with keys and data is associated with attributes. Only the keys associated with the policythat is satisfied by the attributes associating the data can decrypt the data. In CP-ABE schemes, attribute policies areassociated with data and attributes are associated with keys and only those keys that the associated attributes satisfy thepolicy associated with the data are able to decrypt the data.

A. Attribute-based Encryption Scheme

Sahai and Waters proposed an attribute based encryption scheme in 2005. Attribute-based encryption (ABE) isa vision of public key encryption that allows users to Encrypt and decrypt messages based on user attributes. Standardencryption is inefficient when selectively sharing data with many people, since the data needs to be encrypted usingevery User's public key. There are authority, sender and receiver in the ABE scheme, and authority's role is to generatekeys for data sender and users to encrypt or decrypt data. In this scheme, the authority generates keys according toattributes; and these attributes of public key and master key, which are generated by the authority.

All the attributes used in the potential and any data user who wants to add to this system, and owns to attributes don'tinclude pre- defined attributes. The authorities will re-define attributes and generate a public key and master key again.Data sender's to encrypt data with a public key and a set of descriptive attributes. A data receiver to decrypt encrypteddata with private key sent from the authority.
Example: NASA wants to encrypt data.
Attributes :{ Administrator, Manager, Engineer, Astronaut, Apollo, Space Shuttle, ISS, and Mars Rovers}

B. Key Policy Attribute Based Encryption

Key Policy Attribute Based Encryption scheme is a public key cryptography primitive that is for one-to-manycommunications. In this, data are associated with attributes for each of which a public key is defined. The one whoencrypts the data, i.e., the encrypt associates the set of attributes to the data or message by encrypting it with a public key.Users are assigned with an access structure which is defined as an access tree over the data attributes. The nodes that areinterior of the access tree [8].

Key-policy attribute-based encryption (KP-ABE) is an important class of ABE, where cipher texts are labeledwith sets of attributes and private keys are associated with access structures that control which cipher texts a user is ableto decrypt. KP-ABE has important applications in data sharing on un trusted cloud storage. However, the cipher text sizegrows linearly with the number of attributes embedded in cipher text in most existing KP-ABE schemes [12].

In cloud computing, an access control mechanism based on KP-ABE together with a re-encryption technique is used forefficient user revocation. This scheme enables a data owner to reduce most of the computational overhead to cloudservers. The use of this encryption scheme KP-ABE provides fine-grained access control. Each file or message isencrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a setof attributes in KP-ABE, which is generated corresponding to an access structure.The first problem with this scheme is that the encrypted is not able to decide who can decrypt the encrypted dataexcept choosing descriptive attributes for the data, and has no choice but to trust the key issuer. Furthermore, KP-ABE isnot naturally suitable to certain applications.

C. Expressive Key Policy Attribute Based Encryption

This expressive key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic accessstructures (i.e., that may contain negated attributes) and with constant cipher-text size. Towards achieving this goal, showthat a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model. A new efficient identity-based revocation mechanism, when combined with a particular instantiationof our general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-sizecipher texts. The downside of these new constructions is that private keys have quadratic size in the number of attributes.

On the other hand, they reduce the number of pairing evaluations to a constant, which appears to be a unique featureamong expressive KP-ABE schemes.Among the encryption methods in clouds Attribute-based encryption (ABE), allows fine-grained access controlon encrypted data. In the key-policy Attribute based encryption, the primitive enables senders to encrypt messages with aset of attributes and private keys are associated with access tree structure that specifies which all the ciphertexts the keyholder is allowed to decrypt.

III. PROPOSEDAPPROACH

The data confidentiality, less effort is paid to protect users identity privacy during those interactive protocols. Users identities, which are described with their attributes, aregenerally disclosed to key issuers, and the issuers issue privatekeys according to their attributes. We propose AnonyControland AnonyControl-Fallow cloud servers to control users access privileges without knowing their identity information.In this setting, each authority knows only a part of any user'sattributes, which are not enough to figure out the user'sidentity. The scheme proposed by Chase et al. considered thebasic threshold-based KP-ABE. Many attribute basedencryption schemes having multiple authorities have beenproposed afterwards.

In our system, there are four types of entities: N AttributeAuthorities (denoted as A), Cloud Server, Data Owners andData Consumers. A user can be a Data Owner and a DataConsumer simultaneously. Authorities are assumed to havepowerful computation abilities, and they are supervised bygovernment offices because some attributes partially containusers' personally identifiable information. The whole attributeset is divided into N disjoint sets and controlled by eachauthority, therefore each authority is aware of only part ofattributes.

The proposed schemes are able to protect user's privacyagainst each single authority. Partial information is disclosedin AnonyControl and no information is disclosed inAnonyControl-F.

The proposed schemes are tolerant against authoritycompromise, and compromising of up to (N −2) authoritiesdoes not bring the whole system down.We provide detailed analysis on security and performance toshow feasibility of the scheme AnonyControl andAnonyControl-F.We firstly implement the real toolkit of a multi authority basedencryption scheme AnonyControl and AnonyControl-F.

Registration Based Social Authentication Module

The system prepares trustees for a user Alice in this phase.Specifically, Alice is first authenticated with her mainauthenticator (i.e., password),and then a few(e.g., 5) friends,who also have accounts in the system, are selected by eitherAlice herself or the service provider from Alice's friend listand are appointed as Alice's Registration.

Security Module

Authentication is essential for securing your account andpreventing spoofed messages from damaging our onlinereputation. Imagine a phishing email being sent from ourmail because someone had forged your information. Angryrecipients and spam complaints resulting from it become ourmess to clean up, in order to repair your reputation. trustee-based social authentication systems ask users to select theirown trustees without any constraint. We show that the service provider can constraintrustee selections via imposing that no users are selected astrustees by too many other users, which can achieve bettersecurity guarantees.

Attribute based encryption

Attribute-based encryption module is using for each and everynode encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain

concept usinguser data uploaded. the attribute-based encryption have beenproposed to secure the cloud storage. Attribute-BasedEncryption (ABE). In such encryption scheme, an identity isviewed as a set of descriptive attributes, and decryption ispossible if a decrypter's identity has some overlaps with theone specified in the ciphertext.

Multi-authority

A multi-authority system is presented in which each user hasan 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' identityinformation; and tolerates compromise attacks on theauthorities or the collusion attacks by the authorities. This isthe first implementation of a multi-authority attribute basedencryption scheme.

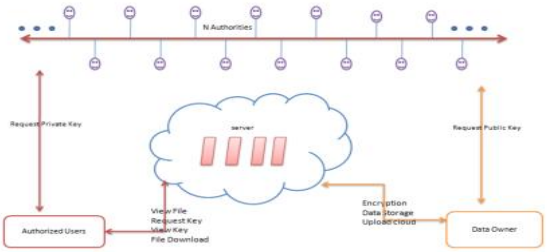

Fig.1. System Architecture

The Architecture encompasses bee agents and their interactionstructure.

a) Employee forager bee agent
b) Scout andonlooker bee agent.
c) Hive - Resource agent.

There are avariety of users in the cloud platform. The cloud users mustdefine their budgetary requirements based on technical andfunctional considerations.

IV. CONCLUSION

Using several authorities in the cloudcomputing system, our suggestedoutlines achieve not onlyfine-grained privilege control but also identity anonymitywhile conducting privilege control based on users' identityinformation. Additionalprominently, our system can bear up toN−2 authority compromise, which is highly desirableparticularly in Internet-based cloud computing environment. Wealso conducted comprehensive security and performance analysiswhich shows that AnonyControl both secure and efficient forcloud storage system.

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE:A Hierarchical Attribute-Based Solution for Flexible andScalable Access Control in Cloud Computing", in IEEETransactions on information forensics and security, Vol.7, No. 2, in April 2012.

[2] Schucheng Yu, Cong Wang, KuiRen, and WenjingLou," Achieving secure, scalable, and fine-grained dataaccess control in cloud computing," in Proc IEEEINFOCOM,2010.

[3] A.Sahai and B.Waters,"Fuzzy Identity BasedEncryption," In Proc. Advances in Cryptology-Eurocrypt,2005, vol.3494,pp.457-473.

[4] S.Muller, S.Katzenbeisser, and C.Eckert," Distributedattribute-based encryption,"in Proc.11th Int.Conf.Information Security and Cryptology,2008,pp.20-36, Springer.

[5] J.Hur and Dong Kun Noh," Attribute-Based Control withEfficient Revocation in Data Outsourcing systems,"IEEE Transactions on Parallel and DistributedSystems,Vol.22, No.7,July 2011.

[6] V.Goyal, O.Pandey, A.Sahai and B.Waters,"Attribute-based encryption for fine-grained acesscontrol of encrypted data," in Proc.ACMConf.Computer and Communications(ACM CCS),Alexandria,VA,2006.

[7] J.Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute based encryption," in Proc.IEEE Symp.Security and Privacy, Oakland, CA,2007.30.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-based encryption for fine-grained access control ofencrypted data," in Proceedings of the 13 th ACM conference on Computer and communications security, pp. 89-98, 2006.

[9] R.Ostrovsky, A.Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," inprocceding of the 14 th ACM Conference on computer and communications security, pp.195-203, 2007.

[10] B.Waters,"Ciphertext-Policy attribute-based encryption" An expressive, efficient, and provably securerealization," public key cryptography V PKC, vol 6571 of LNCS, pp.53-70, 2011.

[11] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute based encryption," IEEE Symp.Securityand Privacy, Oakland, CA, 2007.

[12] Chang-Ji Wang, Sun Yat-sen, Jian-FaLuo,"A Key-policy Attribute-based Encryption Scheme with ConstantSize Ciphertext",IEEE Computational Intelligence and Security, pp 447-451, 2012.

Authors:

Mrs D.SRILATHA Completed Master of Technology in Computer Science and Engineering from Mahaveer institute of science&Technology . Currently working as an Assistant Professor at **Mahaveer Institute of science & Technology, Bandlaguda,Hyderabad**

K.Dinesh Reddy pursing B.Tech in Computer Science Engineering from **Mahaveer Institute of science & Tech, Bandlaguda,Hyderabad**

B. Vinay Kumar pursuing B. Tech in Computer Science Engineering from **Mahaveer Institute of science & Tech, Bandlaguda,Hyderabad**

M. Masthan Reddy pursuing B. Tech in Computer Science Engineering from **Mahaveer Institute of science & Tech, Bandlaguda,Hyderabad**

K. Ankitha pursuing B. Tech in Computer Science Engineering from **Mahaveer Institute of science & Tech, Bandlaguda,Hyderabad**