iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6255

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

Efficient Revocation of Untrusted User in Identity based Cloud Storage System for Shared Big Data

Manjunatha B S[1], Asst.Prof. Latha A[2]
[1]*P. G Student, Department of Computer Science and Engineering, SCE, Bangalore, Karnataka*
[2] *Assistant Professor, Department of Computer Science and Engineering, SCE, Bangalore, Karnataka*

Abstract: Cloud storage is a system which stores the digital data into logical pools .The providers of cloud storage has to enable the accessing of data's stored in it.
The data stored in cloud can be analysed systematically and information can be extracted. The auditing process for data refer to checking the integrity of data stored in cloud shared by a group of users. User revocation is difficult in cloud as other users may share common attributes among them.
This revocation is commonly supported in schemes, as users may be eligible for group membership. Previously, the computational overhead for revocating user in such schemes is linear. The overhead becomes a burden because of the large amount of the data stored in cloud. Thus, overhead can be reduced by user revocation as this process becomes a major challenge practically. In this study, a novel approach of auditing process that achieves high user revocation efficiently in the cloud has been proposed.
This is achieved by generating a key and a new private key update technique. Using this technique, user revocation is realized by just updating the non-revoked group users' private keys rather than authenticators of the revoked user. Meanwhile, the proposed scheme is based on identity-base cryptography that eliminates the certificate management which is complicated in traditional Public Key Infrastructure (PKI) systems.
Keywords: Cloud computing, Encryption, Decryption, Auditing, private key generation, Revocation.

I. INTRODUCTION

The information sharing is a here among the most all things considered utilized associations that the appropriated storing gives. With information sharing association, clients can give their information in the cloud to a social gathering of clients, and decay the largeness of near to information hoarding.
Clients, regardless, will lose the physical power over their information when they share them in the cloud. Any goof (the nonattendance of regard of human or the disappointment of equipment/programming) may make misfortune or naughtiness the information.
To check the information respectability, some coursed amassing dissecting plans for shared information are proposed. Precisely when a get-together client escapes hand or leaves the social affair, the client ought to be denied from the party. All things considered, client refusal is an average sensible need in scattered limit examining for shared information.
In passed on accumulating looking over plans, the information proprietor needs to utilize his/her private key to convey authenticators (marks) for file squares. These authenticators are utilized to demonstrate that the cloud genuinely has these record squares.
Right when a client is denied, the client's private key ought to comparatively be repudiated. For standard flowed accumulating taking a gander at plans for offer information , all of authenticators made by the denied client ought to be changed into the authenticators of one designated non revoked absolute client. For this situation, this non-denied gather client needs to download all of revoked client's squares, re-sign these squares, and trade new authenticators to the cloud. Indisputably, it costs enormous extent of calculation asset and correspondence asset in perspective on the immense size of shared information in the cloud.

II. LITERATURE SURVEY

K.Ren [1] proposed a passed on handling tends to the present most empowering figuring change in setting in data headway. In any case, security and confirmation are seen as key tangles to its wide allocation. Here, the creators plan several principal security difficulties and push further examination of security answers for a solid open cloud condition.

B.Wang [2] proposed as cloud information associations, it is typical for information to be verified in the cloud, yet moreover shared over various clients. Lamentably, the uprightness of cloud information is in danger to caution because of the proximity of equipment/programming thwarted expectations and human goofs. Several sections have been proposed to permit the two information proprietors and open verifiers to productively study cloud information validity without recovering the whole information from the cloud server.

All things considered, open investigating on the uprightness of offered information to these present structures will uncover secret data—character security—to open verifiers. In this paper, we propose a novel protection ensuring instrument that underpins open analyzing on shared informational index away in the cloud. Specifically, we misuse ring engravings to figure assertion metadata expected to review the rightness of shared information

B.Wang [3] gave a data amassing and sharing organizations in the cloud, customers can without a lot of a stretch modify and offer data as a social affair.

To ensure shared data decency can be affirmed straightforwardly, customers in the get-together need to figure blemishes on all of the squares in shared data. Different squares in shared data are normally set apart by different customers due to data modifications performed by different customers. For security reasons, when a customer is denied from the social event, the squares which were as of late set apart by this repudiated customer must be re-set apart by a present customer.

III. METHODOLOGY

System design is the process of defining the architecture, components, modules, interfaces and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. If the broader topic of product development "blends the perspective of marketing, design, and manufacturing into a single approach to product development," then design is the act of taking the marketing information and creating the design of the product to be manufactured. Systems design is therefore the process of defining and developing systems to satisfy specified requirements of the user.it is shown in the below fig 1

A. Requisites Accumulating and Analysis

It’s the first and foremost stage of the any project as our is an academic leave for requisites amassing, we followed of IEEE Journals and Amassed so many IEEE Relegated papers and final culled a paper designated by setting and substance importance input and for analysis stage we took references from the paper and did literature survey of some papers and amassed all the requisites of the project in this stage.

B. System Design

In System Design has divided into three types like GUI Designing, UML Designing with avails in development of project in facile way with different actor and its utilizer case by utilizer case diagram, flow of the project utilizing sequence, Class diagram gives information about different class in the project with methods that have to be utilized in the project if comes to our project our UML Will utilizable in this way The third and post import for the project in system design is Data base design where we endeavor to design data base predicated on the number of modules in our project.

C. Implementation

The Implementation is Phase where we endeavor to give the practical output of the work done in designing stage and most of Coding in Business logic lay coms into action in this stage its main and crucial part of the project.

D. Testing

It is done by the developer itself in every stage of the project and fine-tuning the bug and module predicated additionally done by the developer only here we are going to solve all the runtime errors.

As our Project is academic leave, we can do any automatic testing so we follow manual testing by endeavour and error methods.

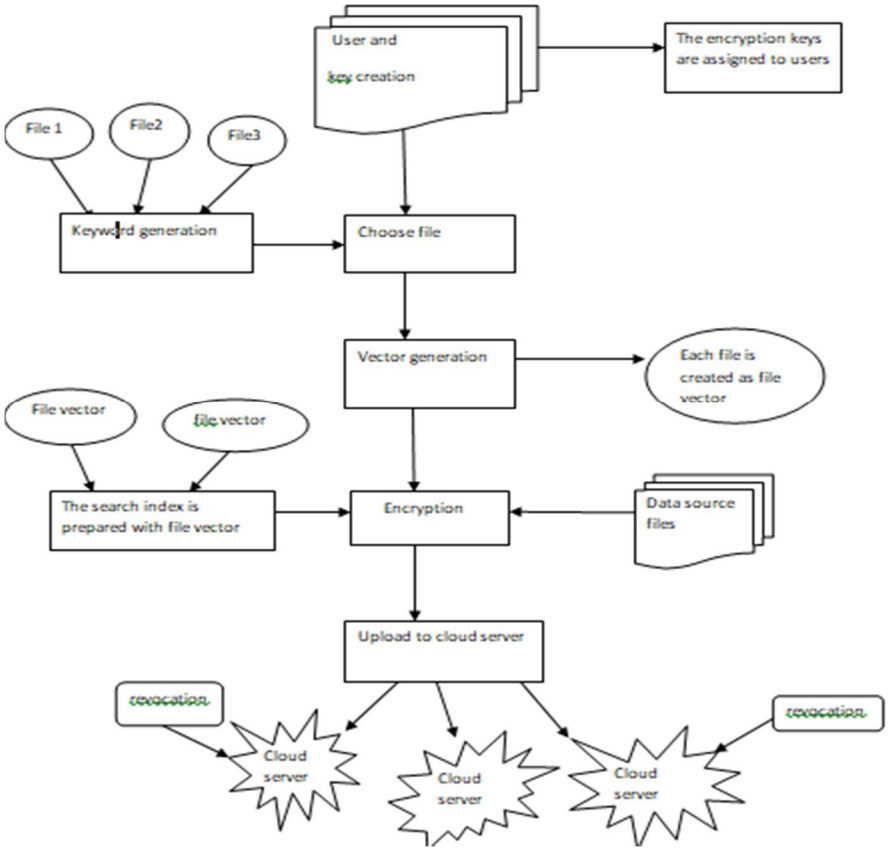


Fig.1 System Architecture

IV. EXPERIMENTAL RESULTS

This system provides the revocation which is not show in this paper.it only encrypts the data given by the user/owner .it is then later tested and validated to the system.

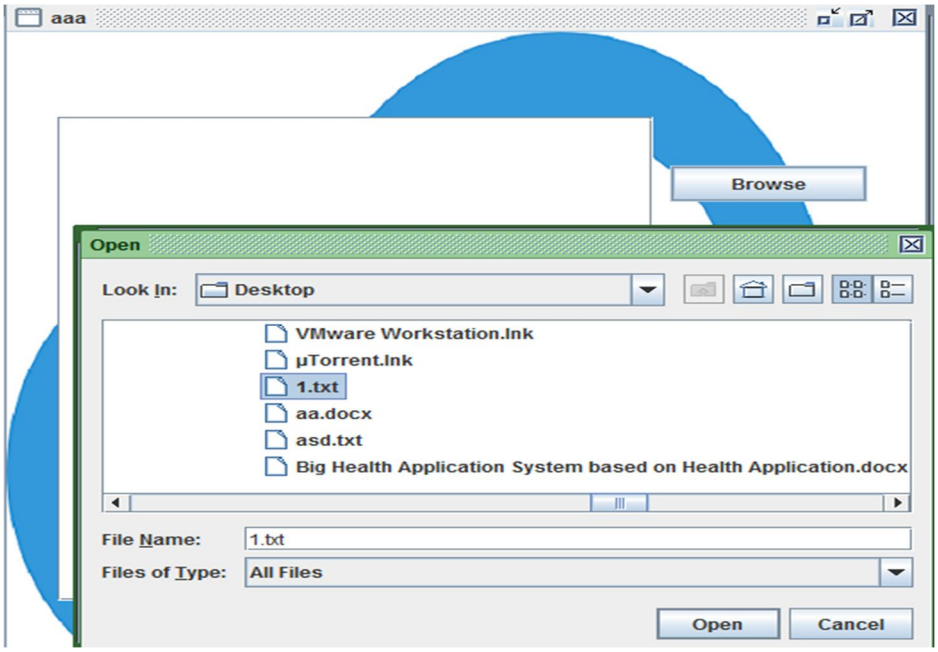


Fig 2 owner browsing the file

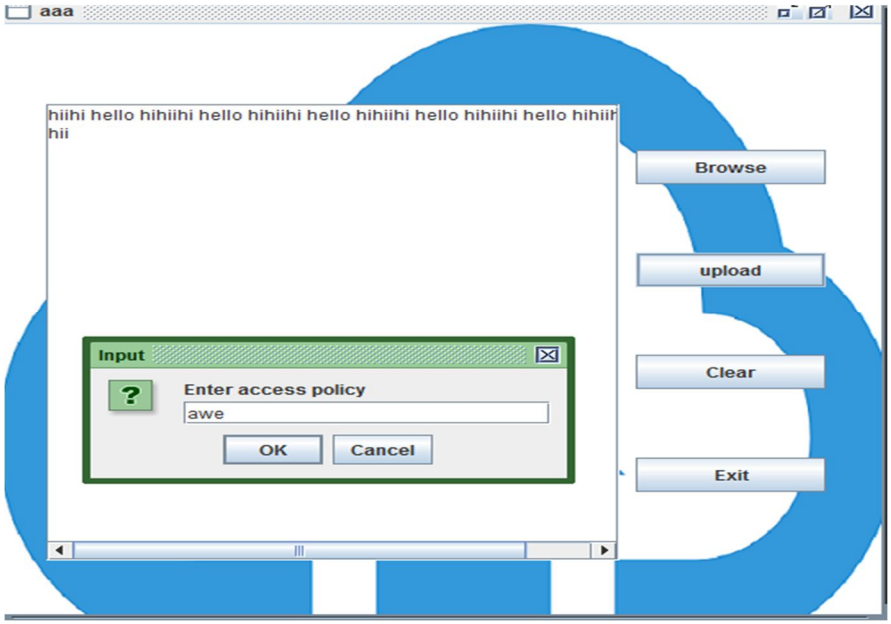


Fig 3 owner entering access policy for the file

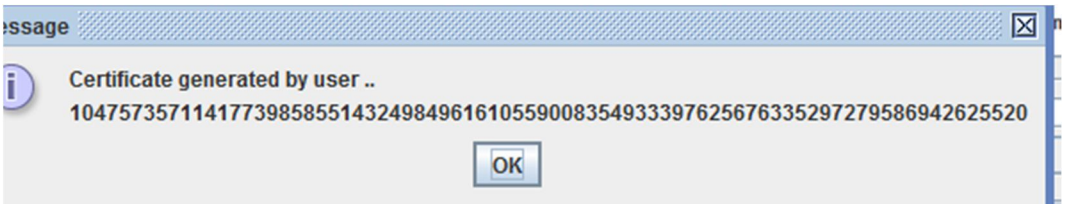


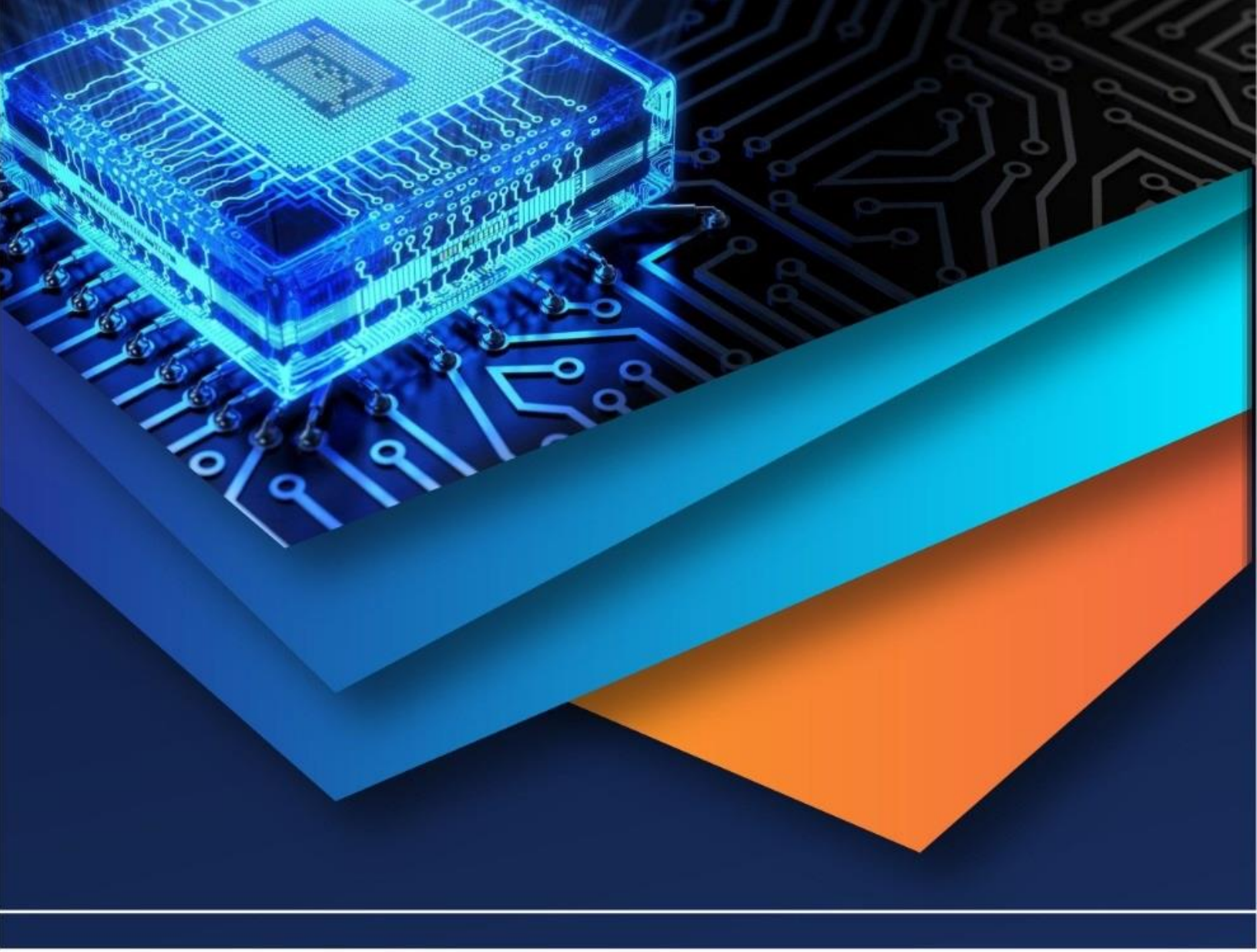
Fig.4 encryption of the file

V. CONCLUSION

In this study , we propose an identity-based cloud storage auditing scheme for shared data, which supports real efficient user revocation. In our scheme, the cloud or the non-revoked user does not need to re-sign any file blocks of the revoked user. The overhead of user revocation in our scheme is fully independent of the number of the revoked user's blocks. Security proof and experimental results show that our proposed scheme is secure and efficient.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69- 73, 2012..
[2] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," In Proc. of IEEE Cloud 2012, pp. 295-302, 2012.
[3] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY