ISSN 2320 – 2602

Volume 4 No.4, April 2015

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/ijacst/static/pdf/file/ijacst06442015.pdf

Data Security in Cloud Using AES Algorithm Among Multiple Owners

Ali Raheem Abbas Alsultani, Y.V.K. Sudhakar

M.Sc (Computer Science) Mahatma Gandhi College Affiliated to Acharya Nagarjuna University Guntur, AP, India,Ali_it83@yahoo.com

M.Tech (CSE) Mahatma Gandhi College Affiliated to Acharya Nagarjuna University Guntur, AP, India, sudakartechcs@yahoo.com

ABSTRACT

Cloud computing is associate degree rising computing paradigm within which resources of the computing infrastructure area unit provided as services over the net. As promising because it is, this paradigm conjointly brings forth several new challenges for knowledge security and access management once users confidential against untrusted servers, existing solutions sometimes apply cryptological ways by revealing knowledge cryptography keys solely to approved users. one among the largest considerations with cloud knowledge storage is that of knowledge integrity verification at untrusted servers. To preserve knowledge privacy, a basic resolution is to encode knowledge files, so transfer the encrypted knowledge into the cloud. To resolve this downside recently the simplest economical technique Anglesey given for secured multi owner knowledge sharing in but we have a tendency to known some limitations within the same approach in terms of responsible ness and quantify ability. Therefore during this paper we have a tendency to area unit more extending the fundamental Anglesey by adding the responsibleness still as rising the quantifiability by increasing the quantity of cluster managers dynamically.

Key words: *Dynamic groups, Multi owner, Data Sharing , Cloud Computing.*

1. INTRODUCTION

In cloud computing, the cloud service suppliers (CSPs), like Amazon, square measure able to deliver numerous services to cloud users with the assistance of powerful datacenters. By migrating the native information management systems into cloud servers, users will relish high-quality services and save important investments on their native infrastructures. Cloud computing is one in every of the best platform that provides storage of information in terribly lower value and out there for all time over the web Cloud computing is Internet-based computing, whereby shared resources, computer code and knowledge square measure provided to computers and devices on demand. many trends square measure gap up the age of Cloud Computing, that is associate Internet-based development and use of engineering. Cloud Computing suggests that over merely saving thereon implementation prices. Cloud offers huge chance for brand spanking new innovation, and even disruption of entire industries. Cloud computing is that the long unreal vision of computing as a utility, wherever information homeowners will remotely store their information within the cloud to get pleasure from on demand high-quality applications and services from a shared pool of configurable computing resources[2].

2. BASIC CONCEPT

Maintaining the integrity information plays an important role within the institution of trust between data subject and repair supplier. Thoughunreal as a promising service platform for the web, the new information storage paradigm in “Cloud” brings concerning several difficult style problems that have profound influence on the safety and performance of the system. one in all the most important issues with cloud information storage is that of information integrity verification at untrusted servers. what's a lot of serious is that for saving cash and space for storing the service supplier would possibly neglect to stay or deliberately delete seldom accessed information files that belong to a normal shopper. take into account the massive size of the outsourced electronic information and also the client’s unnatural resource capability, the core of the matter may be generalized as however will the shopper notice associate economical thanks to perform periodical integrity verifications while not the native copy of information files. To preserve information privacy, a basic resolution is to encode information files, and so transfer the encrypted information into the cloud [3][5]. CS2 provides security against the cloud supplier, shoppers square measure still in a position not solely to with efficiency access their information through a research

interface however additionally to feature and delete files firmly. many security schemes for information sharing on untrusted servers are planned secure filing system designed to be bedded over insecure network and P2P file systems like NFS, CIFS, Ocean Store, and Yahoo! case.

3. LITERATURE SURVEY

3.1 Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

Shucheng Yu_, Cong Wang†, Kui Ren†, and Wenjing Lou_Dept. Of ECE, Worcester Polytechnic Institute, Email: {yscheng, wjlou}@ece.wpi.edu

This paper addresses this challenging open issue with, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to interested cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability[1].

3.2 Plutus: Scalable, secure file sharing on untrusted storage

MaheshSan Francisco, CA, USA March 31–April 2, 2003.

This paper has introduced novel uses of cryptographic primitives applied to the problem of secure storage in the presence of untrusted servers and a desire for owner managed key distribution. Eliminating almost all requirements for server trust (we still require servers not to destroy data – although we can detect if they do) and keeping key distribution (and therefore access control) in the hands of individual data owners provides a basis for a secure storage system that can protect and share data at very large scales and across trust boundaries.

3.3 Sirius: Securing Remote Untrusted Storage

Eu-Jin Goh_, Hovav Shacham†, Nagendra Modadugu, Dan Boneh‡ Stanford University[6][10].

This paper presents serious, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, OceanStore, and Yahoo! Briefcase. Sirius assumes the network storage is interested and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by Sirius using hash tree constructions. The series contains a novel method of performing file random access in a cryptographic file system without the use of a block server.

3.4 Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing

Rongxing Lu†, Xiaodong Lin‡, Xiaohui Liang†, and Xuemin (Sherman) Shen†

In this paper proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in the cloud, anonymous authentication on user access, and provenance tracking of disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

3.5Ciphertext-Policy Attribute-Based Encryption: An Expressive, E_cient, and Provably Secure Realization

Brent Waters _University of Texas at Austin

This Paper presents a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP- ABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any Encryptor to specify access control in terms of any access formula over the attributes in the system. In our most e_cient system, ciphertext size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model[4].

3.6Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

Vipul Goyal¤ Omkant Pandey*y* Amit Sahai*z* Brent Waters *x.*

This Paper presents more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for ¯ne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to the sharing of audit-log information and broadcast encryption.

3.7Revocation and Tracing Schemes for Stateless Receivers?

Dalit Naor1, Moni Naor2??, and Je® Lotspiech1.

This paper provides a general traitor tracing mechanism that can be integrated with any Subset-Cover revocation scheme that satis¯es a \bifurcation property". This mechanism does not need an a priori bound on the number of traitors and does not expand the message length by much compared to the revocation of the same set of traitors.

4. EXISTING SYSTEM

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. Proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme[7][11]. Presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data as figure 1.

Figure 1. Existing System Model

5. PROPOSED SYSTEM

This paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments[9] as figure 2.

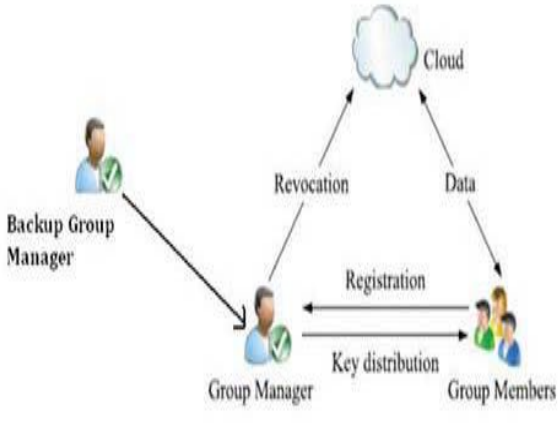

Figure 2. Proposed System Model

6. CONCLUSION

In this paper, we design a Distributed Accountability for Data Sharing in the Cloud, Mona, for dynamic groups in an interested cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well. Proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into filegroups and encrypting each filegroup with a unique file-block key, the data owner can share the filegroups with others through delivering the

corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

REFERENCES

1. K. Kent and M. Souppaya. (1992). Guide to Computer Security Log Management, NIST Special Publication 800-92 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
2. U.S. Department of Health and Human Services. (2011, Sep.). HIPAA—General Information [Online]. Available: https://www.cms.gov/ hipaageninfo
3. PCI Security Standards Council. (2006, Sep.) Payment Card Industry (PCI) Data Security Standard—Security Audit Procedures Version 1.1[Online].Available:
4. https://www.pcisecuritystandards.org/pdfs/pci−audit−procedures−v1-1.pdf
5. http://www.tutorialspoint.com/uml/uml_overview.htm
6. http://townsendsecurity.com/products/encryption-and-tokenization/alliance-AES-encryption
7. Sarbanes-Oxley Act 2002. (2002, Sep.). A Guide to the Sarbanes-Oxley Act [Online]. Available: http://www.soxlaw.com/
8. A Practitioner's Guide to Software Test Design, Lee Copeland, 2003
9. C. Lonvick, The BSD SYSLOG Protocol, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.
10. SANS (2012), Cloud Security Fundamentals, Security 524, Volume 2, *Cloud Security*. The SANS Institute
11. William H. Mitchell Mitchell Software Engineering (.com)