International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Data Sharing With Efficient Cloud Storage

P. Danusha Chowdary[1], R. Pranutha[2], M. Sharmilla[3], Dr. S. Padma Priya[4]
(Professor), Computer Science and Engineering, Prathyusha Engineering College, Tiruvallur

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 We propose key-aggregate cryptosystem (KAC), a special type of public-key encryption. In KAC, users encrypt files not only under a public key and also with private key. In this we explain how to compress secret keys in public-key cryptosystem which supports delegation of secret keys for different cipher text classes in cloud storage.Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.Here the aggregate key is of constant size. 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.
Keywords—smart grid, big data, TDEA, map-reduce algorithm, identity based encryption.

I. INTRODUCTION

The emergence of cloud computing brings a revolutionary innovation to the management of the data resources. Within this computing environments, the cloud servers can offer various data services, such as remote data storage and outsourced delegation computation , etc. For data storage, the
servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's demands. As applications move to cloud computing platforms, ciphertext-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. Taking medical data sharing as an example (see Fig.1), with 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. Since the cloud server may not be credible, the file cryptographic storage is an effective method to prevent private data from being stolen or tampered. In the meantime, they may need to share data with the person who satisfies some requirements. The requirements, i.e, access policy, could be {Medical Association Membership ∧ (Attending Doctor ∨ Chief Doctor) ∧ Orthopedics}. To make such data sharing be
achievable, attribute-based encryption is applicable. Fig. 1. Medical data sharing system There are two complementary forms of attribute based encryption. One is key-policy attribute-based encryption (KP-ABE), and the other is ciphertext-policy attribute-based encryption (CPABE). In a KP-ABE system, the decision of access policy is made by the key distributor instead of the encipherer, which limits the practicability and usability for the system in practical applications. On the contrary, in a CP-ABE system, each ciphertext is associated with an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if the key's attribute set satisfies the access structure associated with a ciphertext. Apparently, this system is conceptually closer to traditional access control methods. On the other hand, in a ABE system, the access policy for general circuits could be regarded as the strongest form of the policy expression that circuits can express any program of fixed running time. Delegation computing is another main service provided by the cloud servers. In the above scenario, the healthcare organizations store data files in the cloud by using CP-ABE under certain access policies. The users, who want to access the data files, choose not to handle the complex process of decryption locally due to limited resources. Instead, they are most likely
to outsource part of the decryption process to the cloud server. While the untrusted cloud servers who can translate the original ciphertext into a simple one could learn nothing about the plaintext from the delegation. The work of delegation is promising but inevitably suffers from two problems.

The cloud server might tamper or replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext.

The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorized one that he/she is not eligible.

Further, during the deployments of the storage and delegation services, the main requirements of this research are presented as

follows.

A. Confidentiality

In distinguish ability under selective chosen plaintext attacks (IND-CPA)). With the storage service provided by the cloud server, the outsourced data should not be leaked even if malware or hackers infiltrate the server. Besides, the unauthorized users without enough attributes to satisfy the access policy could not access the plaintext of the data. Furthermore, the unauthorized access from the untrusted server who obtains an extra transformation key should be prevented.

B. Verifiability

During the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly. Namely, the cloud server could not respond a false transformed ciphertext or cheat the authorized user that he/she is unauthorized. Thus, in this paper, we will attempt to refine the definition of CP-ABE with verifiable delegation in the cloud to consider the data confidentiality, the finegrained data access control and the verifiability of the delegation. The related security definition and INDCPA security game used in the proof are presented in
section 3.2 to depict the above attacks of the adversaries.

II. CLOUD COMPUTING

Cloud computing is a technology to access the resources available in the servers through Internet. Cloud computing technology becomes popular in the recent years due to its several advantages over traditional methods, like flexibility, scalability, agility, elasticity, energy efficiency, transparency, and cost saving. Cloud resources are shared resources which can be accessed by any one, anytime and anywhere. It is accessible through any devices like mobile, desktops, laptops, tablets etc... The resources and information are provided for the users based on on-demand services. It allows the users to pay only for the resources and workloads they use. Cloud is nothing but a server and a number of servers interconnected through it. Cloud providers are the one who own large data centers with massive computation and storage capacities. They sell these capacities on-demand to the cloud users who can be software, service, or content providers for the users over the internet. In the recent years the major cloud providers are Google, Microsoft, and Amazon etc...

III. OBJECTIVE

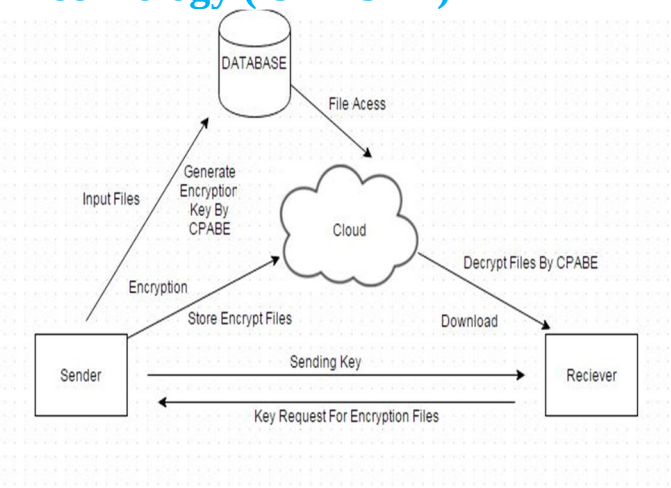
To design an application that use cloud space efficiently, with secure sharing of data by authenticating only valid user to read encrypted file using aggregate key which of very small size.

A. Existing System

Data sharing is an important functionality in cloud storage. For example, bloggers can let their friends view a subset of their private pictures; an enterprise may grant her employees access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others forsharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly. However, finding an efficient and secure way to share partial data in cloud storage is not trivial. In a shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Data in a target VM could be stolen by instantiating another VM coresident with the target one. A cryptographic solution, for example, with proven security relied on number-theoretic assumptions is more desirable.

B. Proposed System

We propose key-aggregate cryptosystem (KAC), a special type of public-key encryption. In KAC, users encrypt files not only under a public-key and also with private key. We proposed how to “compress” secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.



System Architecture for Secure Data Sharing With Efficient Cloud Storage

IV. SYSTEM DESIGN

A. System Architecture

The overall system architecture depicts the functionalities carried out in the Application. The architecture of the online portal consists of users like administrator, physician, insurance company and pharmacist. It depicts that files uploaded by the user are encrypted and stored in database and during the retrieval of files the application authenticates before displaying the information. The key has to be given by the user to read the encrypted file.

V. SYSTEM IMPLEMENTATION

A. Authentication and File Encryption.

In this module the User has to enter the details for registration then he/she can access the database.After registration the user can login to the site.

The authentication and authorization process facilitates the system to protect itself and besides it protects the whole mechanism from the unauthorized user. Here registration of user involves username, email id ,password.

B. File Encryption and Data Storing

After user login, the user can upload the files to the cloud.The uploaded files are encrypted using circuit cipher text-policy attribute based hybrid encryption algorithm. The keys are generated. Then the encrypted files are stored in cloud.

C. Cloud data sharing

The original user initially upload's files data to the cloud, and shares it with other users. The shared files are encrypted by the owner. So whenever the other user's want to access or decrypt the file required keys permission to be accessed.

D. File Decryption

The other user first send key requests to the original user. The aggregate keys are sent in mail to other user by the original user. The file will be decrypted by the aggregate key's which was generated. Finally, any user with an aggregate key can decrypt any cipher text provided that the cipher text's class is contained in the aggregate key via Decrypt.

VI. CONCLUSION

To the best of our knowledge, we firstly present a circuit ciphertext-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 ciphertextpolicy 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.

VII. FUTURE ENHANCEMENT

A limitation in our work is the predefined bound of the number of maximum ciphertext classes. In cloud storage, the number of ciphertexts usually grows rapidly. So we have to reserve enough ciphertext classes for the future extension. Otherwise, we need to expand the public-key as we described in Section. Although the parameter can be downloaded with ciphertexts, it would be better if its size is independent of the maximum number of ciphertext classes. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

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.