IJRRECS/January 2016/Volume-4/Issue-1/5108-5112 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A NOVEL PROPOSAL FOR PROTECTING USER PRIVACY IN CLOUD STORAGE SYSTEM

Shaik Moulana Azad[1], K.David Raju[2]

[1]M.Tech Student, Dept of CSE, St. Peter's Engineering College, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, St. Peter's Engineering College, Hyderabad, T.S, India

ABSTRACT:

The services of cloud storage have tuned out more and more popular and users store their information on cloud and permit their information at any instant. Due to the privacy of user, data that is stored on cloud is usually encrypted and defended from access by means of other users. When considering the situation of cloud storage, we spotlight our efforts on deniable public key encryption system. Since it is difficult to fight outside coercion, we build an encryption system that will assist cloud providers to avoid the predicament. In our method we present cloud providers means to generate false user secrets. User privacy is sheltered and the notion comes from particular encryption scheme known as deniable encryption. In our work we make available a novel method of cloud storage encryption that permits cloud providers to generate convincing false user secrets to defend user privacy. Although coercers cannot inform the obtained secrets are proper or not, cloud provider make sure that user confidentiality is still strongly protected. We make use of attribute-basis encryption features for protecting of stored information by means of fine-grained access control method and deniable encryption to avoid outside auditing.

Keywords: Attribute-basis encryption, Fine-grained access control, Cloud storage, Deniable public key encryption, Coercion, User privacy, Cloud storage encryption.

1. INTRODUCTION:

For the most of the projected methods will believe service providers of cloud storage are trustworthy and are unable to hack. On the other hand some of the entities might interrupt communications among users as well as cloud providers and afterwards force storage providers to provide user secrets by means of government power [1]. As it is tricky to fight outside coercion, we build an encryption system that will assist cloud providers to avoid the predicament. In our method we present cloud providers means to generate false user secrets. When false user secrets, exterior coercers can obtain forged information from user stored cipher text and once coercers imagine received secrets are actual; they are satisfied and cloud providers will not reveal any actual secrets. Hence user privacy is still secluded and the notion comes from particular encryption scheme known as deniable encryption. In our work we provide a novel method of cloud storage encryption that permits cloud providers to generate convincing false user secrets to defend user privacy. While coercers cannot inform if obtained secrets are proper or else not, cloud provider make sure that user confidentiality is still strongly protected. Our method has two significant properties such as user can get hold of accurate message by means of a suitable secret key, irrespective of whether cipher-text is usually encrypted or else deniably encrypted. Secondly, fake key is used to decrypt usually encrypted cipher-text.

2. AN INTRODUCTION TOWARDS DENIABLE ENCRYPTION:

Services of cloud storage have become more and more popular and due to the significance of privacy, lot of methods of cloud storage encryption were projected to defend information from those who do not contain permission [2]. Most of the methods imagine that cloud providers are protected and cannot be hacked; on the other hand, a number of authorities might force cloud providers to make known user secrets on e cloud, hence circumventing methods of storage encryption. In our work we explain a deniable attribute-basis encryption method for the services of cloud storage. Deniable encryption includes senders as well as receivers building believable false proof of forged data in cipher texts so that exterior coercers are fulfilled. Since it is difficult to fight outside coercion, we build an encryption system that will assist cloud providers to avoid the predicament. In our

method we present cloud providers means to generate false user secrets. We utilize attribute-basis encryption features for protecting of stored information by means of fine-grained access control method and deniable encryption to avoid outside auditing. Our technique is on basis of waters cipher-text policy-attribute based encryption method and our system permits users to be competent to offer false secrets that seem genuine towards outside coercers. Our method of cloud storage encryption permits cloud providers to generate convincing false user secrets to defend user privacy. Although coercers cannot inform if obtained secrets are proper or else not, cloud provider make sure that user confidentiality is still protected. The notion of deniable encryption was initially proposed and like normal methods of encryption, deniable encryption is divided as deniable shared key method and public key method. The perfect method of deniable encryption is ad hoc, complete, bi-deniability as well as non-interactive deniability; on the other hand, there is study that is focused on determining limits of deniable schemes. We provide cloud providers means to generate false user secrets and when false user secrets, exterior coercers can obtain forged information from user stored cipher text and once coercers imagine received secrets are actual; they are satisfied and cloud providers will not reveal any actual secrets [3][4]. For this reason user privacy is still secluded and the notion comes from particular encryption scheme known as deniable encryption.

3. AN OVERVIEW OF BUILDING PROPOSED DENIABLE SCHEME:

Deniability comes from actuality that coercers cannot confirm the projected evidence is incorrect and thus have no basis to refuse the specified evidence and this approach obstruct coercion efforts as coercers recognize that their efforts are ineffectual. We utilize this idea so that cloud providers can offer audit-free storage services. Deniable encryption includes senders as well as receivers building believable false proof of forged data in cipher texts so that exterior coercers are fulfilled. In our work we describe a deniable attribute-basis encryption method for the services of cloud storage. In cloud storage situation, data owners who store up their information on cloud are senders in deniable encryption system. Those who access encrypted information acts as receiver in deniable encryption system, that includes

cloud providers, who contain system wide secret and should decrypt the entire encrypted information. We make use of attribute-basis encryption features for protecting of stored information by means of fine-grained access control method and deniable encryption to avoid outside auditing. We provide a novel method of cloud storage encryption that permits cloud providers to generate convincing false user secrets to defend user privacy. Our method is on basis of waters cipher-text policy-attribute based encryption method and our system permits users to be competent to offer false secrets that seem genuine towards outside coercers. While coercers cannot inform if obtained secrets are proper or else not, cloud provider make sure that user confidentiality is still strongly protected. In our method user can get hold of accurate message by means of a suitable secret key, irrespective of whether cipher-text is usually encrypted or else deniably encrypted. Fake key is used to decrypt usually encrypted cipher-text. In the proposed system situation, cloud service providers are considered as receivers in several deniable schemes. Different from most of the earlier deniable encryption methods, we do not make use of transparent sets to put into practice deniability. Like normal methods of encryption, deniable encryption is divided as deniable shared key method and public key method. When fake user secrets, exterior coercers can obtain forged information from user stored cipher text and once coercers imagine received secrets are actual; they are satisfied and cloud providers will not reveal any actual secrets [5]. User privacy is secluded and the notion comes from particular encryption scheme known as deniable encryption. We build deniable encryption method all the way through multidimensional space. All the information is encrypted to multidimensional space and only with accurate composition of proportions is innovative data accessible. By means of false composition, cipher-texts are decrypted towards pre-determined false data. The information describing dimensions is set aside secret. We take advantage of composite order bilinear groups to build multidimensional space. As we desire our scheme to be block-wise deniable by means of constant encryption setting, we intend our system to be plan-ahead system of deniable encryption [6]. We prefer our system to contain non-interactive property for user-friendliness hence, our method is multi-distributional.

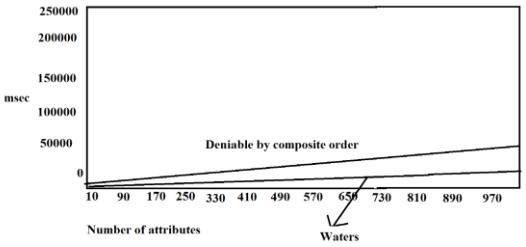

Fig1.An overview of Encryption benchmark

4. CONCLUSION:

When considering collaborative cloud data property, attribute-basis encryption is the most appropriate encryption methods for cloud storage. As it is difficult to fight outside coercion, we build an encryption system that will assist cloud providers to avoid the predicament. In our method we present cloud providers means to generate false user secrets. User confidentiality is still secluded and the notion comes from particular encryption scheme known as deniable encryption. Deniable encryption comprises senders as well as receivers building believable false proof of forged data in cipher texts so that exterior coercers are fulfilled. In our work we describe deniable attribute-basis encryption method for the services of cloud storage and provide a novel method of cloud storage encryption that permits cloud providers to generate convincing false user secrets to defend user privacy. While coercers cannot inform if obtained secrets are proper or else not, cloud provider make sure that user confidentiality is still strongly protected. We exploit attribute-basis encryption features for protecting of stored information by means of fine-grained access control method and deniable encryption to avoid outside auditing. Our system is on basis of waters cipher-text policy-attribute based encryption method and our system permits users to be competent to offer false secrets that seem genuine towards outside coercers.

REFERENCES

[1] D. M. Freeman, "Converting pairing-based cryptosystems fromcomposite-order groups to prime-order groups," in Eurocrypt,2010, pp. 44–61.

[2] A. B. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in Eurocrypt, 2012,pp. 318–335.

[3] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of technology, 1996.

[4] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supportingdisjunctions, polynomial equations, and inner products," inEurocrypt, 2008, pp. 146–162.

[5] S. Meiklejohn, H. Shacham, and D. M. Freeman, "Limitations ontransformations from composite-order to prime-order groups: Thecase of round-optimal blind signatures," in Asiacrypt, 2010, pp.519–538.

[6] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext securityfrom identity-based encryption," SIAM J. Comput., vol. 36,no. 5, pp. 1301–1328, 2007.