IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Key Aggregate Cryptosystem for Group Sharing Data on Cloud Storage

Ashwini Patil[1], Lathashree Chintakindi[2], Prof. Rajana Kedar[3], Amrutamasal[4], Pritam Shinde[5]

Student, Computer Dept, KJCOEMER, Pune, India [1, 2, 4, 5]

Professor, Computer Dept, KJCOEMER, Pune, India [3]

Abstract: Data sharing is a very important practicality in cloud storage. This paper generally tend to expose the way to firmly, expeditiously, and flexibly proportion understanding with others in cloud garage. This paper have a tendency to describe new public-key cryptosystems that manufacture steady-length ciphertexts exact reasonably priced delegation of cryptography rights for any set of ciphertexts are workable. The newness is that one will mixture any set of mystery keys and construct them as compact as one key, however encompassing the ability of all the keys being aggregate. In opportunity words, the important thing holder will unharness a constant-length aggregate key for flexible alternatives of ciphertext set in cloud garage, but the contrary encrypted files out of doors the set stay confidential. This compact combination key can be handily sent to others or be preserve on terribly revolving credit with very limited comfy storage. This system offer formal security analysis of schemes inside the common place version. This machine have a tendency to moreover describe opportunity software of this schemes. Mainly, this schemes offer the number one public-key patient managed cryptography for versatile hierarchy,that was although to be legendary.

Keywords: Public key encryption, master key, ABE scheme, cloud computing, web based services, data sharing.

I. INTRODUCTION

One of the most potency drawbacks of the foremost present ABE(Attribute-Based Encryption) schemes is that coding is costly for aid-constrained devices because of pairing operations, and therefore the form of pairing operations needed to decode a ciphertext grows with the nice of the access policy. The on pinnacle of statement motivates unitedstates to check ABE (Attribute-Based Encryption) with verifiable outsourced coding at some stage in this thesis work. Right here careworn that ABE (Attribute-Based Encryption) subject with comfortable outsourced coding does not basically guarantee verifiability (i.e., correctness of the transformation accomplished by using the server).

II. LITERATURE REVIEW

Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

Description:
In this paper they describe, each ciphertext is labeled by the encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of ciphertexts the key can decrypt.

We call such a scheme a Key-Policy Attribute-Based Encryption (KP-ABE), since the access structure is specified in the private key, while the ciphertexts are simply labeled with a set of descriptive attributes.

Aggregate and Veriably Encrypted Signatures from Bilinear Maps

Description:
In this paper they describe, the concept of an aggregate signature, present security models for such signatures, and give several applications for aggregate signatures.
An efficient aggregate signature from a recent short signature scheme based on bilinear maps.

Aggregate signatures are useful for reducing the size of certificate chains (by aggregating all signatures in the chain) and for reducing message size in secure routing protocols such as SBGP.

Dynamic and Efficient Key Management for Access Hierarchies
In this paper they describe, problem of key management in an access hierarchy has elicited much interest in the literature.
Solution to the above problem has the following properties:

(i) only hash functions are used for a node to derive a de-scendant's key from its own key;
(ii) the space complexityof the public information is the same as that of storing the hierarchy;
(iii) the private information at a class consists of a single key associated with that class;
(iv) updates (revocations, additions, etc.) are handled locally in the hierarchy;
(v) the scheme is provably secure against collusion;
(vi) key derivation by a node of its descendant's key is bounded by the number of bit operations linear in the length of the path between the nodes.

IJARCCE

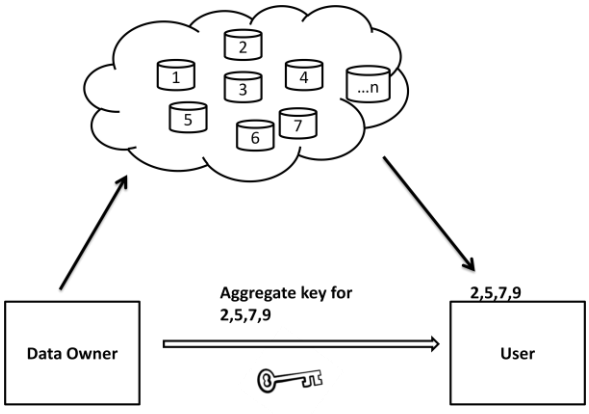
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

III. EXISTING SYSTEM

There exist many communicative ABE(Attribute-Based Encryption) schemes anywhere the name of the game writing algorithmic program entirely desires a continuing variety of pairing computations. These days, green et al. planned a treatment to the present drawback by means of introducing the belief of ABE (Attribute-Based Encryption) with outsourced mystery writing, that for the maximum component eliminates the secret writing overhead for customers. Supported the present ABE (Attribute-Based Encryption) schemes, inexperienced et al. conjointly given concrete ABE (Attribute-Based Encryption) schemes with outsourced secret writing.
In these present schemes, a user affords associate degree untrusted server, say a proxy operated by means of a cloud carrier dealer, with a transformation key TK that lets in the latter to translate any ABE(Attribute-Based Encryption) ciphertext CT happy by means of that consumer's attributes or get entry to coverage into a truthful ciphertext CT', and it entirely incurs a tiny low overhead for the consumer to get better the plaintext from the remodeled ciphertext CT'. The safety property of the ABE(Attribute-Based Encryption) theme with outsourced mystery writing guarantees that companion degree mortal (inclusive of the malicious cloud server) be not able to be told something concerning the encrypted message but, the subject gives no guarantee at the correctness of the transformation accomplished with the aid of the cloud server. In the cloud computing placing, cloud carrier suppliers ought to have sturdy financial incentives to return lower back incorrect answers, if such answers need less paintings and are not going to be detected by customers.

IV. ARCHITECTURAL DESIGN



V. PROPOSED SYSTEM

We considered the verifiability of the cloud's transformation and supplied a technique to test the correctness of the transformation. However, this did not formally define verifiability. But it is not viable to assemble ABE with verifiable outsourced decryption following the version described in the present. Moreover, the method proposed in existing is based on random oracles (RO). Unfortunately, the RO version is heuristic, and a proof of protection inside the RO model does not immediately mean whatever about the safety of an ABE scheme in the actual world. It's miles widely known that there exist cryptographic schemes which might be secure inside the RO version but are inherently insecure whilst the RO is instantiated with any actual hash feature.

On this thesis paintings, first of all adjust the unique version of ABE with outsourced decryption in the current to allow for verifiability of the changes. After describing the formal definition of verifiability, this gadget advise a new ABE model and based in this new version construct a concrete ABE scheme with verifiable outsourced decryption. This scheme does now not depend on random oracles.

This paper most effective awareness on CP-ABE with verifiable outsourced decryption. The equal approach applies to KP-ABE with verifiable outsourced decryption. To assess the overall performance of ABE scheme with verifiable outsourced decryption, and put in force the CP-ABE scheme with verifiable outsourced decryption.

VI. MATHEMATICAL MODEL

Key Aggregate Mathematical Model
Set of Input = {m,n,c}
Set of Output = {c,m}

1. Generate a pair of large, random primes p and q.
2. Compute the modulus n as n = pq.
3. Select an odd public exponent e between 3 and n-1 that is relatively prime to p-1 and q-1.
4. Compute the private exponent d from e, p and q. (See below.)
5. Output (n, e) as the public key and (n, d) as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the eth power modulo n:

c = ENCRYPT (m) = m^e mod n .

The input m is the message; the output c is the resulting ciphertext. In practice, the message m is typically some kind of appropriately formatted key to be shared. The actual message is encrypted with the shared key using a traditional encryption algorithm. This construction makes it possible to encrypt a message of any length with only one exponentiation.

The decryption operation is exponentiation to the dth power modulo n:

m = DECRYPT (c) = c^d mod n .

VII. CONCLUSION

How to protect users' facts privacy is a vital query of cloud garage. With extra mathematical equipment,

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

cryptographic schemes have become extra versatile and regularly involve a couple of keys for a unmarried application. In this text, “compress” mystery keys in public-key cryptosystems which help delegation of secret keys for exceptional ciphertext classes in cloud garage is proposed. No matter which one a number of the power set of lessons, the delegate can usually get an mixture key of constant size. This machine is morebendy than hierarchical key task that can best shop spaces if all key-holders proportion 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 Environ-ment,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security (ACNS),vol. 7341, pp. 526-543, 2012.

[2] 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.

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

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, “Storing Shared Dataon the Cloud via Security-Mediator,” in International Conference on Distributed Computing Systems ICDCS 2013. IEEE, 2013.

[5] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng,”Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage” IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.

[6] Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,”in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06). ACM, 2006, pp. 89–98.