ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT

Volume 2, Issue 6, June 2016

Performance Evaluation of Public Auditing and Privacy Preserving For Sheared Data on Cloud

Sheetal Agrawal[1], Vasundhara Pawar[2], Karishma Rokade[3], Rajeshri Shekokare[4], Prof. A. G. Khairnar[5]

UG Student, Dept. Of IT Engg., NDMVP KBT College Of Engg., Nashik, M.S., India[1,2,3,4]
Professor, Dept. Of IT Engg., NDMVP KBT College Of Engg., Nashik, M.S, Nashik, M.S.,India [5]

ABSTRACT— With cloud stockpiling administrations, it is ordinary for data to be put away in the cloud, as well as shared over various clients. In any case, open auditing for such shared data — while preserving personality privacy — stays to be an open test. In this paper, we propose the primary privacy-preserving system that permits open auditing on shared data put away in the cloud. Specifically, we misuse ring marks to process the confirmation data expected to review the trustworthiness of shared data. With our instrument, the character of the endorser on every piece in shared data is kept private from an outsider evaluator (TPA), who is still ready to openly check the honesty of shared data without recovering the whole record. Our test results show the adequacy and effectiveness of our proposed component when auditing shared data.

KEYWORDS – Public auditing, privacy-preserving, shared data, cloud computing.

I. INTRODUCTION

On cloud data is stored,but security is a noteworthy sympathy toward the customer while utilizing the cloud administrations gave by the administration supplier. There can be some security issues and clashes between the client and the administration supplier. To determine these issues, an outsider can be utilized as an examiner called as Third gathering inspector (TPA). Here, we have utilized different components to guarantee dependable data stockpiling utilizing cloud administrations. It by and large spotlights in transit of giving computing assets in type of administration as opposed to an item and utilities are given to customer over web. Really cloud is a stage where data proprietor remotely store their data in cloud.

The primary objective of cloud computing idea is to secure and ensure the data which go under the property of customer. The security of cloud computing environment is selective exploration range which requires further preparing from both scholarly and examination groups. In the corporate world there are countless which is getting to the data and changing the data. In the cloud, application and administrations move to incorporated tremendous data focus and administrations and administration of this data may not be reliable, into cloud environment the computing assets are under control of administration supplier and the outsider examiner guarantees the data honesty over out sourced data.

II. LITERATURE REVIEW

Existing System

To solve the privacy issue on shared data, we propose Oruta, a privacy-preserving public auditing mechanism. More specifically, we utilize ring signatures to construct homomorphic authenticators, so that a TPA is able to verify the integrity of shared data without retrieving the entire data In addition, we further extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

auditing tasks. Meanwhile, Oruta is compatible with random masking, which has been utilized and can preserve data privacy from TPA.

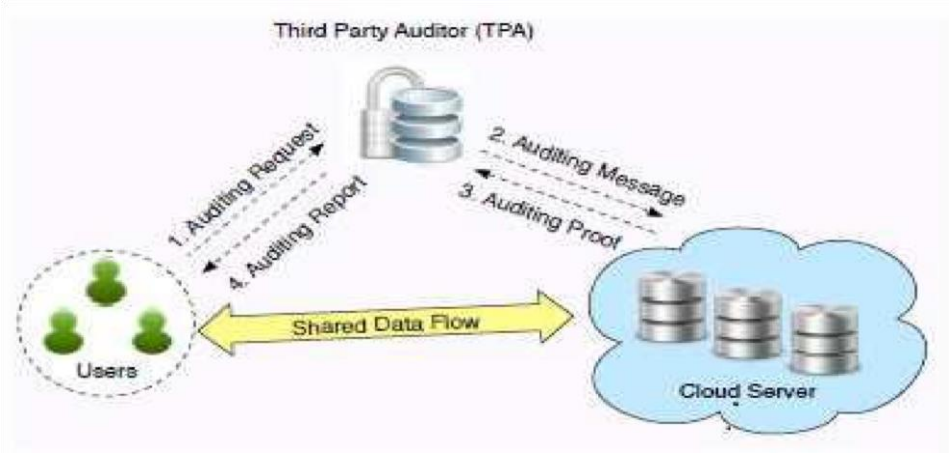

Fig. 1 Existing system

We are building up this component for preserving the privacy of client on untrusted cloud and auditing the data on cloud here client can check the trustworthiness of shared data here we are making utilization of clump auditing to review various documents at the same time in single auditing errand Rando Masking to bolster data privacy amid open auditing assignment. The fundamental objective of cloud computing idea is to secure and ensure the data which go under the property of customer. Utilizing cloud stockpiling, clients can remotely store their data and Use it as oninterest brilliant applications and administrations from a shared pool of configurable computing assets, without the weight of nearby data stockpiling and support. Indeed, clients no more have physical ownership of the outsourced data makes the data respectability assurance in cloud computing an imposing undertaking, particularly for customer with compelled computing assets. In addition, clients ought to have the capacity to recently utilize the cloud stockpiling as though it is neighborhood, without stressing over the need to check its honesty. Hence, empowering open auditability for cloud stockpiling is of basic significance so clients can turn to an outsider evaluator (TPA) to check the classification of outsourced data and be straightforward. To safely present a viable TPA, the auditing procedure ought to get no new vulnerabilities toward client data privacy, and acquaint no extra online weight with client. Here, we propose a safe cloud stockpiling framework supporting privacy-preserving open auditing. Further extend our outcome to empower the TPA to perform reviews for numerous clients at the same time and productively.

III. PROBLEM DEFINITION

It should be designed to achieve following properties:

(1) Public Auditing: The user is able to publicly verify the integrity of shared data without retrieving the entire data.
(2) Correctness: The user is able to correctly detect whether there is any corrupted block in shared data.
(3) Unforgetability: Only a user in the group can generate valid verification information on shared data.
(4)Privacy preserving: To preserve the privacy of user on cloud.

Focusing on drawbacks and inadequacies of existing process, definitely there is need of an efficient system. The proposed system rectifies the demerits and defects of existing process to a greater extend.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

DISADVANTAGES OF EXISTING SYSTEM

1. Failing to audit the integrity of shared data in cloud for dynamic groups. (new member added in group) during public auditing will reveal significant confidential information to public verifiers(TPA).

2. Protect these confidential information is essential and critical to preserve identity privacy from public verifiers during public auding.

3. When multiple user send request to TPA for integrity check load arrive on TPA.TPA is not able to handle it.
4. Blockless verification allow a verifier to audit the correctness of data stored in the cloud server with single block. If other block get change verifier don't get information about it
5. d-Duplication is not avoided

IV. PROPOSED SOLUTION

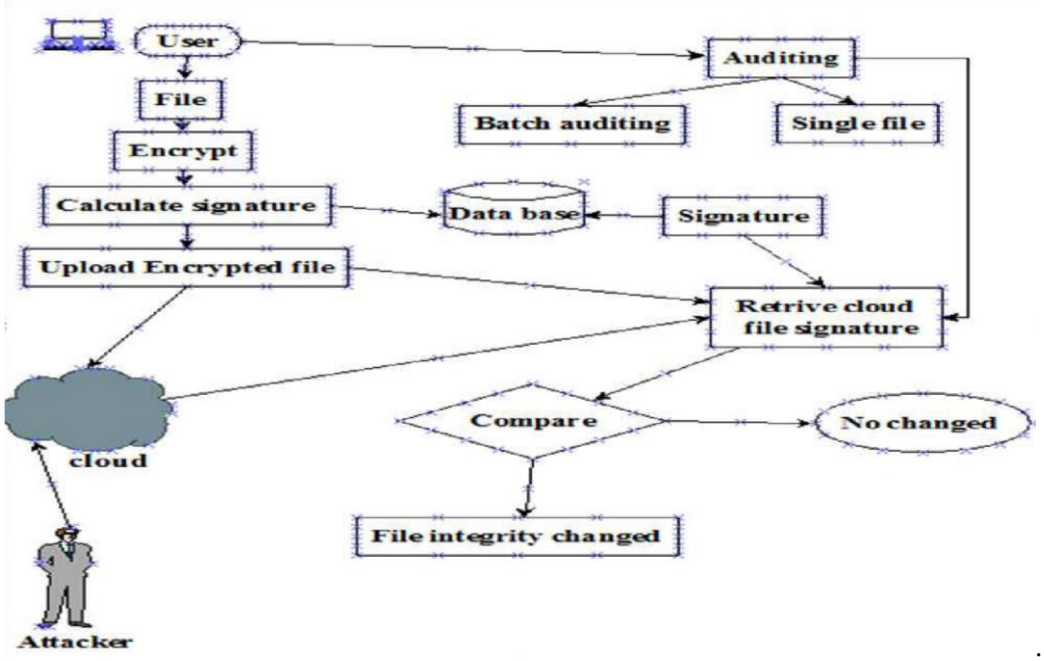

Fig. 2 System Architecture

AES Algorithm- The Advance Encryption Standard (AES)

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

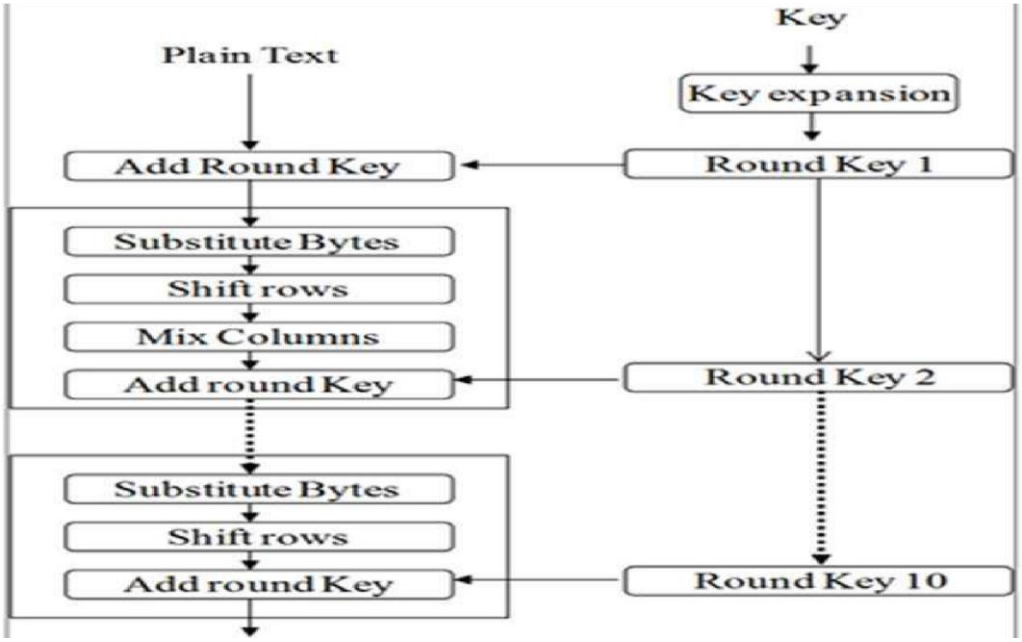

Fig 3. The Advance Encryption Standard (AES)

Four different stages are use

One Permutation and three substitution Substitutes bytes: Uses and S box to perform a byte by byte substitution of the block

shift rows : A simple permutation

Mix columns : Substitution that makes use of arithmetic over GF (2n)

Add round key : Simple bit wise X-OR of the current block with a portion of the expanded key

SECURE HASH ALGORITHM-1

SHA-1 Algorithm takes an input message of length less than 264bitsandproduceoutputof160bitsmessagedig

SHA Diagram

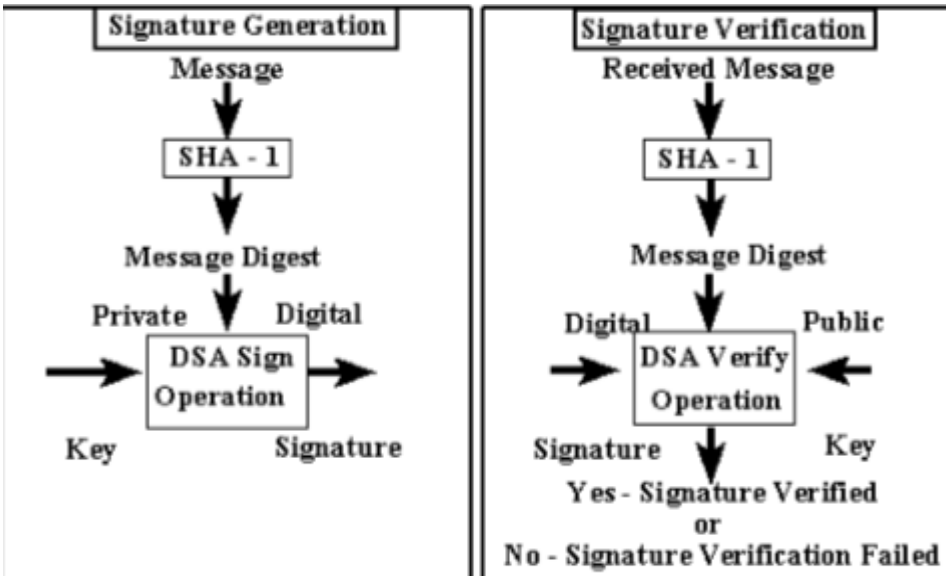

Fig 4. SHA Shell

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

1. APPEND PADDING BITS: Padding means addition of bits to the orignal message.To make length of orignal message to a value 64 bits less than multiple of 512.The padding message consist of single 1 bit followed by many 0 bits as required. The length of padding bits is in between 1 to 512.
2. APPEND LENGTH: Original message padding.
3. INITILIZE MD5 BUFFER:- The buffer is represented as five 32 bits registers as P,Q,R,S,T as. all constants are big endian. four register are same as MD5. P=67 45 23 01 Q=EF CD AB 89 R=98 BA DC FE S=10 32 54 76 TC3 D2 E1 Fo.
4. PROCESS MESSAGE IN 512 BITS(32 BITS 16 WORD)BLOCK: It consist of 4 rounds of 20 steps each round takes 512 bit block processed it and produces 160 bit output. the output of fourth round is added to first round CV to produce CV(q+1).
5. OUTPUT: output of size 160 bits generated.

Cloud Information:

Cloud used- Dropbox

Keys: 3 types of keys are used

1. App key
2. Secret key
3. Token key

Cloud Operations:

1. Upload file
2. Attack file
3. Download file
4. Audit files

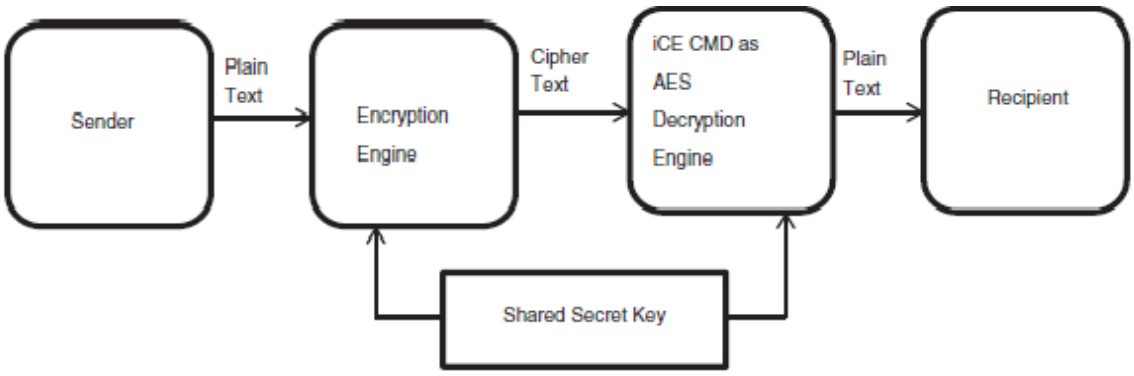

Fig 5. AES Algorithm For Decryption

- Sender creates a cipher text message by encrypting plain text message .
- AES Encryption engine shared Secret key.
- The sender sends the cipher text message to recipient
- The recipient decrypts the cipher text message back into plain text with shared secret key

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

V. RESULT ANLYSIS

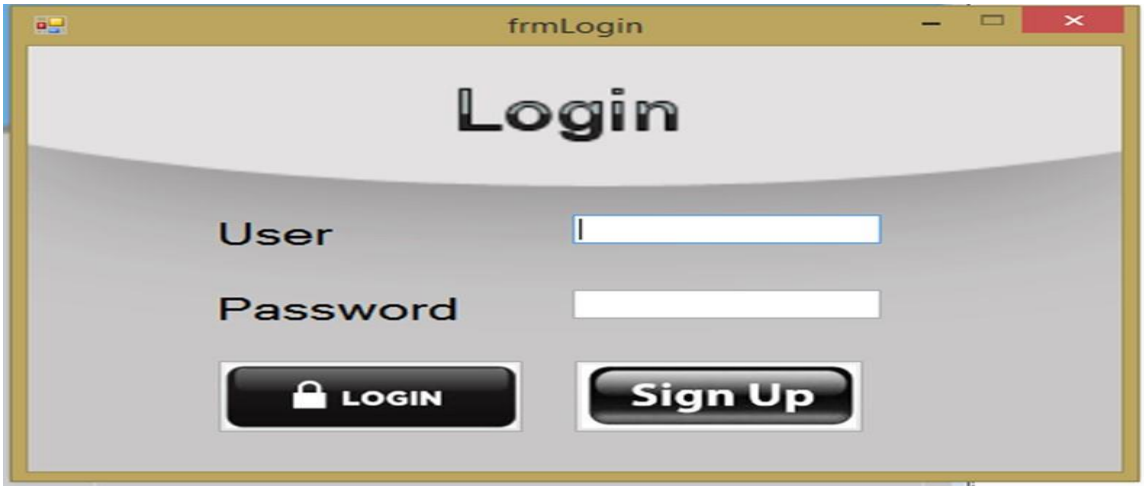

Fig. 6 Login

Fig. 7 Account Sign Up

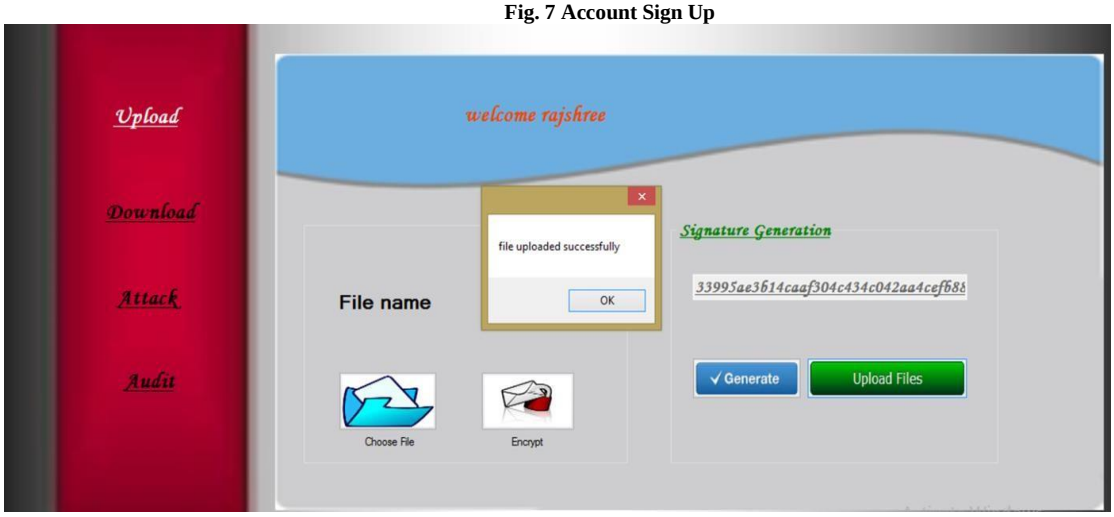

Fig. 8 Digital Signature Generation Form

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

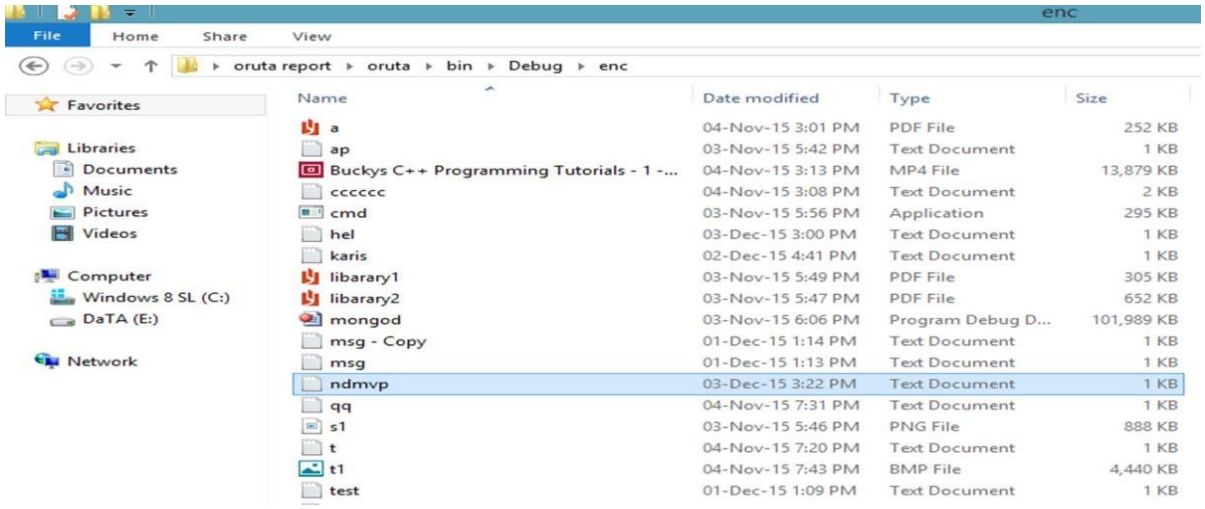

Fig 9. Encrypted Files

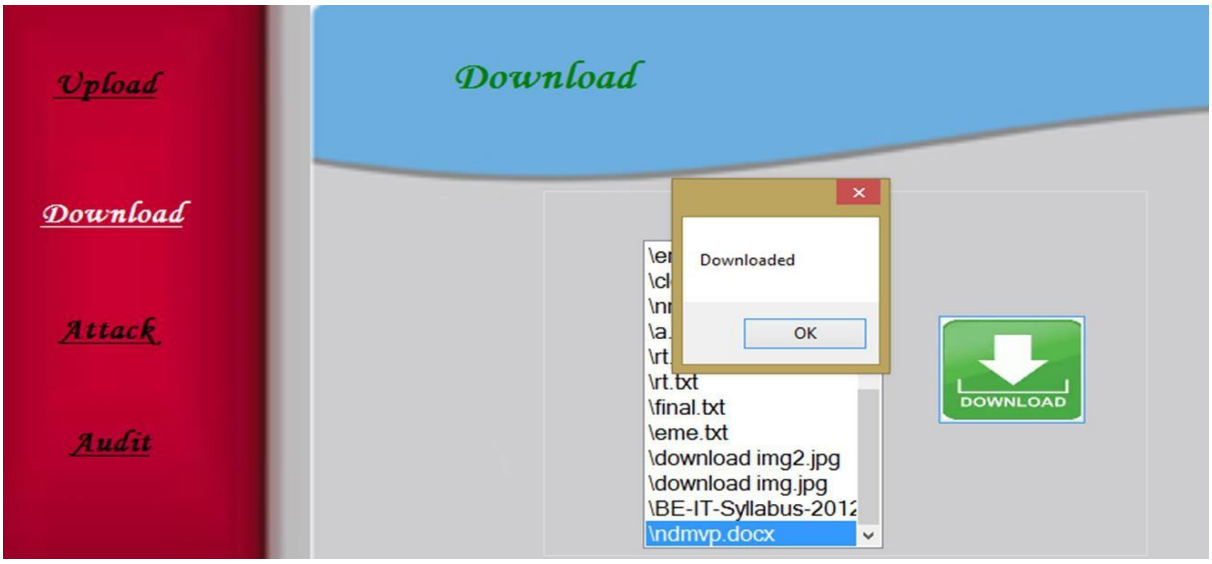

Fig 10. Encrypted (Digital Signature)File Download

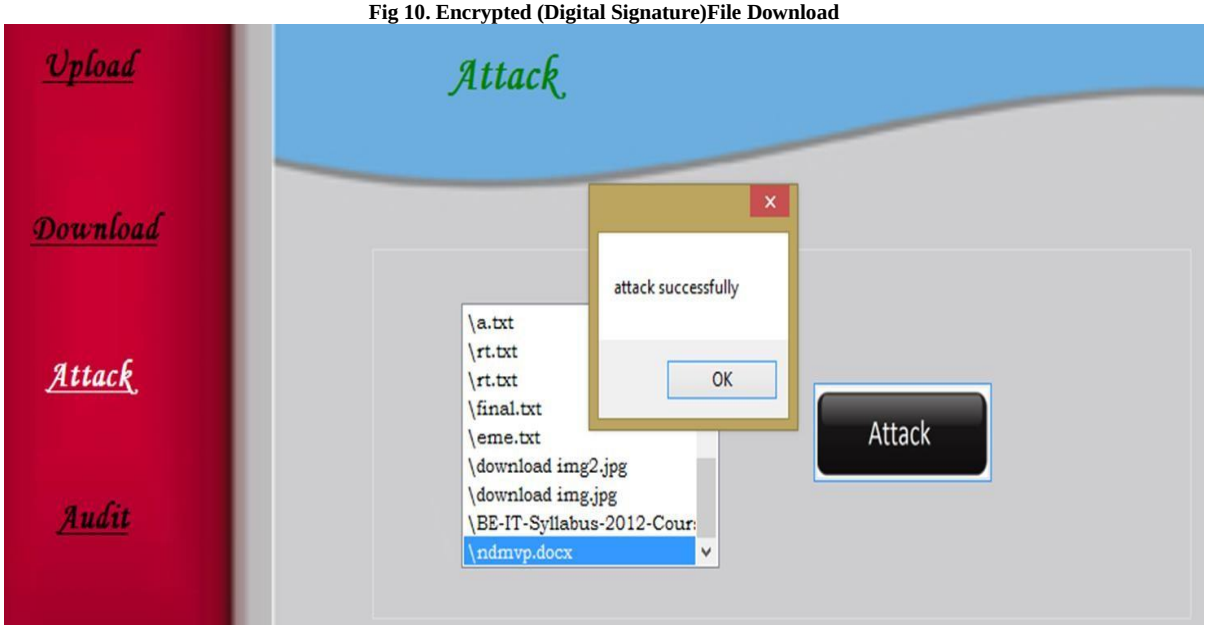

Fig 11. Attacker Attack on file

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 6, June 2016

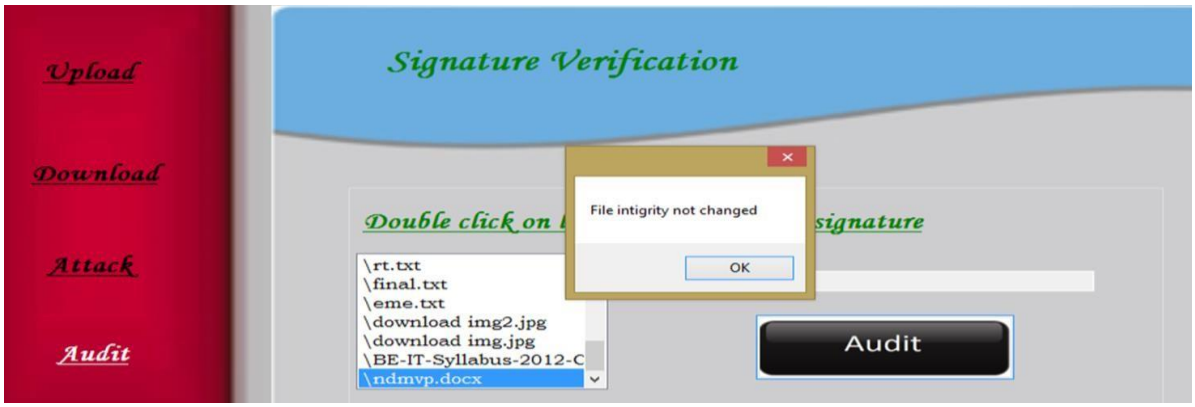

Fig 12. Integrity of File Changes

VI. CONCLUSION

In this paper, we propose the primary privacy preserving open auditing system for shared data in the cloud. We use AES Algorithem for Encryption and Decryption, Protect the confidential information and to preserve identity privacy from public verifiers during public auding. Audit the integrity of shared data in cloud for dynamic groups . (new member added in group) during public auditing will not reveal significant confidential information to public verifiers(TPA).Batch Auditing concept is use so that multiple files are audited simuntaneously.D-Duplication is avoided.

REFERENCES

[1]Boyang Wang, Baochun Li, and Hui Li, Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud.

[2] M. Armbrust, A. Fox, R. Grifth, A. D.Joseph, R. H.Katz, A. Kon- winski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Za- haria, A View of Cloud Computing.

[3]G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peter- son, and D. Song, Provable Data Possession at Untrusted Stores.

[4]C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.

[5]R. L. Rivest, A. Shamir, and Y. Tauman, How to Leak a Secret.

[6]D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and Veriably Encrypted Signatures from Bilinear Maps.

[7]H. Shacham and B. Waters, Compact Proofs of Retrievability.

[8]Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, Dynamic Audit Services for Integrity Verication of Outsourced Storage in Clouds, [8] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing.