International Journal of Science Engineering and Advance Technology

Elimination of De-duplication and Reduce Communication Overhead In Cloud

[1]P.NaveenKumar, [2]Nadella. Sunil
[1]FinalMaster of Science in Computer Science, Ideal college of Arts and Sciences, Vidyuth Nagar, Kakinada, East Godavari, AP, India
[2] Associate Professor, Department of Computer Science, Ideal college of Arts and Sciences, Vidyuth Nagar, Kakinada, East Godavari, AP, India

ABSTRACT:
We extend an attribute-based storage system with safe deduplication in a hybrid cloud setting, where a private cloud is accountable for duplicate detection and a public cloud manages the storage. Related with the prior data deduplication systems, our system has two compensations. It can be used to private portion data with users by agreeing access policies slightly distribution of decryption keys. It realizes the typical view of semantic security for data privacy while existing systems only accomplish it by critical and punier security notion. In adding, we set into view an organization to alter a cipher text over one starter policy into cipher texts of the equal plaintext but beneath other starter guidelines deprived of revealing the basic plaintext.

KEYWORDS: access policies, locked encryption, deduplication

1INTRODUCTION:
The usual Attribute Based Encryption system is ineffective to accomplish secure de duplication which is a system to excluding storage space and network bandwidth by refusing terminated copies of the encrypted data stored in the cloud. On the other hand, to the best of our knowledge, stand-up buildings for safe deduplication are not initiated on attribute-based encryption. Yet, since ABE and secure deduplication have been extensively efficient in cloud computing, it would be wanted to enterprise a cloud storage system having both goods. An encryption method that meets this requirement is called ABE, where a user's private key is linked with an attribute set, a message is encrypted under astarterpolicy over a set of attributes, and a user can decrypt a cipher text with his/her private key if his/her set of featuresplacates the starter procedureaccompanying with this cipher text.

2LITERATURE SURVEY:
Prior attribute-based encryption systems used attributes to label the encrypted data and constructed policies into user's keys; while in our system attributes are rummage-sale to label a user's credentials, and a gathering encrypting data controls a rule for who can decrypt. Thus, our methods are theoretically closer to old-style access control methods such as role-based access control (RBAC).

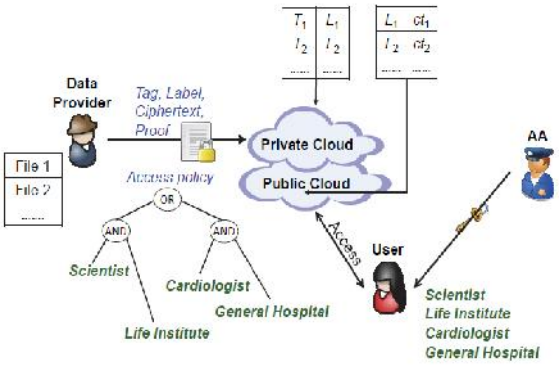
Though founded on convergent encryption, clouded up leftovers safe thanks to the meaning of a constituent that gears an extra encryption operation and an access switch mechanism. Also, as the obligation for deduplication at block-level raises a subject with admiration to key management, we propose counting a new constituent in order to tool the key management for each block composed with the real deduplication operation. We demonstrate that the overhead which was familiarized by these new machineries is trifling and does not influence the general stowage and computational charges.

3PROBLEM DEFINTION:
Upon getting a subcontracting appeal from a data provider for uploading a cipher text and a related tag, the cloud innings a so-called parity checking algorithm, which checks if the tag in the inward request is indistinguishable to any tags in the storage system. If there is a match, then the fundamental plaintext of this incoming cipher text has previously been stored and the new ciphertext is castoff. It seems that such a system with a tag attached to the cipher text does not offer the standard notion of semantic refuge for data privacy.

4PROPOSED APPROACH:
Theclassification is the major that reaches the average notion of semantic security for data privacy in attribute-based deduplication systems by resorting to the hybrid cloud building.Then, we placeout a practice to adapt a cipher textfinished one admission policy into cipher texts of the same plaintext but

below any other admittance policies lacking revealing the underlying plaintext.This method might be of autonomous interest in calculation to the application in the planned storage system.Thirdly, we offeratactic based on two cryptographic primitives, plus a zero-knowledge proof of facts and a vow scheme, to reach data uniformity in the system.

5SYSTEM ARCHITECTURE:



6PROPOSED METHODOLOGY:

6.1Data Provider:
Data provider uploading file to cloud with tag,label and securitykey for the wished-foroutline guarantees data veracitycontrary to any tag irregularity attack. Thus, haven is higher in the anticipatedoutline.

6.2Cloud Storage:
ProtectedDeduplication with thegoalmouth of valid storage space for cloud storage services, Douceur et al the first answer for complementaryprivacy and efficacy in accomplishment deduplication called convergent encryption, where a message is coded under a message-derived key so that undistinguishable plaintexts are coded to the same cipher texts.

6.3Deduplication:
Data deduplication is anexpert data densitymethod for removingidenticalreproductions of reiterating data. Connected and slightlyidentical terms are brightdensity and single-instance storing. This method is used to progress storage use and can also be functional to network data transfers to lessen the number of bytes that must be sent. In the deduplication development, exclusivelumps of data, or byte patterns, are branded and warehoused during a progression of analysis. Deduplication techniques take plus of data parallel to categorize the same data and condense the storage space.

6.4Attribute Authority:
The Attribute Authority subjectsalloperators a decryption key related with user set of attributes at the user side, all user can transfer an item, and decrypt the cipher text with the attribute-based private key made by the AA if this user's quality set contents the admissionconstruction.

7 SECURE CIPHERTEXT-POLICY ATTRIBUTE-BASED STORAGE ALGORITHM

Setup:
This setup algorithm hasproducts the public parameter pars and the master private key msk for the system.

KeyGen:
Taking the public parameter pars, the master private key msk and an attribute set **A** as the involvement, this attribute-based private key generation algorithm engenders an attribute built private key sk**A** for the attribute set **A**.

Encrypt:
Captivating the public parameter pars, a message M and an access structure A over the universe of attributes as the input, this encryption algorithm outputs a trapdoor key skT and a tuple CT. Both skT and CT are forwarded to the private cloud.

Validity Test:
Attractive the public parameter pars and a tuple CT as the input, this cogency testing algorithm analyzesCT and outputs 1 if pf is a lawfulresistant for or 0 thentrack by the private cloud.

Equality-Test:
Pleasing the public parameter pars and two tuples T1, L1, ct1 and T2, L2, ct2 as the input, this parity testing algorithm outputs 1 if both T1, L1, ct1, T2, L2, ct2 are made from the similarfundamental message or 0 otherwise run by the private cloud.

Re-encrypt:
Enchanting the public parameter pars, the trapdoor key skT, a tag and cipher text pair L, CT and acharge structure A0 as the input, this re-encryption algorithm manufactures a novelcipher text ct0 connected with A0 distribution the alike label L of the cipher text ct0 track by the private cloud.

Decrypt:
Enchanting the public parameter pars, a label and cipher text pair L; CT and an attribute-based private key sk**A** connected to an attribute set **A** as the input, this decryption algorithm productivitieseach the message M when the private key sk**A** mollifies the

entree structure of the cipher textCT and the label L is unswerving with M path by the operator.

8RESULTS:

MASTER SECRET KEY(MSK) USER REQUESTS

ID	User Name	Owner Name	File Name	Secret Key
1	Rajesh	Sukumar	Dengue.txt	Permitted
2	tmksmanju	Manjunath	Malaria.txt	Permitted
3	tmksmanju	Sukumar	Dengue.txt	Permitted
4	arun	sai	saifile.jsp	Permitted
5	teja	nav	nav.jsp	Give Permission

User Request for Master Key to access the File

CONTENT KEY USER REQUESTS

ID	User Name	Owner Name	File Name	Content Key
1	Rajesh	Sukumar	Dengue.txt	Permitted
2	tmksmanju	Manjunath	Malaria.txt	Permitted
3	tmksmanju	Sukumar	Dengue.txt	Permitted
4	arun	sai	saifile.jsp	Permitted
5	teja	nav	nav.jsp	Give Permission

User Request for Content Key to access the File

DOWNLOAD FILE

Role : (Doctor)

File Contents

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML
1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<%@page import ="java.util.*"%>
<%@page import ="java.sql.*"%>
<%@page import
="java.util.*,java.security.Key,java.util.
Random,javax.crypto.Cipher,javax.crypto.sp
ec.SecretKeySpec,org.bouncycastle.util.enc
oders.Base64"%>
<%@ page
import="java.sql.*,java.util.Random,java.i
o.PrintStream,java.io.FileOutputStream,jav
a.io.FileInputStream,java.security.DigestI
nputStream,java.math.BigInteger,java.secur
ity.MessageDigest,java.io.BufferedInputStr
```

Download

With the help of master key and content key User can download the file.

EXTENSION WORK:

In this scheme it encodes the File with Convergent Encryption using 256-bit AES algorithm in cipher block chaining mode, where the convergent key is from SHA-256 Hashing of the file which decreases message and totaling overhead and advances refuge and honesty?

9CONCLUSION:

Our storage scheme is constructedunderneath a hybrid cloud architecture, where a private cloud operates the calculation and a public cloud manages the storage. The private cloud is if with a trapdoor key allied with the corresponding cipher text, with which it can transmission the cipher text over one access rule into cipher texts of the identical plaintext under any other access policies deprived oflifealert of the original plaintext. After in receipt of a stowingdemand, the private cloud first checks the rationality of the uploaded item over the attached proof. If so, each time it is required, it revives the cipher text into a cipher text of the same plaintext over an access policy which is the unification set of both contactguidelines.

10REFERENCES:

[1] D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing/Elsevier,2014. [Online]. Available: http://www.elsevier.com/books/cloud-storageforensics/quick/978-0-12-419970-5

[2] K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography: Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[3] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics: State-of-the-art and future directions," Digital Investigation, vol. 18, pp. 77–78, 2016.

[4] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

[5] D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179– 193, 2014.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[7] B. Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneck in the data domain deduplication file system," in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 26- 29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[9] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, "Message-locked encryption for lock-dependent messages," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer, 2013, pp. 374–391.

[10] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. USENIX Association, 2013, pp. 179–194.

[11] M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in Public-Key Cryptography – PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 – April 1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol. 9020. Springer, 2015, pp. 516–538.

[12] S. Bugiel, S. N¨ urnberger, A. Sadeghi, and T. Schneider, "Twin clouds: Secure cloud computing with low latency - (full version)," in Communications and Multimedia Security, 12th IFIP TC 6 / TC 11 International Conference, CMS 2011, Ghent, Belgium, October 19- 21,2011. Proceedings, ser. Lecture Notes in Computer Science, vol. 7025. Springer, 2011, pp. 32–44.

[13] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems (extended abstract)," in Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA. ACM, 1985, pp. 291– 304.

[14] M. Fischlin and R. Fischlin, "Efficient non-malleable commitment schemes," in Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, ser. Lecture Notes in Computer Science, vol. 1880. Springer, 2000, pp. 413–431.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.

[16]Hui Cui, Robert H. Deng, Yingjiu Li, and Guowei Wu, Attribute-Based Storage Supporting Secure Deduplication Of Encrypted Data In Cloud,2017

Pantham NaveenKumar is a student of Ideal College of Arts and Science Kakinada. Presently he isin Final Masterof Science inComputer Science this college and affiliated to Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh. His area of interest includes Computer Networks and Object-Oriented Programming languages, all current trends and techniques in Computer Science.

Mr. Nadella Sunil,

Presently working as Director and AssociateProfessor in P.G. Department of ComputerScience, Ideal college of arts and Sciences,Kakinada.He obtained M.Sc., (Applied Mathematics) from Andhra University,M. Phil in Applied Mathematics from Andhra University and M. Tech(CSE) from University College of Engineering, JNTUK.Received Professor I. VenkataRayudu Shastabdi Poorthi Gold Medal,applied Mathematics Prize and T.S.R.K. Murthy Shastabdi Prize from Andhra University. Have Lecturer Ships in bothMathematical Sciences, Computer Sciences and Applications disciplines. Presently Pursuing Ph.D in Computer Science from JNTU Kakinada.