ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Key Aggregate Cryptosystem for Scalabledata Sharing in Cloud Storage

[I]A.Yughahara Rao, [II]D.Sandeep, [III]M.Bharat, [IV]B.Harika, [V]D.Phaneendra Pavan Kumar
[I]Associate Professor, [II,III,IV,V]Students
[I,II,III,IV,V]Dept. of CSE, Lendi Institute of Engg. and Tech., Vizianagaram, A.P, India.

Abstract
Data sharing is an important functionality in cloud storage. In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled

Keywords
Cloud service providers, public-key cryptosystems, compact aggregate key, first public-key patient.

I. Introduction

Cloud computing has evolved through a number of phases which include grid and utility computing, Application Service Provision (ASP), and Software as a Service (SaaS).But the overarching concept of delivering computing resources through a global network is rooted in the sixties. Since the sixties, cloud computing has developed along a number of lines, with Web 2.0 being the most recent evolution. However, since the internet only started to offer significant bandwidth in the nineties, cloud computing for the masses has been something of a late developer.

Other key factors that have enabled cloud computing to evolve include the maturing of virtualization technology, the development of universal high-speed bandwidth, and universal software interoperability standards, said UK cloud computing pioneer Jamie Turner.

A new way for public-key encryption is used called as key aggregate cryptosystem (KAC)[1]. The encryption is done through an identifier of Cipher text known as class, with public key. The classes are formed by classifying the cipher text. The key owner has the master secret key which is helpful for extracting secret key. So in above scenario now the Alice can send a aggregate key to bob through a email and the encrypted data is downloaded from drop box through the aggregate key.

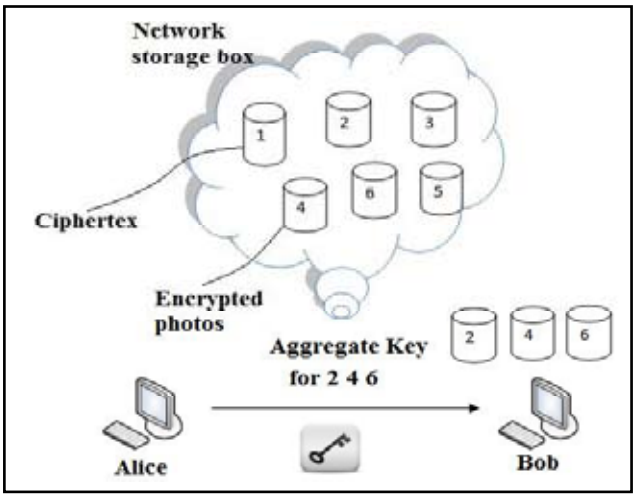


Fig.1 : File sharing between Alice and Bob

Existing System

There exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations. Recently, Green et al. proposed a remedy to this problem by introducing the notion of ABE with outsourced decryption, which largely eliminates the decryption overhead for users. Based on the existing ABE schemes, Green et al. also presented concrete ABE schemes with outsourced decryption.

transformation key TK that allows the latter to translate any ABE cipher text CT satisfied by that user's attributes or access policy into a simple cipher text CT', and it only incurs a small overhead for the user to recover the plaintext from the transformed cipher text CT'. The security property of the ABE scheme with outsourced decryption guarantees that an adversary (including the malicious cloud server) be not able to learn anything about the encrypted message; however, the scheme provides no guarantee on the correctness of the transformation done by the cloud server. In the cloud computing setting, cloud service providers may have strong financial incentives to return incorrect answers, if such answers require less work and are unlikely to be detected by users.

Drawbacks of Existing System:

- Unexpected privilege escalation will be exposed all.
- It is not efficient.
- Shared data will not be secured.

Proposed System

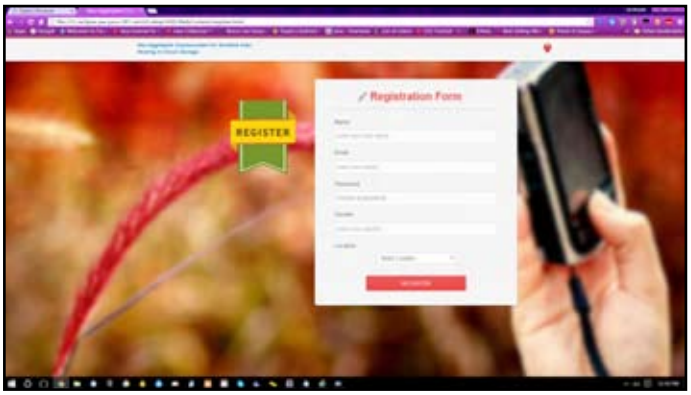
We considered the verifiability of the cloud's transformation and provided a method to check the correctness of the transformation. However, the we did not formally define verifiability. But it is not feasible to construct ABE schemes with verifiable outsourced decryption following the model defined in the existing. Moreover, the method proposed in existing relies on random oracles (RO). Unfortunately, the RO model is heuristic, and a proof of security in the RO model does not directly imply anything about the security of an ABE scheme in the real world. It is well known that there exist cryptographic schemes which are secure in the RO model but are inherently insecure when the RO is instantiated with any real hash function.

In this thesis work, firstly modify the original model of ABE with outsourced decryption in the existing to allow for verifiability of the transformations. After describing the formal definition of verifiability, we propose a new ABE model and based on this new model construct a concrete ABE scheme with verifiable outsourced decryption. Our scheme does not rely on random oracles.
In this paper we only focus on CP-ABE with verifiable outsourced decryption. The same approach applies to KP-ABE with verifiable outsourced decryption.To assess the performance of our ABE scheme with verifiable outsourced decryption, we implement the CP-ABE scheme with verifiable outsourced decryption and conduct experiments on both an ARM-based mobile device and an Intel-core personal computer to model a mobile user and a proxy, respectively.

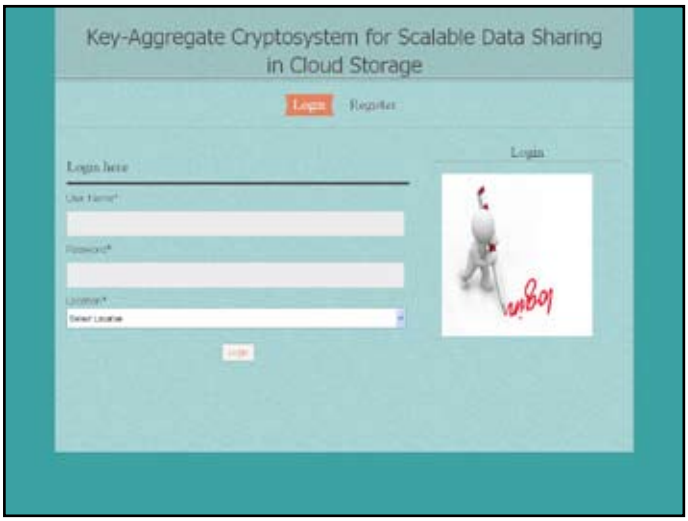
A. Advantages:

- It is more secure.
- Decryption key should be send via secure channel and kept secure.
- its is an efficiency public key encryption sheme which supports flexible delegation.

A. Register Form:



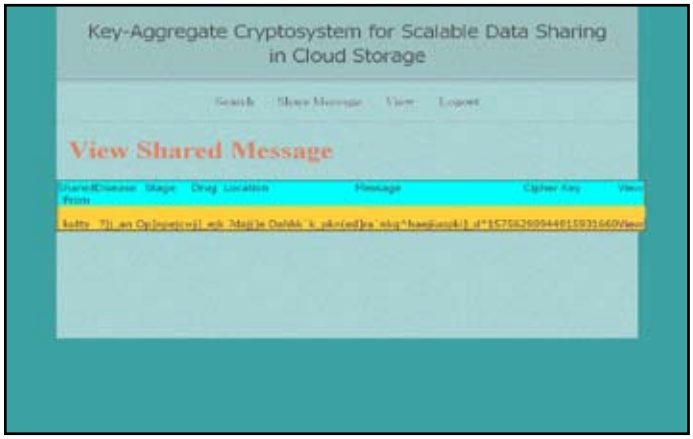
B.Login page:



C. Search page:

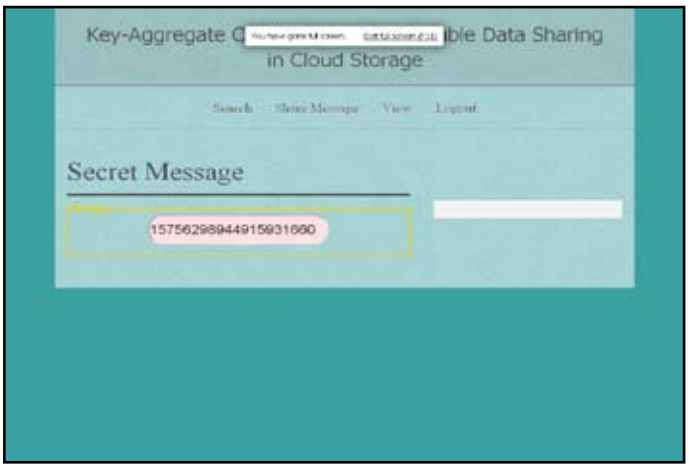
D. Secret Page:

E. view Message:

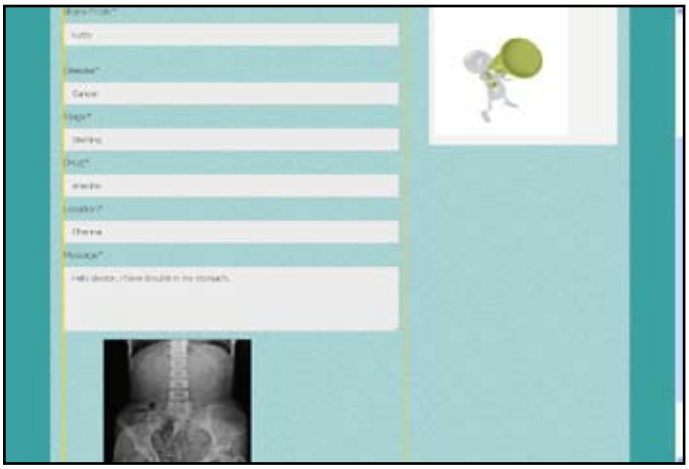


ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

F. Ciphertext Key:



G. Share Message Page:



H. Encrypted Text:

Conclusions

How to protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this article, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No matter which one among the power set of classes, the delegatee 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.

References

[1] *S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE -Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.*

[2] *L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.*

[3] *http://link.springer.com/chapter/10.1007%2F978-3-642-28368-0_28#page-1*

[4] *http://digital.cs.usu.edu/~mingli/papers/Wang_ICDCS_2013.pdf*

[5] *http://crypto.stanford.edu/~dabo/papers/aggreg.pdf*

[6] *http://www.cse.nd.edu/~mblanton/papers/ccs05.pdf*

[7] *http://research.microsoft.com/enus/um/people/horvitz/ccsw_2009_benaloh_chase_horvitz_lauter.pdf*

.