IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Enabling Efficient Consumer Revocation for Identity based Cloud Storage Auditing for Shared Big Data Records

Ayushi P Bohara[1*], Chethan A [2], Haripriya B [3], Harshitha V [4], Arun Biradar[5]

[1,2,3,4,5]Dept. of Computer Science ,East West Institute of technology, Vishveswaraya Technological University, Bangalore, India

DOI: https://doi.org/10.26438/ijcse/v7si15.2126 | Available online at: www.ijcseonline.org

Abstract: Cloud storage auditing schemes for shared facts refer with checking the integrity of cloud facts shared via a collection of customers.User revocation is commonly supported in such schemes, as customers may be issue to organization or may misbehave.Previously, the computational overhead for consumer revocation in such schemes was linear with the entire quantity of document blocks possessed by a revoked consumer. In this paper, we advise a singular storage auditing scheme that achieves consumer revocation unbiased of the full variety of file blocks possessed via the revoked consumer in the cloud. This is carried out through exploring a novel approach for key era and a brand new personal key replace method. By using this approach, we realize consumer revocation via simply updating the non revoked customers' personal keys rather than authenticators of the revoked consumer. The integrity auditing of the revoked consumer's data can nonetheless be efficaciously achieved when the authenticators aren't updated. Meanwhile, the proposed scheme is based totally on identification-base cryptography, which gets rid of the complex certificate control in conventional Public Key Infrastructure (PKI) structures. the safety and efficiency of the proposed scheme are confirmed through both evaluation and experimental consequences.

Keywords—Revocation,Key Generation,Cloud Computing.

I. INTRODUCTION

THE information sharing is a standout amongst the most broadly utilized administrations that the distributed storage gives. With information sharing administration, clients can impart their information in the cloud to a gathering of clients and diminish the weight of nearby information stockpiling. Clients, nonetheless, will lose the physical authority over their information when they share them in the cloud. Any mistake may make misfortune or harm the information [1]. So as to check the information trustworthiness, some distributed storage inspecting plans for shared information are proposed [2– 8]. At the point when a group user gets out of hand or leaves the group, the client ought to be revoked from the group. Inthis way, client renouncement is a typical reasonable need in distributed storage evaluating for shared information.

In distributed storage examining plans, the information proprietor needs to utilize his/her private key to produce authenticators(signatures) for record . These authenticators are utilized to demonstrate that the cloud genuinely has these record. At the point when a client is revoked, the client's private key ought to likewise be disavowed. For conventional distributed storage evaluating plans for offer information [2–5], all of authenticators created by the revoked client ought to be changed into the authenticators of one assigned nonrevoked bunch client. For this situation, this non-revoked bunch client needs to download all of denied client's records, re-sign these records, and transfer new authenticators to the cloud[6-8].When a client is revoked, the cloud will change the authenticators of the renounced client's squares into the authenticators of one non-repudiated bunch client comparing to these squares, with a re-marking key. The calculation overhead of client revocation is as yet straight with the absolute number of document squares put away by the revoked client in the cloud. In spite of the fact that this technique alleviates the weight on the non-revoked bunch client, it exchanges the weight to the cloud.

We build a novel distributed storage reviewing plan for shared information supporting genuine effective client revocation in this paper. So as to acknowledge proficient client revocation, we think of a novel methodology for key generation.We likewise propose a novel private key update strategy to help client revocation. At the point when clients are revoked from the group, the non-renounced clients can refresh their private keys by this strategy to make the distributed storage evaluating still work, while the personality data of the group does not have to change. Furthermore, the denied clients are not allowed to transfer information and authenticators to the cloud any more. Along

these lines, the majority of the authenticators produced before client revocation need not be recomputed. In this manner, the overhead of client revocation is completely autonomous of the absolute number of the revoked consumers. Even when the measure of information is massive, the group can easily complete user revocation in all respects productively.

The rest of this paper is organized as follows: In SectionII,we present related work. In Section III, we present the system model, the design goals,notations, definition and preliminaries. In Section III , we describe the proposed scheme. In Section IV we present the result and discussion and we give the security analysis and theperformance evaluation of our scheme. Finally,we conclude our paper in Section V.

II. RELATED WORK

Step by step instructions to guarantee the uprightness of re-appropriated information put away in the untrusted cloud is a hotly debated issue. Up to now, a ton of plans have been proposed dependent on different methods.Ateniese et al. [10] firstly proposed the notion of "Provable Data Possession" (PDP) based on homomorphic authenticators and sampling strategies. Juels et al. [11] proposed a "Proof of Retrievability" (PoR) model by using the tools of spot checking and error correcting codes to ensure both possession and retrievability of the data at untrusted servers. Shacham et al. [12] proposed a compact version of PoR, which efficiently realized public auditing based on the BLS short signature. To supportdynamic cloud data auditing, Ateniese et al. [13] proposed a novel dynamic PDP scheme. Wang et al. [14] proposed a full data dynamic auditing scheme by employing the Merkle Hash Tree. Later, some other cloud storage auditing schemes supporting datadynamics [15–19] were proposed sequentially. To protect the privacy of data, Wang et al. [20] proposed a publiccloud storage auditing scheme with data privacy preservation by utilizing random masking technique. To reduce the damage of key exposure in cloud storage auditing, Yu et al. [21–23] proposed cloud storage auditing schemes with key-exposure resilience by using key update technique [24, 25]. Some other cloud storage auditing schemes [26–28] have already been proposed.

The above plans are altogether founded on the PKI framework. PKI based distributed storage evaluating plans for the most part include confused declaration the board and endorsement confirmationThe information sharing is a generally utilized administration that the cloud capacity gives. User revocation is a realistic necessity in cloud storage auditing schemes for shared data. When a group user misbehaves or leaves the group, the user should be revoked from the group. Jiang et al. [34] proposed a shared data integrity auditing scheme with user revocation. However, the efficiency is low because the scheme is based on group signature. Wang et al. [6] firstlyproposed a cloud storage auditing scheme with user revocation based on the proxy re-signature technique.

In spite of the fact that the productivity of client denial has improved , the overhead ofclient denial is as yet direct with the quantity of the disavowed client's squares. When one appearances with substantial scale information, the client disavowal will bring about tremendous burden.

III. METHODOLOGY

A. System Model

The system model in our scheme includes five entities: the group user, the group manager, the cloud, the Private Key Generator (PKG), and the Third Party Auditor (TPA).

FIG: The system model

- **Group user**:There are numerous gathering clients in a cloud. Each gathering client can impart information to others through the distributed storage. Gathering clients can join or leave the group. The lawful gathering clients are straightforward and won't release any private data to other people.
- **Group Manager:** The group manager is a powerful entity. It can be viewed as an administrator of the group. When a user leaves the group, the manager is in charge of revoking this user. The revoked user cannot upload data to the cloud any more.
- **Cloud:** The cloud gives huge extra room what's more, registering assets for gathering clients. Through the cloud capacity, bunch clients can appreciatetheinformation sharingadministration.
- **PKG**:The PKG is trusted by different elements. It is in control of creating framework open parameters and the personality key of the gathering as per the gathering's personality (ID).
- **TPA:**The TPA is in charge of examining the honesty of cloud information in the interest of gathering clients. At the point when the TPA needs to review the information

uprightness, it will send an examining challenge to the cloud. In the wake of getting the inspecting challenge, the cloud will react to the TPA with a proof of information ownership. trustworthiness by checking the rightness of the file.

B. Design Goals

To guarantee efficient user revocation in identity-based cloud storage auditing for shared data, our planned plan should meet the accompanying objectives

- **Correctness**:to guarantee that the confirmation from the cloud can pass the TPA's approval, if the cloud, bunch clients, the gathering chief and the TPA are straightforward and comply with the specified methodology.
- **Soundness:** to guarantee that the cloud can't pass the TPA's verification on the off chance that it doesn't store bunch clients' unblemished information.
- **Secure user revocation:** to guarantee that the renounced clients can't transfer information and the comparing authenticators to the cloud any more.
- **Efficient user revocation:** to guarantee that the calculation overhead of client denial is totally autonomous of the absolute number of repudiated client's blocks.
- **Public auditing:**to guarantee that the TPA can check the trustworthiness of shared cloud information for the benefit of gathering clients

C. Algorithms

1. AES

KeyExpansion(byte key[4*Nk] , word w[Nb * (Nr +1)],Nk)

Begin

i=0

while (i<Nk)

w[i]=word[key[4*i],key[4*i+1],key[4*i+2],key[4*i+2]

i = i + 1

end while

i = Nk

while (i<Nb * (Nr + 1))

word temp = w[i- 1]

if (i mod Nk = 0)

temp = SubWord (RotWord(temp)) xorRcon[i/Nk]

else if (Nk = 8 and i mod Nk = 4)

temp = SubWord(temp)

end if

w[i] = w[i – Nk] xor temp

i = i + 1

end while

End

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respecti

2. DES

read Hamiltonian in input algebra

transform Hamiltonian to output algebra

apply symmetries

define generator scheme

define simplification rules

adjust simplification rules to minimal order 0

while new representatives in $H^{(0)}$:

run loop for all old generator representatives in$H^{(0)}$, all new observable representatives in $H^{(0)}$

run loop for all new generator representatives in $H^{(0)}$, all new observable representatives in $H^{(0)}$

end while

for m in (1,…., n) :

adjust simplification rules to minimal order m

for each block in ([$\eta^{(1)}$, $H^{(m-1)}$],….,[$\eta^{(m-1)}$, $H^{(1)}$]) :

run loop for all generator representatives in $\eta^{(\dots)}$,all new observable representatives in $H^{(\dots)}$

end for

while new representatives in $H^{(m \neq 0)}$:

run loop for all old generator representatives in $\eta^{(0)}$, all new observable representatives in $H^{(m)}$

run loop for all new generator representatives in$\eta^{(m)}$, all new observable representatives in $H^{(0)}$

end while

end for

output Hamiltonian and DES

DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintextmessage, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means of permutation and substitution. The process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks.

3. MD5

The MD5 hash is calculated according to this algorithm. All values are in little-endian

Step 1: Append padding bits

Step 2: Append length bit

Step 3 : Initialize MD buffer

- We use four 32 bit buffer

A=01234567

B=89ABCDEF

C=FEDCBA98

D=76543210

Step 4:Process message in 16-Word blocks

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.The MD5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures. MD5 has been deprecated for uses other than as a non-cryptographic checksum to verify data integrity and detect unintentional data corruption.The MD5 message digest hashing algorithm processes data in 512-bit blocks, broken down into 16 words composed of 32 bits each. The output from MD5 is a 128-bit message digest value.

IV. RESULTS AND DISCUSSION

This section deals with the performance of the proposed system that is being evaluated. The admin can only add or remove a group manager. The group manager can add and remove the group members. Whenever a user is added into agroup they are given a private key from which the particular user can upload or download a file. The system is independentof the number of revoked user's. This is because the files uploaded by theuser is stored in the cloudand hence more secure. Any user can access the files stored in cloud authenticated and uploaded by a revoked user. The group manager can add or delete the group user if the group manager thinks the group user is misbehaving. The revoked user can never access the content of the files or change the content of the file. The file once uploaded to the cloud is viewed in encrypted form so the user will not understand the content of the file.

Fig 4.1: Admin Login

Fig 4.3: Cloud Details

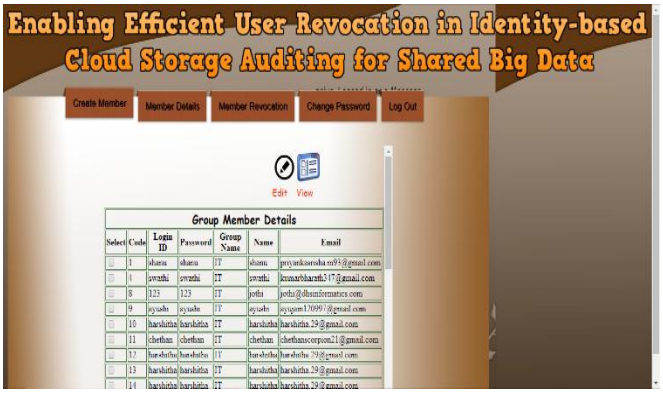

Fig 4.5 : Group Members

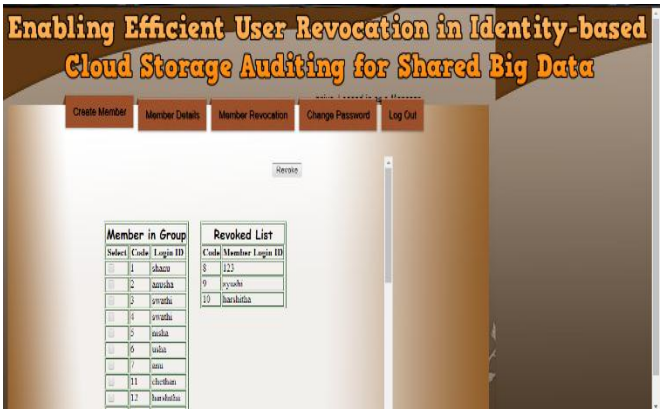

Fig 4.6: Revoke list

Fig 4.7: File upload process

Fig 4.8: Download process

V. CONCLUSION AND FUTURE SCOPE

This paper concludes that enabling efficient consumer revocation in identity based cloud storage auditing for shared big data records is a more secure approach for shared data records in the cloud. Once a user is added to a group and the user uploads a file it generates a signature through which integrity for the file is checked. The signature changes if the contents of the file uploaded is changed. This enables the misbehaviour of the file. Since our paper has the files encrypted the data integrity is ensured. The computation overhead due to user revocation is reduced due to the data being stored in the cloud. The file blocks being stored in the cloud is independent of the number of users revoked in the group.

REFERENCES

[1]. Hui Cui, Robert H Deng, Joseph K Liu, Xui Yi, " Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices" IEEE Transactions on Industrial Informatics, Volume: 14 , Issue: 8 , Aug. 2018

[2]. Suzuki T, Emura K, Ohigashi T, "A Generic Construction of Integrated Secure-Channel Free PEKS and PKE and its Application to EMRs in Cloud Storage" J Med Syst. 2019 Mar 28, vol 43(5):128.

[3]. Xing Q, Wang B, Wang X, Tao J, "Unbounded and revocable hierarchical identity-based encryption with adaptive security, decryption key exposure resistant, and short public parameters", 12 Apr 2018, vol 13(4), /journal pone.

[4]. G. Yang, J. Yu, W. Shen, Q. Su, F.Zhang, R Hao ,"Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability" ,April 2016

[5]. J. Yu, K.Ren, C. Wang,"Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates" , August 2016.

[6]. H. Wang , "Proxy provable data possession in public clouds" , vol. 113, pp. 130-139, 2016.

[7]. J. Yu, K. Ren, C. Wang, V. Varadharajan ,"Enabling cloud storage auditing with key-exposure resistance", 39(10), 9359–9366, Sept 2018.

[8]. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation," IEEE Trust com/Big DataSE /ISPA,pp. 434-442, 2015.

[9]. J. Yu, K. Ren, and C. Wang, "Enabling Cloud StorageAuditing with Verifiable Outsourcing of Key Updates,"IEEE Transactions

on Information Forensics and Security, vol. 11, no.5, pp. 1362-1375, 2016.
[10]. J. Yu and H. Wang, "Strong Key-Exposure ResilientAuditing for Secure Cloud Storage," IEEE Transactionson Information Forensics and Security, vol. 12, no.8, pp.1931-1940, 2017.
[11]. J. Yu, H. Rong, H. Xia, H. Zhang, X. Cheng, and F.Kong, "Intrusion-resilient identity-based signatures: Concrete scheme in the standard model and generic construction," Information Sciences, vol. 442-443, pp. 158-172, 2018.
[12]. J. Yu, R. Hao, H. Zhao, M. Shu, and J. Fan, "IRIBE:Intrusion-resilient identity-based encryption,"InformationSciences, vol. 329, pp. 90-104, 2016.
[13]. W. Shen, G. Yang, J. Yu , H. Zhang, F. Kong, and R. Hao, "Remote data possession checking with privacy-preserving authenticators for cloud storage," Future Generation Computer Systems, vol. 76, pp. 136-145, 2017.
[14]. F. FatemiMoghaddam, P. Wieder, and R. Yahyapour, "Federated PolicyManagement Engine for Reliable Cloud Computing," in IEEEInternational Conference on Ubiquitous and Future Networks (ICUFN2017*)*, 2017.
[15]. F. FatemiMoghaddam, P. Wieder, and R. Yahyapour, "PolicyManagement Engine (PME) - A Policy-Based Schema to Classify andManage Sensitive Data in Cloud Storages," J. Inf. Secur.Appl., vol. 36,pp. 11–19, 2017.
[16]. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu and R. Hao, "Light-weight and Privacy-preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium," Journal of Network and Computer Applications,vol. 82, pp.56-64, 2017.
[17]. M. Sookhak, A. Gania, M. K. Khanb, and R. Buyyac, "Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing," Information Science, vol.380, pp. 101-116, 2017.
[18]. L. Rao, H. Zhang, and T. Tu, "Dynamic Outsourced Auditing Services for Cloud Storage Based on Batch-Leaves- Authenticated Merkle Hash Tree," IEEE Transactions on Services Computing, Available online 26 May 2017 DOI:10.1109/TSC.2017.2708116.
[19]. J. Yu and H. Wang, "Strong Key-Exposure Resilient Auditing for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 12, no.8, pp. 1931-1940, 2017.

Authors Profile

*Ms.*Ayushi.P.Bohara studying in 8th sem CSE dept, EasT West Institute of Technology.Area of Intrests are cloud computing,Iot,big data

*Mr.*Chethan.A studying in 8th sem CSE dept, EasT West Institute of Technology.Area of Intrests are cloud computing,Iot,big data

*Ms.*Haripriya.B studying in 8th sem CSE dept, EasT West Institute of Technology.Area of Intrests are cloud computing,Iot,big data

Ms.Harshitha.V studying in 8th sem CSE dept, EasT West Institute of Technology.Area of Intrests are cloud computing,Iot,big data

Dr.Arun Biradar, He is currently working as head of department,Dept of Computer Science,East West Institute of Technology. He has presented more than 50 reference papers. . His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education.

