ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing

Ch.Ramesh Kumar
Associate Professor & HOD,
Department of CSE,
Malla Reddy Engineering College & Management Sciences,
Kistapur, Medchal, Hyderabad.

K.Saddam Hussain
M.Tech Student,
Department of CSE,
Malla Reddy Engineering College & Management Sciences,
Kistapur, Medchal, Hyderabad.

Abstract:
In this Project, we show how Circuit Cipher text policy schema based extends the User Revocation schema with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing. Third, we formally prove the security of the proposed scheme based on the security Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet.

As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.

Index Term:
Cloud Computing, ABE, CP-ABE, KP-ABE, CIA, IBE, Cloud storage.

1. INTRODUCTION:

Cloud computing is novel processing system that is based on virtualization, parallel and distributed computing, utility processing, and service oriented architecture. In the past decades, distributed computing has developed as a standout amongst the most compelling ideal models in the IT business, and has pulled in broad consideration from both the academia and industry. Nonetheless, the individual client prerequisites might be differing and require diverse types of outsourced calculation, while current PVC plans support only a single structure. Customers might wish to demand estimations from a specific server or to issue a solicitation to a huge pool of servers.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The access policy is totally in view of authorization relationship where the relationship is between user attributes and asset properties. The properties might be any data of the client's profession, work parts that is given and is utilized to concede the access. However, all together to outline an access strategy component there are numerous difficulties to conquer some of them are

(1) User can transfer any sort of information such as content, media etc.
(2) Any can give any number of attributes and thus two or more clients might have same characteristics.
(3) Any individual might fabulous any sort of access to any number of clients.

This methodology permits the client to actualize the access control on their information specifically in content sharing service instead of central administrator. To give an intricate access policy component, we require adaptable and versatile cryptographic key administration estimations. For enhancing these disservices, we are utilizing attribute based encryption. Subsequently, we employed CP-ABE (Cipher Text Policy schema – Attribute Based Encryption) method as a solution for the aforementioned problem. In CP-ABE, the beneficiary can unscramble the information just when the client attribute fulfill the access policy.

2. Aim

a) To avoid User identity revealed.
b) To avoid Access Control is not distributed giving rise to single point of failure
c) Increased complexity because policies are embedded in user's key.

3. LITERATURE SURVEY

3. 1) Above the Clouds: A Berkeley View of Cloud Computing

Provided certain obstacles are overcome, we believe Cloud Computing has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new interactive Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get their results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. The economies of scale of very large-scale datacenters combined with ``pay-as-you-go" resource usage has heralded the rise of Cloud Computing.

It is now attractive to deploy an innovative new Internet service on a third party's Internet Datacenter rather than your own infrastructure, and to gracefully scale its resources as it grows or declines in popularity and revenue. Expanding and shrinking daily in response to normal diurnal patterns could lower costs even further. Cloud Computing transfers the risks of over-provisioning or under-provisioning to the Cloud Computing provider, who mitigates that risk by statistical multiplexing over a much larger set of users and who offers relatively low prices due better utilization and from the economy of purchasing at a larger scale. We define terms, present an economic model that quantifies the key buy vs. pay-as-you-go decision, offer a spectrum to classify Cloud Computing providers, and give our view of the top 10 obstacles and opportunities to the growth of Cloud Computing.

3.2) Outsourcing the Decryption of ABE Cipher-texts

Attribute-based encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attributes.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For example, a user can create a cipher-text that can be decrypted only by other users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for many cloud storage and computing applications. However, one of the main efficiency drawbacks of ABE is that the size of the cipher-text and the time required to decrypt it grows with the complexity of the access formula.

In this work, we propose a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE cipher-texts are stored in the cloud. We show how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE cipher-text satisfied by that user's attributes into a (constant-size) El Gamal-style cipher-text, without the cloud being able to read any part of the user's messages.

To precisely define and demonstrate the advantages of this approach, we provide new security definitions for both CPA and replayable CCA security with outsourcing, several new constructions, an implementation of our algorithms and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

3.3) Attribute-Based Encryption with Verifiable Outsourced Decryption

Attribute-based encryption (ABE) is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher-texts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy.

Recently, Green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher-text satisfied by that user's attributes or access policy into a simple cipher-text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher-text. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. In this paper, we consider a new requirement of ABE with outsourced decryption: verifiability.

Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users.

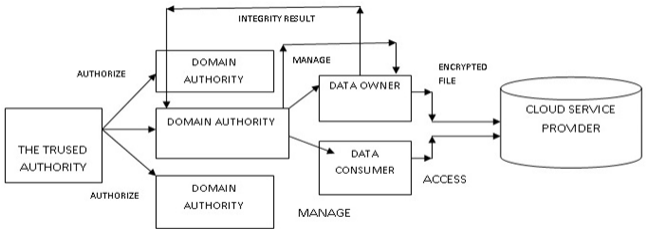
3.4) Decentralizing Attribute-Based Encryption

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing our system, our largest technical hurdle is to make it collusion resistant.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge cipher-text and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of composite order. We prove security under similar static assumptions to the LW paper in the random oracle model.

4. SYSTEM ARCHITECTURE



5. IMPLEMENTATION

a) Attribute Authority Authorities will need to give the key, according to the client's key solicitation. Each client's solicitation must be raised to authority to get access key via mail. There are two correlative types of trait based encryption. One is key policy- attribute based encryption (KP-ABE) and the other is Cipher-text-Policy Schema based Attribute Encryption (CPSBAE). In a KP-ABE framework, the decision of access arrangement is made by the key merchant rather than the en-cipher, which constrains the practicability and ease of use for the framework in the practical applications. If the decryption is incorrect then that account will be blocked.

The blocked account will get the access if the authority decide to give access to the particular account.

b) Cloud Server Cloud server will have access to the file which is transferred by the data proprietor. Cloud server needs to unscramble the documents accessible under their consent. Moreover, information user will need to unscramble the information to get to the first content by giving the particular key. File has been decoded effectively and accommodated for consumer. This process is done only after the cloud is login.

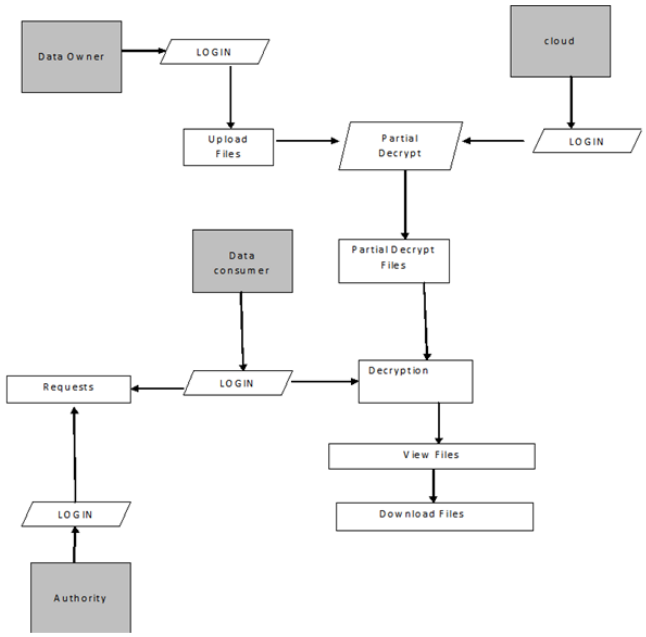


Fig:- Data flow in cloud

c) Data Owner: Information proprietor will need to enroll at first to access the profile. Information Owner will transfer the document to the cloud server in the scrambled arrangement Arbitrary encryption key era is going on while transferring the file to the cloud Scrambled record will be put away on the cloud . To upload the particular file owner should be login.

d) Data Consumer: Information consumer will at first request the key to the Authority to confirm and decode the file in the cloud. Information customer can get to the file in view of the key obtained from mail id. According to the key obtained to the consumer can check and unscramble the information from the cloud.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

To do this process the consumer should register in the cloud . To access the particular file consumer must be login.

6. Circuit Cipher text Based Schema

The schema is as follows:

6.1 Setup (1λ):

It takes as input the security parameter 1λ and outputs the system master key MK and public parameters PK. ver is initialized. Enc (M, AS, PK): It takes as input a message M, an access structure AS, and current public parameters PK, and outputs Cipher-text CT.

6.2 KeyGen (MK, S):

It takes as input current system master key MK and a set of attributes S that describes the key. It outputs a user secret key SK in the form of (ver, S, D, D^{-} = {Di , Fi} i∈S).

6.3 ReKeyGen (γ, MK):

It takes as input an attribute set γ that includes attributes for update, and current master key MK. It outputs the new master key MK′, the new public key PK′ (computation of PK′ can be delegated to proxy servers), and a set of proxy re-key's rk for all the attributes in the attribute universe U. ver is increased by 1. Note that, for attributes in set U −γ, their proxy re-key are set as 1 in rk.

6.4 ReEnc(CT, rk , β):

It takes as input a cipher-text CT, the set of proxy re-key's rk having the same version with CT, a set of attributes β which includes all the attributes in CT's access structure with proxy re-key not being 1 in rk. It outputs a re-encrypted cipher-text CT′ with the same access structure as CT.

6.5 ReKey (D, rk , θ $^{-}$):

It takes as input the component D^{-} of a user secret key SK, the set of proxy re-key's rk having the same version with SK, and a set of attributes θ which includes all the attributes in SK with proxy re-key not being 1 in rk. It outputs updated user secret key components D^{-}′. Dec (CT, PK, SK): It takes as input a cipher-text CT, public parameters PK, and the user secret key SK having the same version with CT. It outputs the message M if the attribute set of SK satisfies the cipher-text access structure.

7. CONCLUSION:

In this paper, we addressed an important issue of attribute revocation for attribute based systems. In particular, semi-trustable proxy servers are available, and proposed a scheme supporting user's attribute revocation schema. A unique property of our proposed scheme is that it places minimal load on authority upon the events in user's revocation. We achieved this by uniquely combining the proxy re-encryption technique with CPSBAE and enabled the authority to delegate most laborious tasks to proxy servers. Our proposed scheme is provably secure against chosen cipher-text attacks. In addition, we also showed the applicability of our method to the KP-ABE scheme. An experimental design shows the effectiveness and efficiency of our proposed work.

8. REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," University of California, Berkeley, Technical Report, no. UCB/EECS-2009-28, 2009.

[2] M. Green, S. Hohenberger and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[3] J. Lai, R. H. Deng, C. Guan and J. Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption," in Proc. IEEE Transactions on information forensics and security, vol. 8, NO. 8, pp.1343-1354, 2013.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[4] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[5] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: an Expressive, Enficient, and Provably Secure Realization," in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[6] B. Parno, M. Raykova and V. Vaikuntanathan, "How to Delegate and Verify in Public: verifiable computation from attribute-based encryption," in Proc. TCC, pp.422-439, Springer-Verlag Berlin, Heidelberg, 2012.

[7] S. Yamada, N. Attrapadung and B. Santoso, "Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication," in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.

[8] J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai and B. Waters, "Attribute-Based Encryption for Circuits from Multilinear Maps," in Proc. CRYPTO, pp.479- 499, Springer-Verlag Berlin, Heidelberg, 2013.

[10] S. Gorbunov, V. Vaikuntanathan and H. Wee, "Attribute-Based Encryption for Circuits," in Proc. STOC, pp.545-554, ACM New York, NY, USA, 2013.

[11] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption," in Proc. EUROCRYPT, pp.457-473, Springer-Verlag Berlin, Heidelberg, 2005.

[12] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. CCS, pp.89-98, ACM New York, NY, USA, 2006.

[13] R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack," in Proc. CRYPTO, pp.13-25, Springer-Verlag Berlin, Heidelberg, 1998.

[14] R. Cramer and V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack," in Proc. SIAM Journal on Computing, vol. 33, NO. 1, pp.167-226, 2004.

[15] D. Hofheinz and E. Kiltz R, "Secure hybrid encryption from weakened key encapsulation," in Proc. CRYPTO, pp.553-571, Springer-Verlag Berlin, Heidelberg, 2007.

Authors Biography

Ch. Ramesh Kumar, working as Assoc. Prof & Head of the Department of Computer Science and Engineering in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA. India. he has several international publications to his credit. His research interests include Software reuse, Software performance, Software testing ,Data Mining and cloud computing

K.Saddam Hussain, completed his B.E in Muffakham Jah college of engineering and technology, 2014. He is pursuing M.Tech. in Computer Science & Engineering from Department of Computer Science & Engineering in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India.. His research interest include cloud, data mining, big data, wireless , knowledge & data engineering and networking.