Applying Attribute - based Encryption to Eliminate Duplicate Copies of Identical Data in Cloud

[1]R. Jaswanth Kumar Reddy, [2]J. Rene Beulah, [3]M. Nalini,

[1]UG Scholar, [2,3]Assistant Professor,
Department of Computer Science and Engineering, Saveetha School of Engineering
Saveetha Institute of Medical and Technical Sciences, Chennai, India
[1]reddemjashwanthreddy@gmail.com, [2]renebeulah@gmail.com, [3]nalini.tptwin@gmail.com

Article Info
Volume 82
Page Number: 10579 - 10584
Publication Issue:
January-February 2020

Abstract

Abstract based cryptography (ABE) has been wide utilized in distributed computing any place an information provider redistributes his/her encoded information to a cloud specialist organization, and may impart the data to clients having specific qualifications (or properties). In any case, the quality ABE framework doesn't bolster secure deduplication that is urgent for wiping out copy duplicates of indistinguishable data in order to spare loads of room for putting away and arrange data measure. During this paper, we will in general blessing Associate in Nursing trait based stockpiling framework with secure deduplication in an extremely cross breed cloud setting, any place an individual cloud is responsible for copy discovery and an open cloud deals with the capacity. Contrasted and the past data deduplication frameworks, our framework has 2 advantages. Right off the bat, it might be wont to confidentially impart data to clients by indicating access strategies as opposed to sharing mystery composing keys. Also, it convey the goods the quality thought of phonetics security for data confidentiality while existing frameworks exclusively accomplish it by defining a more vulnerable security idea. Furthermore, we will in general spot forward a system to switch a ciphertext more than one access approach into ciphertexts of indistinguishable plaintext anyway underneath various access strategies while not uncovering the basic plaintext.

Keywords: *Attribute based cryptography, Deduplication, Cipertext, Plaintext.*

Article History
***Article Received**: 18 May 2019*
***Revised**: 14 July 2019*
***Accepted**: 22 December 2019*
***Publication**: 19 February 2020*

1. Introduction

Distributed computing is significantly encouraged information suppliers need to be relevant again without exposing their information with the cloud sensitive information to external parties special qualified clients to get selected to get information. It expects information convert to encoded structures to gain control tactics to the extent that no one can change clients with specific features (or accreditations) structures can disassemble scrambled Information. An encryption mechanism that meets this need this is called client-attribute-based encryption (ABE) private key quality set, associated with message encoded (or accessed) in an access strategy structure) can have many features and client decode the cipher using his / her private key the alignment of behaviors satisfies the threshold this is the approach to ciphering. However, makes standard ABE framework safe exclusion is one mechanism to prevent this extra room and system transfer speed by wiping repeated duplication of scrambled information away in the cloud. Again, as long as we can we know the current developments are safe the discount is not based on quality encryption. According to Bye, it is safe from ABE widely applicable to discount distribution computing and designing the distribution structure is attractive storage Framework with two features. We are consider the corresponding scenario of A supports the Asset-Based Stockpiling Framework secure exclusion of scraped information in cloud, in which the cloud does not store the file it can be multiple at one time duplicate of encoded equivalent file get involved in the arrangements. A bob, a distributor, hopes to upload a file cloud, and share M with specific users certifications. To do so, Bob M encodes most of the features below the entry strategy, and the corresponding cipher is forwarded to the cloud the ultimate goal of consolidated client adjustment properties that can fulfill the admission process disassemble the cipher. Later, another information supplier, Alice, transfers a cipher for this the equivalent base file M so far attributed is a alternative access settings A0. From the file transferred to the scratching structure, it cannot be clouded understand the plain text of Alice the cipher is similar to Bob, M stores twice. Such copying is obvious stockpiling destroys extra room and distance data transmission.

The paper is organized as follows: Section II tables some of the previous works are available in the literature. Section III provides a detailed description of the proposed work and its importance. Section IV compares the proposed method with the existing approaches in terms of storage complexity. Finally section V gives a brief conclusion.

2. Literature review

Nish ant et al. [1] discussed that distributed computing is very prevalent today as a result of huge measure of information stockpiling and quick access of information over the system. In any case, in today' s situation we locate the some issue to access and store information in cloud similarly information burglary, information misfortune, protection issue, tainted application, information area, security on seller level, security at client level and information duplication. As we find of late investigation 7 Zeta Byte (ZB) information accessible in various stockpiling area following 5 years it will expands the multiple times more information stockpiling. For the better execution of framework we utilize the various information deduplication technique loved particular execution situated information deduplication. In this paper we propose to expel information repetition from accessible disconnected or online information stockpiling just as we give security of information which improves the presentation of framework.

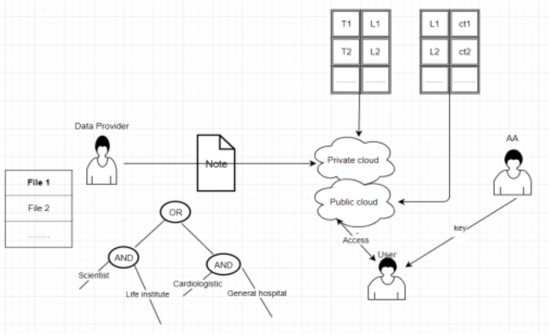
Ankit Srivastava et al. [2] discussed that the enormous information deduplication is one of the most testing errand in the cloud world. There are two significant issue created in the digital world initially is the information conservation on cloud and second one is huge duplication. In this examination proposed another model to take care of the two issues. In this paper proposed altered hash esteem idea, with the assistance of this maintain a strategic distance from enormous information issue and for secure information assurance use HECC calculation for information encryption and decoding. SHA2 calculation expend less time as contrast with SHA-1 for hash esteem age and HECC shows better encryption as contrast with different strategies. In this exploration additionally dissected the various techniques such AES, DSA and ECC for information encryption on the fundamental of time intricacy. The proposed framework shows better outcome as contrast with different past information duplication techniques for the premise of time and security.

Myungwanet al. [3] Scale-that-discussed distributed storage systems are kept in equilibrium information Growth in Capacity required performance. However, this is a challenge to store and manage huge content the information is created by the explosion. A of all the good solutions to reduce heavily data problems are data exclusion, that’s all removing redundant information on multiple nodes in the storage system [4]. However, it is unfair to use the traditional exclusionary style scale-storage due to the latter source reasons. First, not a chunk-lookup to find a discount basic storage as it is portable and long the system supports [5]. Second, it handles the data much is necessary in relation to reduction style size and implementation changes current distributed storage system [6]. Finally, the information processing and additional I / O traffic are mandatory removal can be significantly reduced performance of Scale-Up Storage. To deal with these challenges, we suggest an alternative discount method, that is serious flexible and compatible with current scale-up and storage [7]. Essentially, our discount method uses the double hashing principle using hashes with the underlying scale-in storage, which refers to boundaries current fingerprint hashing [8]. In addition, Ma style incorporates meta information classification system and one reduction object, which controls the amount of the discount online relationships by responding to the system supported post processing is required [9]. We are trending implemented a planned discount method connect Open Supply Scale to Storage. The experimental results show that our style is preserved the total volume of space is more than ninety store, many implementation below typical collection workload, a equivalent or similar performance compared to this Standard Scale-Up Storage [10].

3. Proposed System

In this paper, we present feature-based stockpiling framework for using cipher-setting behavior-based encryption (CP-ABE) supports secure exclusion. Our principle commitments can be formulated as follows.

Encryption is a method used to convert the plaintext or original message into an unintelligible text called ciphertext. Decryption is the reverse process in which the ciphertext is converted back to the plaintext. In other words, the original message is retrieved from the ciphertext. A key is used in both the steps.



The files are stored in cloud by the Data Provider. The Administrator is responsible for the authenticity and confidentiality of the information stored in cloud. The cloud may be a private one or public one. The user expects his data to be safe and secure so that unauthorized persons do not have any access to the information. When a person wants to access a document or file in the cloud, first he has to authenticate himself. Then the administrator will check whether he has the permission to read or edit the file. If he has permission he will be allowed to access. Otherwise he will be denied access and the file owner will be informed about the activity. All the files stored in cloud are in encrypted form. The encryption and decryption key are handled by the file owners and the administrator. The administrator is a third party who is a trusted party. This procedure involves the following steps which are mandatory. This is to ensure the safety of the documents stored in cloud.

a) First, the framework is important the basic idea of the semantic is fulfilled security for behavioral privacy discounts frameworks based on backlogs in Cloud Architecture [11].

b) Second, we came up with a strategy to change cipher for multiple access policy a cipher of equal plain text, however and in some other access settings finding the basic text [12]. Access control systems play an important role the role of cloud data security.

c) This method may have autonomy for an extension to the specified application stockpiling framework [13].

d) Third, we propose a based methodology zero information verification of information and two cryptographic locals the submission conspires to conspire, to fulfill information stability of the framework [14].

The scheme proposed appear to be promising. To prove the effectiveness of the approach, it is compared with an existing similar method and the results of comparison are discussed in the next section.

4. Results & Discussions

In existing methods, the main pitfall is that they do not meet the standard security rule for the primitive requirements. The proposed method overcomes those problems inherently as the input text is unguessable enough for penetrating [15].

Table 1: Computational overheads in Storage System

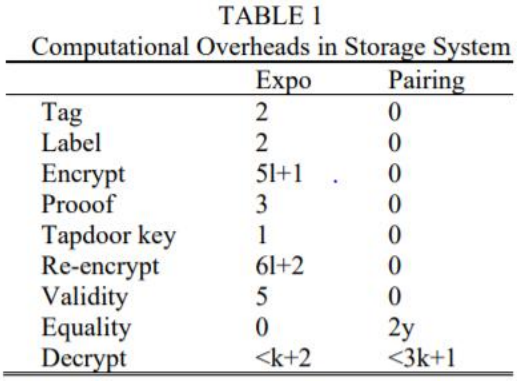


TABLE I
Computational Overheads in Storage System

	Expo	Pairing
Tag	2	0
Label	2	0
Encrypt	5l+1	0
Prooof	3	0
Tapdoor key	1	0
Re-encrypt	6l+2	0
Validity	5	0
Equality	0	2y
Decrypt	<k+2	<3k+1

A hybrid cloud setup is the optimal solution in which the information is first subjected to encryption, then it is outsourced to public cloud where it is verified for duplication which is taken care of by a private cloud.

Table 2: Comparison of Storage Complexity

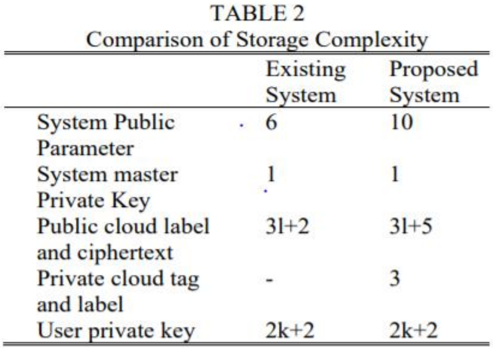


TABLE 2
Comparison of Storage Complexity

	Existing System	Proposed System
System Public Parameter	6	10
System master Private Key	1	1
Public cloud label and ciphertext	3l+2	3l+5
Private cloud tag and label	-	3
User private key	2k+2	2k+2

From the table it is very clear that the proposed system outperforms the existing system in all parameters. The accuracy and validity of the proposed system is verified which is straight forward. The approach seems to be an attractive and feasible solution for solving the issues in the problem domain.

5. Conclusion

Usually Attribute-Based Encryption (ABE) used in distributed computing suppliers re-distribute their scrambled information cloud also provides information to clients qualifications stated. Then again, exclusion is an important policy wxtra room and system transmission capability, whatever distribution with inseparable copy duplicates information. However, the standard ABE frameworks do not reinforce secure duplication, it does too much to apply to some businesses administration of storage. In this paper, we new ways to deal with awareness are presented behavior-based stockpiling framework supports secure exclusion. Our collection the framework works under the crossover cloud engineering, where private cloud is managed ability to count and open cloud handle. The trapdoor key has been assigned to the private cloud related to comparative ciphers, more than one access cipher can be moved access the cipher of equivalent plain text and in some other access settings noticing the hidden plaintext. Background capability Required, Private Cloud First confirms the legality of the transferred property connected testing. Event the evidence is legitimate and the private cloud maintains a label coordinates to see if the calculation is identical keep the basic cipher on the information far. However, suppose this is the case this is important, it gets the cipher back into the cipher plain text similar to the entry procedure this is an association set of two access strategies. The proposed stockpiling framework is worth two important priorities. To begin, it may very well be used differently to provide private information clients instead of determining access policy sharing the decoding key. Also, it fulfills the basic concept of semantic security right now discounted conspiracy a more fragile security idea.

References

[1] Michael Hange, Security Recommendations for Cloud Computing Providers, Federal Office for Information Security, 2010.

[2] Armbrust M, Fox A, Griffith R, Joseph A. D, Katz R. H, Konwinski A, Lee G, Patterson D. A, Rabkin A, Stoica I, and Zaharia M., “Above the clouds: A Berkeley View of Cloud Computing”, EECS Department, University of California, Berkeley, Technical Report, 2009, pp. 1-23.

[3] Zhang Q, Lu Cheng, and RaoufBoutaba, “Cloud Computing: State-of- the-Art and Research Challenges”, Springer Journal of Internet Service Application, Volume 1, Issue 1, 2010, pp. 7-18.

[4] K. Mahesh Babu and J. Rene Beulah (2019). “Air Quality Prediction based on Supervised Machine Learning Methods”, International Journal of Innovative and Exploring Engineering, vil. 8, Issue-9S4, pp. 206-212.

[5] A. Yaswanth Sai Raj and J. Rene Beulah (2019). “Securing Identification Card Against Unauthorized Access”, International Journal of Engineering and Advanced Technology, vol.8, Issue-3S, pp. 550-553.

[6] RajkumarBuyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg and IvonaBrandic, “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility”, Elsevier Science Publishers, Volume 25, Issue 6, 2009, pp. 599-616.

[7] BorkoFurht, “Cloud Computing Fundamentals”, Handbook of Cloud Computing, Chapter-1, Springer Science, Business Media, LLC, 2010, pp.1-17.

[8] Nalini, M. and Uma Priyadarshini, To Improve the Performance of Wireless Networks for Resizing the Buffer, Proceedings of the 2019 international IEEE Conference on Innovations in Information and Communication Technology, Apr 2019.[DOI >10.1109/ICIICT1.2019.8741406].

[9] J. Rene Beulah and D. Shalini Punithavathani (2017). “A Hybrid Feature Selection Method for Improved Detection of Wired/Wireless Network Intrusions”, Wireless Personal Communications, vol. 98, no. 2, pp. 1853-1869 (Springer).

[10] Nalini, M. and Anvesh Chakram, “Digital Risk Management for Data Attacks against State Evaluation”, Published in International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 8, Issue no. 9S4, pp. 197-201, July 2019.[DOI:10.35940/ijitee.I1130.0789S419]

[11] Kuyoro S. O., Ibikunle F. &Awodele O., Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume 3, Issue 5, 2011, pp. 247-255.

[12] Frank Gens, New IDC IT Cloud Services Survey: Top Benefits and Challenges, http://blogs.idc.com/ie/?p=730, December 15th, 2009.

[13] Nalini, M. and Anbu, S., “Anomaly Detection Via Eliminating Data Redundancy and Rectifying Data Error in Uncertain Data Streams”, Published in International Journal of Applied Engineering Research (IJAER), Vol. 9, no. 24, 2014.

[14] Peter Mell and Tim Grance, “The NIST Definition of Cloud Computing”, Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[15] Vaquero L M, Luis Rodero-Merino, Juan Caceres and Maik Lindner, “A Break in the Clouds: Towards a Cloud Definition”,ACM SIGCOMM Computer Communication Review, Volume 39, Issue 1, 2009, pp. 50-55.

[16] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, “An Analysis of Security Issues for Cloud Computing”, Journal of Internet Services and Applications, Springer- Verlag, Volume 4, Issue 1, 2013, pp. 1-12.

[17] V. Prasanna and Dr.M. Thangamani (2017), “Semi-Supervised Ensemble Graph Clustering and Fuzzy Membership Particle Swarm Optimization(FMPSO) based Feature Selection for Cancer Subtype Discovery”, Research Journal of Biotechnology, Special issue – August | ISSN: 0973-6263.

[18] Shanmugam Sai, R. and Nalini, M., Cooperative Quality Choice and Categorization for Multi label Soak Up Process, Proceedings of the 2019 international IEEE Conference on Innovations in Information and Communication Technology, Apr 2019. a[DOI > 10.1109/ICIICT1.2019. 8741469]