IISRC International Conference on Industrial Scientific Research Engineering
International Industrial Scientific Research Corporation
www.worldconferences.org

Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

MD. SAMEERA[1], M. HYMAVATHI[2]
[1]PG Scholar, Dept of CSE, QCET, Nellore, AP, India.
[2]Associate Professor, Dept of CSE, QCET, Nellore, AP, India.

Abstract: In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under the *k*-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

Keywords: Attribute-Based Encryption (ABE), CPA, CCA, CP-ABE and KP-ABE.

I. INTRODUCTION

Circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, Combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control And the correctness of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves Security against chosen-plaintext attacks under the k-multilinear Decisional Diffie Hellman assumption. Moreover, an extensive Simulation campaign confirms the feasibility and efficiency of the proposed solution. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional super-computing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

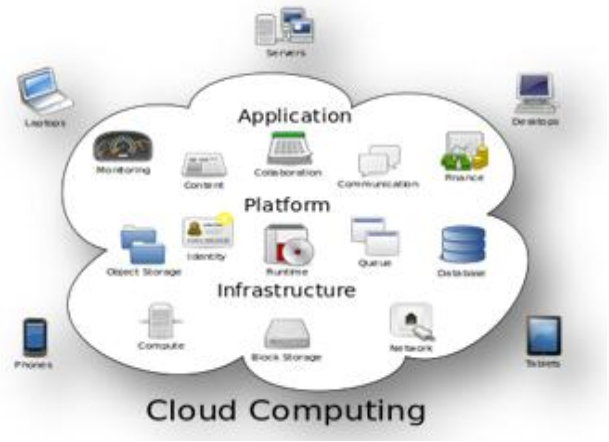

Fig.1. Structure of cloud computing.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them as shown in Fig1. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

II. LITERATURE SURVEY

A. Above the Clouds: A Berkeley View of Cloud Computing

AUTHORS: 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

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.

B. Outsourcing the Decryption of ABE Cipher Texts
AUTHORS: M. Green, S. Hohenberger and B. Waters

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

C.Attribute-Based Encryptionwith Verifiable Outsourced Decryption
AUTHORS: J. Lai, R. H. Deng, C. Guan and J. Weng

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 entrusted 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 ciphertext. 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.

D. Decentralizing Attribute-Based Encryption
AUTHORS: A. Lewko and B. Waters

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. 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.

III. EXISTING SYSTEM

The servers could be used to handle and calculate numerous data according to the user's demands. As applications move to cloud computing platforms, cipher text-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. The increasing volumes of medical images and medical records, the healthcare organizations put a large amount of data in the cloud for reducing data storage costs and supporting medical cooperation. There are two complementary forms of attribute based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is cipher text-policy attribute-based encryption (CPABE).

Disadvantages of Existing System:

- The cloud server might tamper or replace the data owner's original cipher text for malicious attacks, and then respond a false transformed cipher text.
- The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed cipher text to an unauthorized user, he could cheat an authorized one that he/she is not eligible.

IV. PROPOSED SYSTEM

We firstly present a circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. The proposed scheme is proven to be secured based on k-multilinear DecisionalDiffie-Hellman assumption. On the other hand, we implement our scheme over the integers. During the delegation computing, a user could validate whether the cloud server responds a correct transformed cipher text to help him/her decrypt the cipher text immediately and correctly.

Advantages of Proposed System:

- The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.
- They seek to guarantee the correctness of the original cipher text by using a commitment.
- We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CPABE is conceptually closer to the traditional access control methods.

V. ALGORITHM

- **Init:** The VD-CPABE algorithm adversary submits the challenge access structure $f*$ and two equallength messages M0 and M1.
- **Setup:** The simulator runs the Setup algorithm and gives the public parameters PK to the adversary.
- **KeyGen Queries I:** The adversary makes repeated private key queries corresponding to the sets of attributes x1, ..., xq1 . We require that $\forall i \in q1$ we have $f*(xi) = 0$.
- **Encrypt:** The simulator encrypts K0 under the structure $f*$ by using the KEM algorithm. Then
- the simulator flips a random coin v and encrypts Mv under the symmetric key K0 by using the AE algorithm. Then the total ciphertext is given to the VD-CPABE algorithm adversary.
- **KeyGen Queries II:** The adversary makes repeated private key queries corresponding to the sets of attributes xq1 , ..., xq where $f*(x) = 0$.
- **Guess:** The adversary outputs a guess v′ of v. We define the advantage of an adversary A in this game is $Pr[v' = v] - 12$. We'll show that if a KEM scheme is IND-CPA secure and an AE scheme is IND-CCA secure then our hybrid encryption scheme is IND-CPA secure

VI. MODULES

- Attribute Authority
- Cloud Server
- Data owner
- Data Consumer

A. Attribute Authority

Authority will have to provide the key, as per the user's key request. Every users request will have to be raised to authority to get access key on mail. There are two complementary forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is cipher text-policy attribute-based encryption (CPABE). In a KP-ABE system, the decision of access policy is made by the key distributor instead of the enciphered, which limits the practicability and usability for the system in practical applications.

B. Cloud Server

- Cloud server will have the access to files which are uploaded by the data owner
- Cloud server needs to decrypt the files available under their permission.
- Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer.

C. Data Owner

Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud

server in the encrypted format. Random encryption key generation is happening while uploading the file to the cloud. Encrypted file will be stored on the cloud.

D. Data Consumer

Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.

VII. SCREEN SHOTS

Screen shots of this paper is as shown in bellow Figs.2 and 3.

A. Home Page

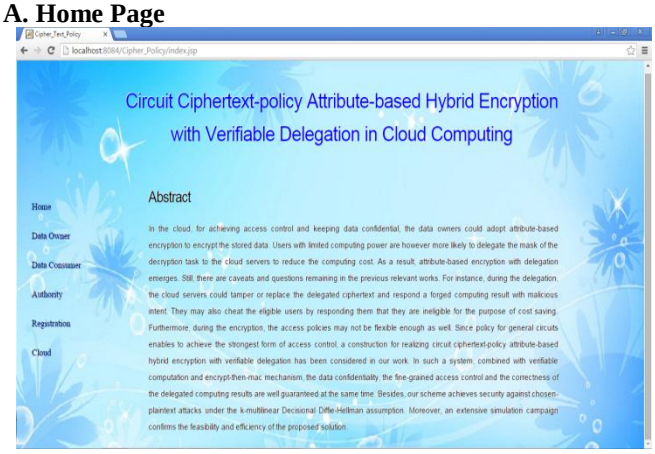

Fig.2.

B. Data Owner Registration

Fig.3.

VII. CONCLUSION AND FEATURE WORK:

To the best of our knowledge, we firstly present a circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secure based on k-multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud. In feature we concentrate to provide data confidentiality factor big data with cloud computing. Through this approach we can reduce cost factor in all aspects and improve the fine grained access multiple data centers.

VIII. 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.

[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.
[16] M. Abe, R. Gennaro and K. Kurosawa, "Tag-KEM/DEM:A New Framework for Hybrid Encryption," in Proc. CRYPTO, pp.97-130, Springer-Verlag New York, NJ, USA, 2008.
[17] K. Kurosawa and Y. Desmedt, "A New Paradigm of Hybrid Encryption Scheme," in Proc. CRYPTO, pp.426-442, Springer-Verlag Berlin, Heidelberg, 2004.
[18] J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, "Securely Outsourcing Attribute-based Encryption with Checkability," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2013.
[19] J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2011.
[20] T. Granlund and the GMP development team, "GNU MP: The GNU Multiple Precision Arithmetic Library, 5.1.1," 2013, http://gmplib.org/.