International Journal of Science Engineering and Advance Technology

Scalable Data Sharing In Cloud using Public Key Cryptosystem

MadetiMohana Krishna Kumar [1], S.Madhri [2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: mohanakrishna49@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract— Data sharing is an important functionality in cloud storage. We show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems that produce constant-size cipher text such that efficient delegation of decryption rights for any set of cipher text is 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. The secret key holder can release the constant-size aggregate key for the flexible choices of cipher text set in cloud storage, but 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 encryption for flexible hierarchy, which was yet to be known.

Key words: Cloud storage, data sharing, key-aggregate encryption, Public Key Encryption.

I. Introduction

New computing paradigms keep rising. Are placement economic computing model created attainable by the advances in networking technology, wherever a consumer will leverage a service provider's computing ,storage or networking infrastructure. With the unprecedented exponential rate of information, there is an Associate in nursing increasing demand for out sourcing information storage to cloud services like a Microsoft's Azure. Storing information remotely to the cloud in an exceedingly versatile on demand manner brings appealing benefits: relief of the burden for storage management, universal information access with the freelance geographical locations, and avoidance of value on hardware and software, and personnel maintenances etc.al though the infrastructures at a lower place the cloud unit of measurement far more powerful and reliable than personal computing devices, they're still facing the broad vary of every internal and external threats for information integrity. Samples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, there do exist various motivations for CSP(cloud service provider) to behave unfaithfully towards the cloud users regarding the standing of their outsourced information. As examples, CSP may reclaim storage for monetary reasons by discarding information that has not been or isn't accessed, or even hide information. Considering information privacy, As a result of its shared atmosphere, things become worst. As information is access from any virtual machines (VMS) but it resides on one physical machine. Information in an exceedingly target VM is also taken by instantiating another VM co-resident with the target one by traditional means that it completely depends upon the server to produce the access management alone once authentication .it recommends that any shocking increase can expose all information. Commonly in study schemes, TPA will check the supply of information on behalf of owner but cloud server doesn't trust TPA. So we've an inclination to follow vary hypothetical approach for good security .users is required to cipher their own information by using their own key before uploading. Information sharing is Associate in nursing crucial usefulness in cloud storage. Sharing encrypted information effectively is form of tough task. Clearly user will transfer encrypted information and decode them, and share with others; however approach violates worth of cloud storage. Finding Associate in nursing economical and secure thanks to share partial information in cloud storage isn't trivial. Consider Associate in nursing example of 2 military camps. Assume that military camp A is willing to share space maps with military camp B. however because of varied information run chance they can't expose maps to every body. That the camp A encrypts all the map victimisation her own keys before uploading. And send key firmly to the camp B however this might cause draw back that they share all the photos.

II. System Analysis

Existing System:

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse.

Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owners anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality.

A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff.

Disadvantages Of Existing System:

1. The costs and complexities involved generally increase with the number of the decryption keys to be shared.

2. The encryption key and decryption key are different in public key encryption.

Proposed System:

In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size. Specifically, our problem statement is "To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts (produced by the encryption scheme) is decry p table by a constant-size decryption key (generated by the owner of the master-secret key)." We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

Advantages Of Proposed System:

1. The extracted key have can be an aggregate key which is as compact as a secret key for a single class.
2. The delegation of decryption can be efficiently implemented with the aggregate key.

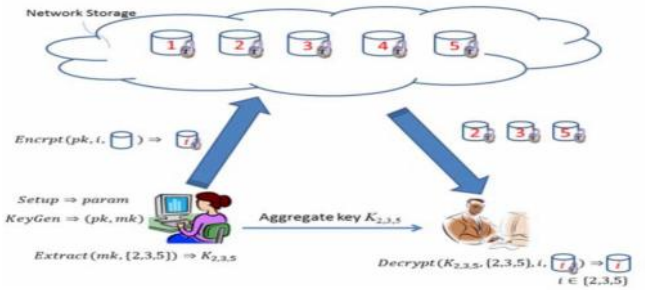

Fig: 1.proposed KAC for data sharing in cloud storage system

III. Implementation

Modules Description:

Data Owner (Alice):

In this module we executed by data owner to the setup account on an untrusted server. The input a security level parameter and the number of ciphertext classes and it outputs the public system parameter param, which is omitted by input of the other algorithms for brevity.

Network Storage (Drop box):

Alice can simply send Bob a single aggregate key via a secure e-mail. Bob can download encrypted photos from the Alice's Dropbox space and then use this aggregate key to decrypt these encrypted photos.

Aggregate Key Transfer:

A key-aggregate encryption scheme for consists of five polynomial-time algorithms. The data owner establishes the public system for parameter via Setup and generates a public/master-secret key pair via key generation. Messages can be encrypted via Encrypt by the anyone who decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate the aggregate decryption key for a set of ciphertext classes via Extract. The generated keys can be passed to delegates securely provided that the cipher text's class is contained in the aggregate key via Decrypt

User (Bob):

The generated keys can be passed to the delegates securely (via secure e-mails or secure devices) finally; any user with the aggregate key can decrypt any ciphertext provided that cipher text's class is contained in aggregate key via Decrypt.

Data Sharing

KAC in meant for the data sharing. The data owner can share the data in desired amount with confidentiality. KCA is easy and secure way to transfer the delegation authority. The aim of KCA is illustrated in Figure 2.

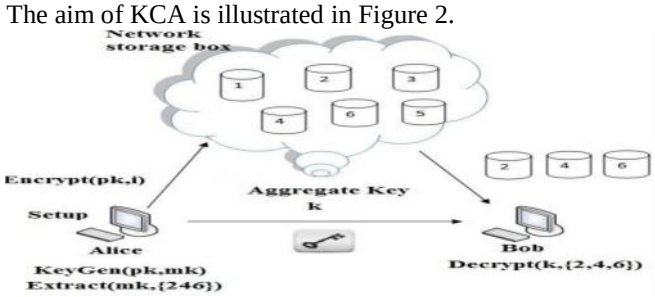

Fig 2 Use of KAC for data sharing

.

IV.ResultAnd Discussion

Our approaches change the compression issue F (F =n inour schemes) to be a tunable parameter, at thecost of O(n)-sized system parameter. Cryptography is tiredconstant time, whereas coding is tired O(|S|) clustermultiplications (or purpose addition on elliptic curves) with2 pairing operations, where S is that the set of ciphertextclasses decryptable by the granted mixture key and |S| ≤ n.of course, key extraction wants O(|S|) clustermultiplications additionally, that a replacement advance onthe stratified key assignment (a ancient approach) thatpreserves areas providing the entireties of the key-holdersshare similar edges is our approach of "compressing" secretkeys in public key cryptosystems. These public keycryptosystems manufacture cipher texts of constant sizenominal economical delegation of secret writing rights forany set of cipher texts is possible. This not exclusivelyenhances user privacy and confidentiality of data in cloudstorage, but it'll this by supporting the distribution orappointing of secret keys varied for diverse} cipher textclasses and generating keys by numerous derivation ofcipher text class properties of the information and itsassociated keys. This sums up the scope of our paper.As there is a limit attack selection the quantity the quantity}of cipher text classes beforehand & in addition to theexponential growth inside the quantity of cipher texts incloud storage, there is a demand for reservation of ciphertext classes for future use. As for potential modificationsand enhancements to our current cause, in future, theparameter size area unit usually altered nominal it'sfreelance of the utmost style of cipher text

classes. to boot,a specially designed cryptosystem, with the employment of an accurate security formula, as associate degree example, the Diffie-Hellman Key-Exchange methodology, which can then be imperviable, or at the foremost proof against outpouring at the aspect of economical key appointing, will confirm that one can transport same keys on mobile devices without fear of outpouring.

Screen Shots

V.Conclusions

A new advance on the class-conscious key assignment (a ancient approach) that preserves areas providing the entireties of the key-holders share similar edges is our approach of "compressing" secret keys publicly key cryptosystems. These public key crypto systems manufacture cipher texts of the constant size of specified economical delegation of secret writing rights for any set of cipher texts is feasible. This not solely enhances user privacy and confidentiality of knowledge in cloud storage, however it will this by supporting the distribution or appointing of secret keys numerous for diverse} cipher text categories and generating keys by various derivation of cipher text category properties of the info and its associated keys. Of cipher text categories beforehand & let alone the exponential growth within the number of cipher texts in cloud storage, there's a requirement for reservation of cipher text categories for future use. As for potential modifications and enhancements to our current cause, in future, the parameter size are often altered specified it's freelance of the utmost variety of cipher text categories. To boot, a specially designed cryptosystem, with the utilization of a correct security algorithmic rule, as an example, the Diffie-Hellman Key-Exchange methodology, which may then be ladder proof, or at the most proof against outpouring at the side of economical key appointing, can make sure that one will transport same keys on mobile devices without worrying of outpouring

VI. References

[1] key –Aggregate Cryptosystem for Scalable Data Sharing in CloudStorage Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng,Jianying Zhou, and Robert H. Deng, *Senior Member, IEEE*

[2] C Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEETrans.Computers*, vol. 62, no. 2, pp. 362–375, 2013

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted data,"in*Proceedings of the 13th ACM Conference on Computer andCommunications Security (CCS '06)*. ACM, 2006, pp. 89–98.

[4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic andEfficient Key Management for Access Hierarchies,"*ACMTransactions on Information and System Security (TISSEC)*, vol.12,no. 3, 2009.

[5] S. S. M. Chow, C.-K.Chu, X. Huang, J. Zhou, and R. H. Deng,"Dynamic Secure Cloud Storage with Provenance," in*Cryptography and Security: From Theory to Applications – EssaysDedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate andVerifiably Encrypted Signatures from Bilinear Maps," in *Proceedingsof Advances in Cryptology - EUROCRYPT '03*, ser. LNCS,vol. 2656.Springer, 2003, pp. 416–432.

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

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

[9] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data onthe Cloud via Security-Mediator," in*International Conference onDistributed Computing Systems - ICDCS 2013*. IEEE, 2013.

[10] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient ControlledEncryption: Ensuring Privacy of Electronic Medical Records," in*Proceedings of ACM Workshop on Cloud Computing Security (CCSW'09)*. ACM, 2009, pp. 103–114.

[11] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-KeyDecryption without Random Oracles," in *Proceedings of InformationSecurity and Cryptology (Inscrypt '07)*, ser. LNCS, vol. 4990.Springer, 2007, pp. 384–398.

[12] G. C. Chick and S. E. Tavares, "Flexible Access Control with MasterKeys," in *Proceedings of Advances in Cryptology - CRYPTO'89*, ser.LNCS, vol. 435. Springer, 1989, pp. 316–322

[13] W.-G. Tzeng, "A Time-Bound Cryptographic Key AssignmentScheme for Access Control in a Hierarchy," *IEEE Transactions onKnowledge and Data Engineering (TKDE)*, vol. 14, no. 1, pp. 182–188,2002.

[14] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," *J.Cryptology*, vol. 25, no. 2, pp. 243–270, 2012Cho,

[15] J., Garcia-Molina, H., Page, L., Efficient Crawling: Through URLOrdering, Computer Science Department, Stanford University,Stanford, CA, USA, 1997.