International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Review on Key Aggregate Policies for Secure Data Sharing in Cloud Storage

Sneha A.Jaswante†* and Nitin R.Chopde†

†Department of Computer Science & Engineering, SGBAU, India

Accepted 07 Feb 2015, Available online 10 Feb 2015, **Vol.5, No.1 (Feb 2015)**

Abstract

Sensitive knowledge changed must be firmly done to verify the integrity of cloud knowledge, to prevent it from being disclosed to or changed by unauthorized parties. Several enterprises source knowledge storage to the cloud specified a member of a corporation or knowledge owner will simply share knowledge with different members or users with confidentiality. The new public- key cryptosystems that turn out constant-size ciphertext where specified ciphertext area unit labelled with sets of attributes and personal keys area unit related to structures that management that user is ready to rewrite. In different words, the key holder will unleash a constant-size mixture key for versatile preferences of ciphertext set in cloud storage, however the opposite encrypted files outside the set stay secret. Additionally to authentication and privacy preservation this theme tries to satisfy all different security necessities with key management and achieves higher measurability once the amount of access levels will increase.

Keywords: *Cloud storage, data sharing, key-aggregate encryption.*

1. Introduction

Cloud computing is an active research topic aiming to create safe conversation environments online. It is internet based computing technology where virtual shared servers provide software, platform, infrastructure, and other resources that delivers the resources as a service to the users over the internet. Internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform is eliminating the responsibility of local machines for data maintenance at the same time. While in a cloud computing system, most data and software that users use reside on the Internet, which bring some new challenges for the system, regarding to security and privacy. On the one hand, although the cloud infrastructures are much more powerful and reliable than personal computing devices, broad range of both internal and external threats for data integrity still exist.

Cloud computing have many advantages in resource sharing, cost reduction, and time saving for new services. Since each application may use resource from multiple servers. The servers may located at multiple locations and the cloud may use different infrastructures across organizations. All these characteristics of cloud computing make it complicated to provide security in cloud computing. To ensure adequate security in cloud computing, various security issues, such as authentication, data confidentiality and integrity, and non-repudiation, all need to be taken into account. Users can access these services available on the cloud without having any previous knowledge on managing the resources involved. Thus, users can concentrate more on the core business processes rather than spending time on gaining knowledge on resources needed to manage their business processes.

2. Literature Survey

Cryptographic key task plans intend to minimize the cost in putting away and overseeing mystery keys for general cryptologic utilization. Using a tree structure, a key for a given extension are frequently usual infer the keys of its relative hubs (yet not the inverse means round) essentially conceding the guardian key verifiably allows all the keys of its relative nodes. There is a system to think of a tree order of symmetric keys by exploitation perpetual assessments of pseudorandom capacity/square figure on a resolute mystery. The thought will be summed up from a tree to a diagram a great deal of cutting edge cryptographic key task plans help access strategy which will be designed by partner non-cyclic chart or a cyclic diagram . The greater part of those plans turn out keys for symmetric-key cryptosystems, despite the fact that the key inferences may require standard number juggling as utilized as a part of open key cryptosystems, that are normally more costly than "symmetric-key

*Corresponding author **Sneha A.Jaswante** is a PG Scholar and **Prof Nitin R.Chopde** is working as HOD

operations" such as pseudorandom perform (C.Chu, S.S.M. Chow *et al,*2014).

Group key management protocol (Y.Challal, H. Seba *et al*,2005) is use to introduce the difficult problems about cluster confidentiality and key management. There area unit two main practical entities use for security of the session that is managed by: a Group Controller (GC) accountable for authentication, authorization and access management, and a Key Server (KS) to confirm confidentiality throughout the multicast session, the sender (source) shares a secret symmetrical key with all valid cluster members, referred to as Traffic Encryption Key (TEK). To multicast a secret message, the supply encrypts the message with the TEK employing a symmetrical secret writing formula.

Proxy ReEncryption schemes (R. Canetti , S. Hohenberger *et al*,2007) is secure in arbitrary protocol settings that are secure against chosen ciphertext attacks. The concept of a CCA secure PRE scheme sounds almost self-contradictory, since on the one hand we want the cipher texts to be nonmalleable, and allow the proxy to translate" the ciphertext from one public key to another. Still, it formulate a meaningful definition of CCA-secure PRE schemes, along with a construction that meets the definition in the standard model and under relatively mild hardness assumptions for bilinear groups.

In bilaterally symmetrical key coding (Benaloh , M. Chase *et al*,2009) conferred coding theme that is originally planned for in short sending sizable amount of keys in broadcast state of affairs(J. Benaloh *et al*,2009). The act of receving the key for a collection of categories that could be a set of all doable ciphertext categories is as follows. A composite modulus is chosen wherever p and letter square measure two giant random primes. A master secret secret is chosen randomly every category is related to a definite prime. These prime numbers is place within the public system parameter. A constant-size key for set is generated. For people who are delegated the access rights for set is generated. However, it's designed for the symmetric-key setting instead. The content supplier must get the corresponding secret keys to cipher information, that isn't appropriate for several applications as a result of technique is employed to get a secret price instead of a try of public/secret keys, it's unclear a way to apply this idea for public-key coding theme. Finally, there square measure schemes that attempt to cut back the key size for achieving authentication in symmetric-key coding, (B. Alomair, R. Poovendran *et al,*2009). However, sharing of decipherment power isn't a priority in these schemes.

Identity-based secret writing (IBE) (D. Boneh *et al*,2001; A. Sahai *et al,2005;S.S.M.Chow et al,2010*) may be a public-key secret writing during which the public-key of a user are often set as an identity-string of the user (e.g., mobile variety, an email address). There's a trusty party known as personal key generator in IBE that holds a master-secret key and problems a secret key to every user with reference to the user identity. The code or will take the general public parameter and a user identity to encrypt a message. The receiver will decode this ciphertext by secret key.(Guo *et al,* 2007) tried to create IBE with key aggregation. All mass key should come back from completely different identity divisions whereas there are exponential variety of identities and so secret keys, solely a add of finite variety of them are often mass the prices of storing and transmission ciphertexts will increase. The in a different way to try to to this is often to use hash operate to the string denoting the category, and keep hashing repeatedly till a chief is obtained because the output of the hash operate. In fuzzy IBE (A. Sahai *et al*,2005), one single compact secret key will decode ciphertexts encrypted below several identities, however not for discretional set of identities and so it doesn't match with the concept of key aggregation.

Attribute-based encryption (ABE) is powerful cryptographic primitive which provide encryption mechanism with fine grained access control. There are two kinds of ABE in the literarures, key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) (Yong Cheng *et al*,2012). In KP-ABE, sender ascribes attributes to the ciphertext which come from pre-defined universal attribute set(C.-K. Chu *et al,*2009). ABE scheme with constant-size cipher texts allowing for as expressive policies as possible maintains each ciphertext to be associated with an attribute, (M. Chase *et al*,2009; T. Okamoto *et al*,2011) and the master-secret key holder can extract a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conforms to the policy. For example, with the secret key for the policy $(3 \vee 5 \vee 7 \vee 9)$, one can decrypt ciphertext tagged with class 3, 5, 7 or 9. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys. But, the size of the key often increases linearly with the number of attributes it encompasses, or the ciphertext-size is not constant.

3. Problem statement and discussion

In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. The local users can store their data in the remote cloud storage servers, from that the users can access the data from anywhere in the world. But storing data in a third party cloud system may affect the data confidentiality. For avoid this issue the data's are encrypted before storing in to storage server. In the general encryption system the data owner encrypts the data by using cryptographic methodology and stores the encrypted data at the cloud storage server. It provides data confidentiality but it does not provide high security and dynamic data modification. The unauthorized user may get the data while transfer from the data owner to the cloud server, or he can decrypt the data directly from the cloud

server by getting cryptographic keys. Then the hacker may perform some modifications at the hacked data and again stored in to the storage server like a data owner. The cloud users and data owner can't identify the data hacking. The data displays like original data. The receiver thing like the data came from the data owner,it affects the data originality, data origin authentication, security and data integrity.

4. Objective

Due to the existence of external and internal attacks within the cloud, cloud users stay involved concerning the integrity of their information within the cloud. On the opposite hand, information house owners need to preserve not solely their identity privacy however conjointly information privacy after they produce the information to be shared to handle the on top of security and privacy threats, our system ought to accomplish the subsequent properties.

In public verifiability the integrity of cloud information (outsourced by information owners) ought to be verifiable by a public supporter. In verification potency a public supporter, particularly agency doesn't possess cloud information, ought to be ready to verify the integrity of cloud information while not retrieving the complete information from the cloud server. In unforgeability the verification data (signatures) for guaranteeing information integrity ought to be existentially unforgeable below adaptive chosen-message attack. In obscurity the identity of a knowledge owner mustn't be disclosed to a public supporter throughout the verification of information integrity additionally, a security treater mustn't be ready to reveal the identity of a information or a knowledge an information owner supported cloud data and corresponding signatures. In information privacy throughout the generation of signatures for a knowledge owner, different parties, even a security treater, mustn't be ready to learn the content of information that the information owner desires to sign. In language potency the communication demand between a security treater and a knowledge owner throughout signature generation ought to be smaller than directly transferring the information to be signed.

Conclusion

The access policy and cryptographic schemes are getting more versatile and often involve multiple keys for a single application. The propose associate innovative design that guarantee the user data privacy with the help of aggregate keys. The aggregate key encryption combined with ciphertext, which provides user revocation and prevents replay attacks with high security. The cloud does not know the type of the user who stores information in the cloud, but only verifies the user's credentials. It is use to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. This approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. These performance results open the space to future improvements that are investigating in this work.

Reference

Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member (2014), Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage, *IEEE Transaction on Parallel and Distributed System*, Vol. 25, No. 2.

Yacine Challal, Hamida Seba (2005), Group Key Management Protocols, *A Novel Taxonomy*, ISSN:1305- 2403

R. Canetti and S. Hohenberger (2007), Chosen Cip hertext Secure Proxy Re-Encryption, *The 14th ACM Conference on Computer and Communications Security (CCS'07).ACM* , pp. 185–194.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter (2009), Patient Controlled Encryption: Ensuring Privacy sof Electronic Medical Records, *ACM Workshop on Cloud Computing Security (CCSW '09). ACM*, pp. 103–114.

J. Benaloh (2009), Key Compression and Its Application to Digital Fingerprinting, *Microsoft Research, Tech. Rep*.

B. Alomair and R. Poovendran (2009), Information Theoretically Secure Encryption with Almost Free Authentication, *J. UCS*, vol. 15, no. 15, pp. 2937–2956.

D. Boneh and M. K. Franklin (2001), Identity-Based Encryption from the Weil Pairing, *Advances in Cryptology – CRYPTO '01, ser. LNCS,* vol. 2139. Springer, pp. 213–229.

A. Sahai and B. Waters (2005), Fuzzy Identity-Based Encryption, *Advances in Cryptology EUROCRYPT, ser. LNCS,* vol. 3494. Springer, pp. 457–473.

S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters (2010), Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions, *ACM Conference on Computer and Communications Security*, pp. 152–161.

F. Guo, Y. Mu, and Z. Chen (2007), Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key,*Pairing-Based Cryptography (Pairing '07), ser. LNCS*, vol. 4575. Springer, pp. 392–406.

F. Guo, Y. Mu, Z. Chen, and L. Xu (2007), Multi-Identity Single-Key Decryption without Random Oracles, *Information Security and Cryptology (Inscrypt '07), ser. LNCS,* vol. 4990. Springer, pp. 384–398.

V. Goyal, O. Pandey, A. Sahai, and B. Waters (2006), Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data, *The 13th ACM Conference on Computer and Communications Security (CCS '06). ACM*, pp. 89–98.

M. Chase and S. S. M. Chow (2009), Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, *ACM Conference on Computer and Communications Security*, pp. 121–130.

T. Okamoto and K. Takashima (2011), Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption, *Cryptology and Network Security (CANS '11)*, pp. 138–159.

C.-K. Chu and W.-G. Tzeng (2007), Identity-Based Proxy Re-encryption Without Random Oracles, *Information Security Conference (ISC'07), ser. LNCS*, vol. 4779. Springer, pp. 189–202.

C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng (2009), Conditional Proxy Broadcast Re-Encryption, *Australasian Conference on Information Security and Privacy (ACISP '09), ser. LNCS,* vol. 5594. Springer, pp. 327–342.

Fengli Zhang, Qinyi Li, Hu Xiong (2012), Efficient Revocable Key-Policy Attribute Based Encryption with Full Security, *Eighth International Conference on Computational Intelligence and Security*, pp. 477-481.

C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou (2013), Privacy-Preserving Public Auditing for Secure Cloud Storage, *IEEE Trans. Computers*, vol. 62, no. 2, pp. 362-375.

Yong Cheng, Jiangchun Ren, Zhiying Wang (2012), Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control, *Second International Conference on Cloud and Green Computing, pp.180-186*