ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Method in Securing Shared Data in Public Cloud with User Revocation

K.Sai Kumar
Department of Computer Science and Engineering
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, RR. District, Hyderabad,
Telangana - 501301, India.

V.Sridhar Reddy
Department of Computer Science and Engineering
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, RR. District, Hyderabad,
Telangana - 501301, India.

ABSTRACT

With data storage and sharing services in the cloud, users can easily change and share data as a group. To secure/make sure of share data (honest and good human quality/wholeness or completeness) can be (checked for truth/proved true) publicly, users in the group need to figure out/calculate signatures on all the blocks in shared data. Different blocks in shared data are usually signed by different users due to data changes (sang, danced, acted, etc., in front of people) by different users. For security reasons, once a user is took back/taken back from the group, the blocks which were (before that/before now) signed by this took back/taken back user must be re-signed by an existing user. The straight forward method, which allows an existing user to download the almost the same part of shared data and re-sign it during user cancellation, is inefficient due to the large size of shared data in the cloud.

In this paper, we propose a novel public auditing (machine/method/way). For the (honest and good human quality/wholeness or completeness) of shared data with (producing a lot with very little waste) user cancellation in mind. By using the idea of substitute re-signatures, we allow the cloud tore-sign blocks for existing users during user cancellation, so that existing users do not need to download and re-sign blocks by themselves. Also, a public verifier is always able to audit the (honest and good human quality/wholeness or completeness) of shared data without retrieving the whole data from the Cloud, even if some part of shared data has been re-signed by the cloud. More than that, our (machine/method/way) can support batch auditing by (checking for truth/proving true) multiple auditing tasks (at the same time).

Experimental results show that our (machine/method/way) can very much improve the (wasting very little while working or producing something) of user cancellation.

INTRODUCTION

WITH data storage and sharing services (such as Drop box and Google Drive) given by the cloud, people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the cloud, every user in the group can not only access and change shared data, but also share the latest version of the shared data with the rest of the group[1]. Although cloud providers promise a more secure and reliable (surrounding conditions) to the users, the (honest and good human quality/wholeness or completeness) of data in the cloud may still be damaged/be broken into, due to the existence of hardware/software failures and human errors. To protect the (honest and good human quality/wholeness or completeness) of data in the cloud, number of (machines/methods/ways) have been proposed. In these (machines/methods/ways), a signature is attached to each block in data, and the (honest and good human quality/wholeness or completeness) of data depends on the correctness of all the signatures. One of

Cite this article as: K.Sai Kumar & V.Sridhar Reddy, "A Novel Method in Securing Shared Data in Public Cloud with User Revocation", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 4 Issue 11, 2017, Page 449-458.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the most significant and common features of these (machines/methods/ways) is to allow a public verifier to (in a way that produces a lot with very little waste) check data (honest and good human quality/wholeness or completeness) in the cloud without downloading the whole data, referred to as public auditing (or represented as Provable Data Possession). This public verifier could be a client who would like to use cloud data for particular purposes (e.g., search, computation, data mining, etc.) or a third party person (who carefully checks business records) (TPA) [3-5] who can provide checking (for truth) services on data (honest and good human quality/wholeness or completeness) to users.

Most of the previous works focus on auditing the (honest and good human quality/wholeness or completeness) of personal data. Different from these works, (more than two, but not a lot of) recent works focus on how to preserve identity privacy from public verifiers when auditing the (honest and good human quality/wholeness or completeness) of shared data. Unfortunately, none of the above (machines/methods/ways), thinks about/believes the (wasting very little while working or producing something) of user cancellation when auditing the correctness of shared data in the cloud [7].

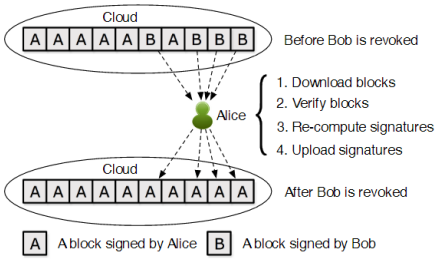


Fig. 1. Alice and Bob share data in the cloud. When Bob is revoked, Alice re-signs the blocks that were previously signed by Bob with her private key.

With shared data, once a user changes a block, she also needs to figure out/calculate a new signature for the changed block. Due to the changes from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be taken back from the group. As a result, this took back/taken back user should no longer be able to access and change shared data, and the signatures created by this took back/taken back user are no longer valid to the group. Therefore, although the content of shared data is not changed during user cancellation, the blocks, which were (before that/before now) signed by the took back/taken back user, still need to be re-signed by an existing user in the group. As a result, the (honest and good human quality/wholeness or completeness) of the whole data can still be (checked for truth/proved true) with the public keys of existing users only [9].

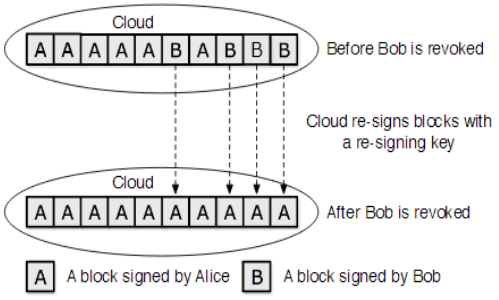


Fig. 2. When Bob is revoked, the cloud re-signs the blocks that were previously signed by Bob with a re-signing key.

Since shared data is (paid someone else to do something) to the cloud and users no longer store it on local devices, a straight forward method to re-figure out/calculate these signatures during user cancellation (as shown in Fig. 1) is to ask an existing user (i.e., Alice) to first download the blocks (before that/before now) signed by the took back/taken back user (i.e., Bob), (check for truth/prove true) the correctness of these blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. However, this plain/honest/easy method may cost the existing user a huge amount of communication and computation useful things/valuable supplies by downloading and (checking for truth/proving true) blocks, and by re-figuring out/calculating and uploading signatures, especially when the number of re-signed blocks is quite large or the membership of the group is often changing [2]. To make this matter even worse, existing users may access their data sharing services done by the cloud with useful thing/valuable supply limited devices, such as mobile phones, which further prevents existing users from maintaining the correctness

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

of shared data (in a way that produces a lot with very little waste) during user cancellation [4].

EXISTING SYSTEM

An existing system the file uploaded in cloud which not signed by user in each time of upload. So that (honest and good human quality/wholeness or completeness) of shared data is not possible in existing system. However, since the cloud is not in the same trusted domain with each user in the group, (paying someone else to do something) every user's private key to the cloud would introduce significant security issue [6].

PROPOSED SYSTEM

Proposed system may lie to verifiers about the wrongness of shared data in order to save the reputation of its data services and avoid losing money on its data services. Also, we also assume there is no secret crime-planning between the cloud and any user during the design of our (machine/method/way). Generally, the wrongness of share data under the above semi trusted model can be introduced by hardware/software failures or human errors happened in the cloud. (thinking about/when one thinks about) these factors, users do not fully trust the cloud with the (honest and good human quality/wholeness or completeness) of shared data [8].

ADVANTAGES

- Blocking User account
- Security question
- Login with secret key in each time

SYSTEM ARCHITECTURE

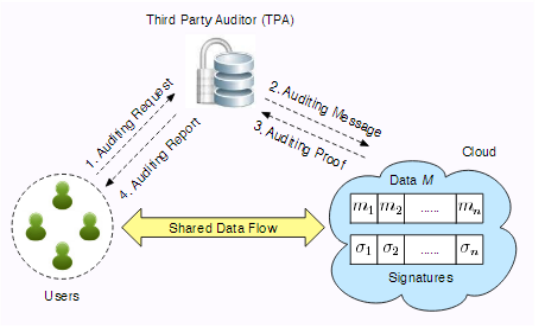


Fig. 3. The system model includes the cloud, the TPA, and users.

SYSTEM OVERVIEW:

The system model includes three things/businesses: the cloud, the third party person (who carefully checks business records) (TPA), and users who share data as a group (as illustrated in Fig. 3). The cloud offers data storage and sharing services to users. The TPA can publicly audit the (honest and good human quality/wholeness or completeness) of shared data in the cloud for users. In a group, there is one original user and some group users. The original user is the original owner of data. This original user creates and shares data with other users in the group through the cloud. Both the original user and group users can access, download and change shared data [10].

Shared data is further divided into some blocks. A user can change a block in shared data by (doing/completing) an insert, delete or update operation on the block. Generally, the (honest and good human quality/wholeness or completeness) of shared data is threatened by three factors. First, the (computer service another company does for you over the Internet) provider may accidentally and carelessly (add unwanted things to/make dirty) shared data due to hardware/software failures and human errors. Second, an external enemy may try to dishonest (in a way that ruins your trust) shared data in the cloud, and prevent users from using shared data correctly. Third, a took back/taken back user, who no longer has the right as existing users, may try to illegally change shared data. (thinking about/when one thinks about) these threats, users do not fully trust the cloud with the (honest and good human quality/wholeness or completeness) of shared data. To protect the (honest and good human quality/wholeness or completeness) of shared data, each block in shared data is attached with a signature, which is figured out/calculated by one of the users in the group. When shared data is, at first, created by the original user in the cloud, all the signatures on shared data are figured out/calculated by the original user. After that, once a user changes a block, this user also needs to sign the changed block with his/her own private key. By sharing data among a group of users, different blocks may be

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

signed by different users due to changes from different users. When a user in the group leaves or misbehaves, the group needs to take back this user. Generally, as the creator of shared data, the original user acts as the group manager and can take back users for the group. Once a user is took back/taken back , the signatures figured out/calculated by this took back/taken back user become invalid to the group, and the blocks that were (before that/before now) signed by this took back/taken back user need to be re-signed by an existing user, so that the correctness of the whole data can still be (checked for truth/proved true) with the public keys of existing users only. Note that allowing every user in the group to share acommon group private key and sign each block with it, is also a possible way to protect the (honest and good human quality/wholeness or completeness) of shared data. However, when a user is took back/taken back from the group, a new group private key needs to be securely distributed to every existing user andall the blocks in the shared data have to be re-signed with the new private key, which increases the complex difficulty of very important management and affects the (wasting very little while working or producing something) of user cancellation [13].

Design Goals

To correctly (check for truth/prove true) the (honest and good human quality/wholeness or completeness) of shared data with (producing a lot with very little waste) user cancellation, our public auditing (machine/method/way) should (accomplish or gain with effort) the following properties:

(1) Correctness: The TPA can correctly check the (honest and good human quality/wholeness or completeness) of shared data.

(2) Efficient and Secure User Revocation: On one hand, once a user is took back/taken back from the group, the blocks signed by the took back/taken back user can be (in a way that produces a lot with very little waste) re-signed. On the other hand, only existing users in the group can create valid signatures on shared data, and the took back/taken back user can no longer figure out/calculate valid signatures on shared data.

(3)Public Auditing: The TPA can audit the (honest and good human quality/wholeness or completeness) of shared data without retrieving the whole data from the cloud, even if some blocks in shared data have been re-signed by the cloud [15].

IMPLEMENTATION

MODULE:

- Data Owner (Group Member)
- Cloud Server
- ProxyServer
- Data Integrity
- Public Verifier
- DataConsumer(End-User/Group Member)

MODULES DESCRIPTION:

Data Owner (Group Member)

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner (turns into secret code) the data file and then store in the cloud. The Data owner can have capable of controlling/moving around/misleading the secret/unreadable data file.

Cloud Server

The (computer service another company does for you over the Internet) provider manages a cloud to provide data storage service [11]. Data owners (turn into secret code) their data files and store them in the cloud for sharing with data people (who use a product or service). To access the shared data files, data people (who use a product or service) download (turned into secret code) data files of their interest from the cloud and then (change secret codes into readable messages) them.

ProxyServer

The (related to being a substitute for someone or something) Server manages all data forwards to (computer service another company does for you over the Internet) provider and if there is any un matching key then it will sent to public Verifier to take back the user details.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data (honest and good human quality/wholeness or completeness)

Data (honest and good human quality/wholeness or completeness) is very important in (computer file full of information) operations in particular and Data warehousing and Business intelligence in general. Because Data (honest and good human quality/wholeness or completeness) secured/made sure of that data is of high quality, correct, consistent and (easy to get to, use, or understand) [12].

Public Verifier

The Public Verifier will (sing, dance, act, etc., in front of people) the cancellation and un cancellation of the remote user if he is the attacker or evil and cruel user over the cloud data.

Data Person (who uses a product or service) (End User / Group Member)

In this module, the user can only access the data file with the secret/unreadable combined key if the user has the privilege to access the file.

PERFORMANCE

We first discuss the communication and computation cost of our (machine/method/way). Then we (figure out the worth, amount, or quality of) the performance of our (machine/method/way) in experiments [14].

A. Communication Cost

the size of an auditing message $\{(l, yl)\}l\in L$ is $c.(|n| +|q|)$bits, where c is the number of selected blocks, $|n|$is the size of an element of set $[1, n]$ and $|q|$is the size of an element of Zq. The size of an auditing proof $\{\alpha,\beta, \{idl\}l\in L\}$ *is* $2d \cdot |p|+c(|id|)$ bits, where d is the number of existing users in the group, |p|is the size of an element of *G1 or Zp*, $|id|$is the size of a block identifier. Therefore, the total communication cost of an auditing task is $2d \cdot |p| + c \cdot (|id| + |n| + |q|)$bits.

B. Computation Cost

As shown in **ReSign [16]** of our mechanism, the cloud first verifies the correctness of the original signature on a block, and then computes a new signature on the same block with a re-signing key.

The computation cost of re-signing a block in the cloud is *2ExpG1 +MulG+2Pair+HashG1*, where *Exp*G1 denotes one exponentiation in *G1*, *MulG1*denotes one multiplication in *G1*, Pair denotes one pairing operation one$G1\times G1 \rightarrow G2$, and *Hash*G1 denotes one hashing operation in *G1*. The cloud can further reduce the computation cost of the re-signing on a block to ExpG1 by directly re-signing it without verification [7].

The public auditing performed by the TPA ensures that the re-signed blocks are correct. Based on Equation, the computation cost of an auditing task in our mechanism is *(c+d) ExpG1+(c+2d)MulG1+(d+1)Pair+dMulG2 + cHashG1*.

C. Experimental Results

We evaluate the performance of our mechanismin experiments. We utilize Pairing Based Cryptography Library (PBC)1 to implement cryptographic operations in our mechanism. All the experiments are tested under Ubuntu withan Intel Core i5 2.5GHz Processor and 4GB Memory over1, 000 times. In the following experiments, we assume the size of an element of *G1orZp is* $|p|=160bits$, the size of an element of *Zq* is |q|=80bits, the size of a block identifier is|id|=80 bits, and the total number of blocks in shared data is n=1,000,000. By utilizing aggregation methods from the size of each block can be set as 2KB, then the total size of shared data is 2GB.

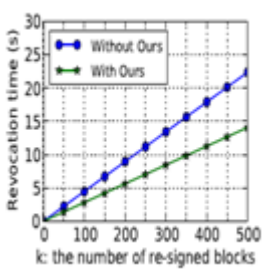
1).Performance of User Revocation:

As introduced in Section I, the main purpose of our (machine/method/way) is to improve the (wasting very little while working or producing something) of user cancellation. Without our (machine/method/way), to take back a user in the group, an existing user needs to download the blocks were (before that/before now) signed by the took back/taken back user, (check for truth/prove true) the correctness of these blocks, re-figure out/calculate signatures on these blocks and upload the new signatures. In this experiment, we

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

assume the download speed and upload speed for the data storage and sharing services is 1Mbps and 500Kbps, (match up each pair of items in order). We also assume the cloud and an existing user power/advantage the same type of machine (Intel Core i5 2.5GHz Processor and 4GB Memory) to (do/complete) user cancellation. Let k represent the number of re-signed blocks during user cancellation. The performance of our (machine/method/way) during user cancellation is presented in Figure. The cloud can not only (in a way that produces a lot with very little waste) re-sign blocks but also save existing users' computation and communication useful things/valuable supplies. As shown in Figure, when the number of re-signed blocks is 500, which is only 0.05% of the total number of blocks, the cloud in our (machine/method/way) can re-sign these blocks within 15 seconds. In contrast, without our (machine/method/way), an existing user needs about 22 seconds to re-sign the same number of blocks by herself.

Besides, the 500 re-signed blocks that this existing user downloaded costs her extra radio frequency/ability during user cancellation. Both of the two cancellation time are linearly increasing with an increase of k--the number of re-signed blocks. Since we assume the cloud and an existing user have the same level of computation useful thing/valuable supply in this experiment, it is easy to see that the gap in terms of cancellation time between the two lines in Figure is mainly introduced by downloading the re-signed blocks. In a practical cloud (surrounding conditions), the cloud should have more powerful computation abilities than personal devices, which allows the cloud to finish the re-signing on data even sooner [9].



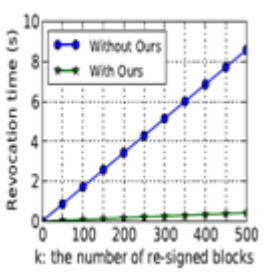


Fig.4.Impact of k on revocationFig.5.Impact of k on revocation time(s) time without verification(s).

Also, as we analysed before, the cloud can even directly re-sign data without checking (for truth), which can further improve the (wasting very little while working or producing something) of re-signing about 100 times. More specifically, the re-signing time on one block with checking (for truth) is 28.19 milliseconds while the one without checking (for truth) is only 0.28 milliseconds.

Note that due to the existence of transmission errors in networks, it is not a good idea to allow an existing user to re-sign the blocks without (checking for truth/proving true) them. Even if an existing user directly re-signs the blocks without checking (for truth), compared to our (machine/method/way), this user still needs to spend some extra time to download the blocks. As illustrated in Fig.4.When the number of re-signed blocks is still 500, the cloud in our (machine/method/way) can re-sign these blocks in about 0.14 seconds; while an existing user needs about 8.43 seconds by herself.

With the comparison between Fig.4 and Fig.5, we can see that the checking (for truth) on original signatures before re-signing is one of the main factors that can slow down the whole user cancellation process. Meanwhile, as shown in Fig.4 and Fig.5, the key advantage of our (machine/method/way) is that we can improve the (wasting very little while working or producing something) of user cancellation and release existing users from the communication and computation heavy load introduced by user cancellation.

2) Performance of Auditing:

We can see from Fig.6 and Fig.7 that, in order to maintain a higher detection chance, a verifier needs more time and communication overhead to finish the auditing job on shared data. Meanwhile, the auditing time (the time that the TPA needs to (check for truth/prove true) the correctness of an auditing proof based on Equation is linearly increasing with the number of existing users in the group. Our (machine/method/way) allows a verifier to (in a way that produces a lot with very little waste) audit the correctness of shared data without retrieving the whole data from the cloud. More specifically, when

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

c=460 and d=10, the communication cost of an auditing job (the communication cost that the TPA needs/demands during an auditing task) is about 11.9KB, and the auditing time of the whole data is only about 300 milliseconds [12]

With the comparison between Fig.4 and Fig.5, we can see that the checking (for truth) on original signatures before re-signing is one of the main factors that can slow down the whole user cancellation process. Meanwhile, as shown in Fig.4 and Fig.5, the key advantage of our (machine/method/way) is that we can improve the (wasting very little while working or producing something) of user cancellation and release existing users from the communication and computation heavy load introduced by user cancellation.

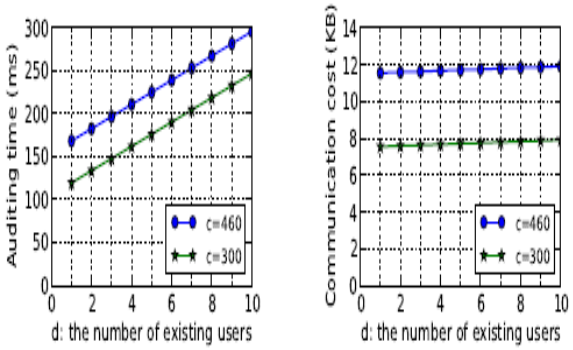
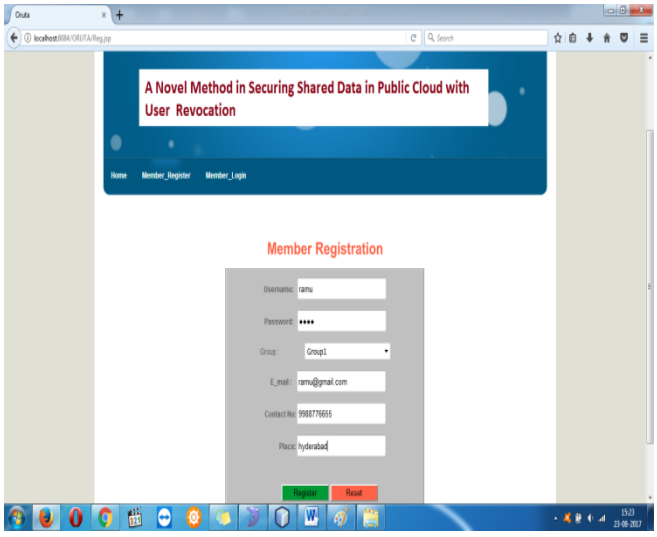
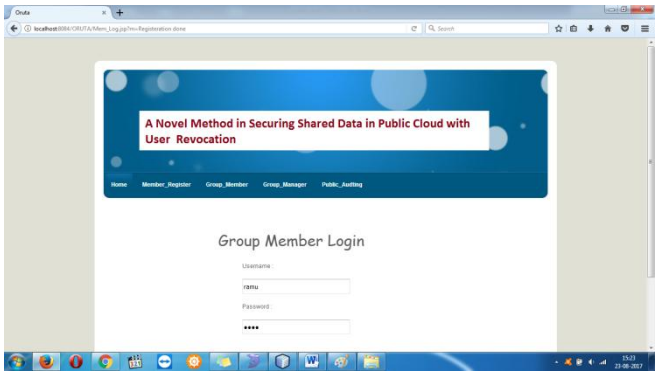
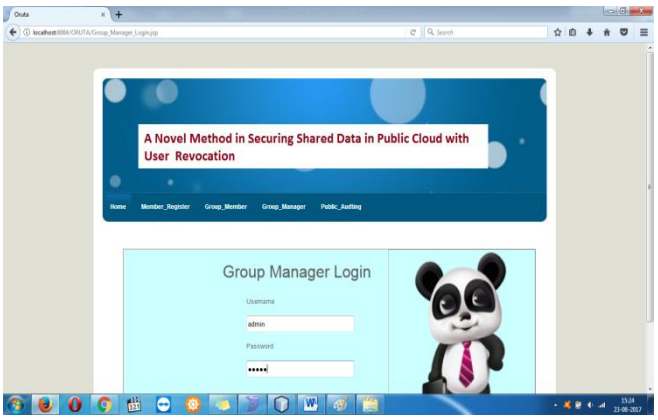


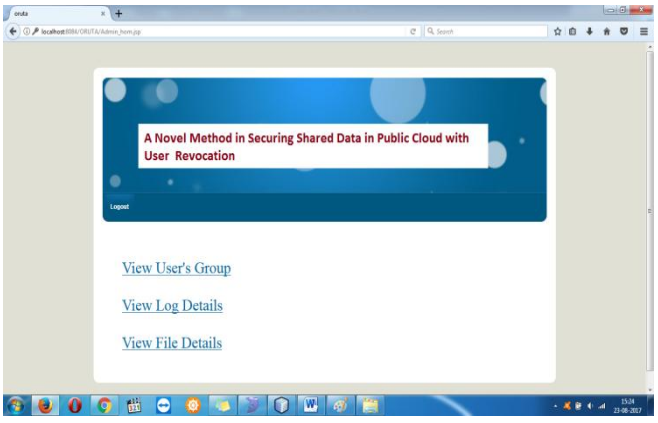
Fig.6.Impact of d on auditing communicationtime(ms). Fig.7.Impact of d on cost (KB).

Screen Shots

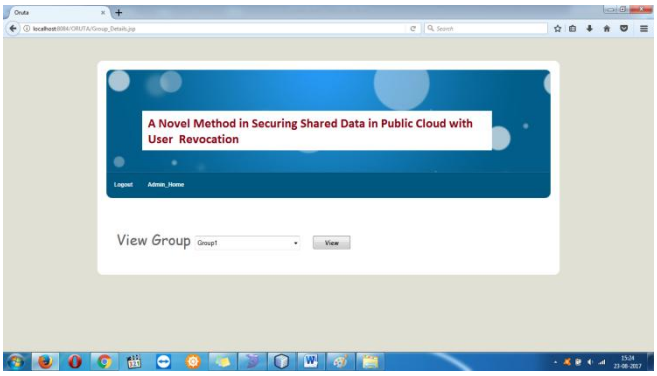


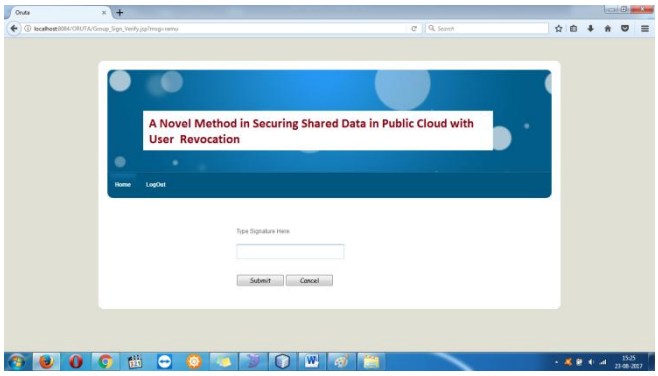


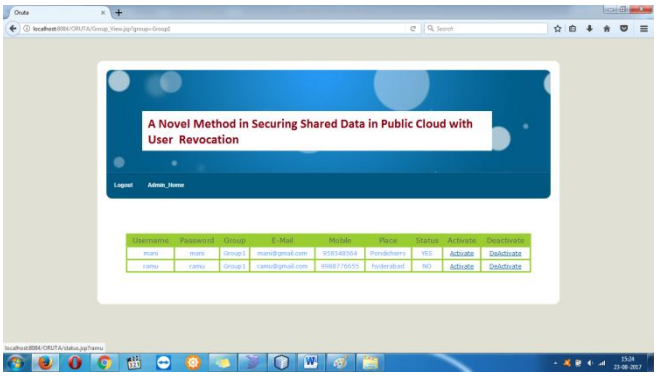


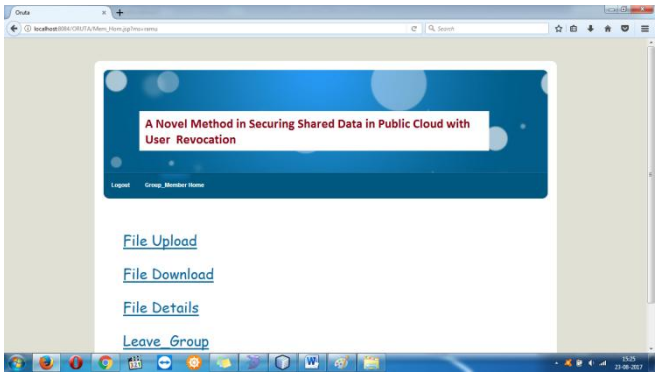


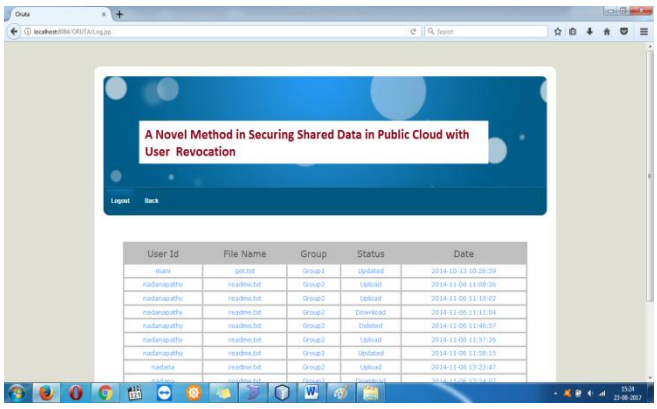
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

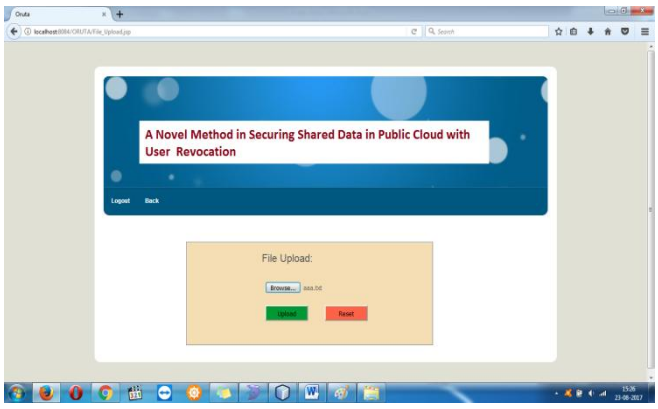


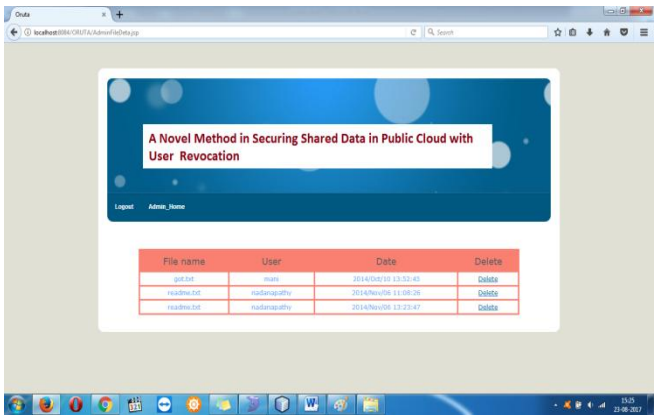




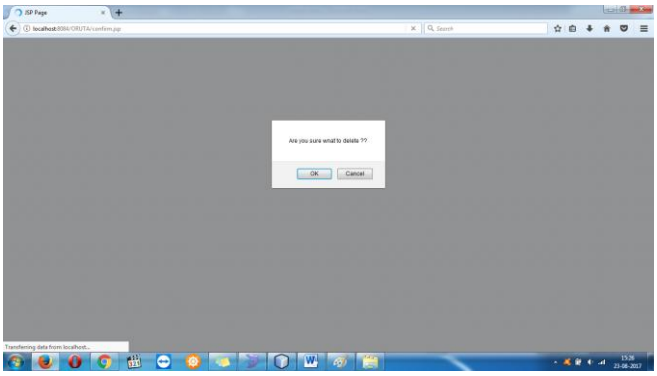








ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



CONCLUSION

In this system, we proposed a new public auditing (machine/method/way) for shared data with (producing a lot with very little waste) user cancellation in the cloud. When a user in the group is took back/taken back, we allow the semi-trusted cloud to re-sign blocks that were signed by the took back/taken back user with (related to being a substitute for someone or something) re-signatures. Experimental results show that the cloud can improve the (wasting very little while working or producing something) of user cancellation, and existing users in the group can save a big amount of computation and communication useful things/valuable supplies during user cancellation.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revoation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.

[8] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.

[10] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted.

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.

[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[13] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.

[14] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud," in the Proceedings of IEEECloud 2012, 2012, pp. 295–302.

[15] S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-user DynamicProofs of Data Possession Using Trusted Hardware," inProceedings of ACM CODASPY'13, 2013, pp. 353–364.

[16] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing forShared Data with Large Groups in the Cloud," in the Proceedingsof ACNS 2012, June 2012, pp. 507–525.