International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 1 (February 2016), pp.63-71

http://www.meacse.org/ijcar

Cloud Storage Auditing With Key Generation Using Blowfish Algorithm

N.Meenakshi and G.Sasikala

Department of CSE, Valliammai Engineering College, Chennai-603203, India

Abstract

Cloud storage auditing is used to verify the reliability of data in the cloud storage system. Mainly it can be focused on to maintain the user's data in a secure manner, by using the key generation algorithm. In this Paper, Users can upload data in the cloud system, then generating two set of keys for the users(Publickey, Secret key).And also develop an novel Authentication to support forward security and blockless verifiability. Here two methods are used, I.Blowfish algorithm for key generation process II. Binary tree structure method used to provide the security and performance in an advanced manner.

Key Words: Cloud Storage Auditing, Key Generation, Blowfish, Binary Search Tree.

I. Introduction

Cloud storage auditing [2] used to verify the data stored in public cloud system.In recent years, auditing protocols[4] for cloud storage have attracted more consideration and have been researched effectively. These protocols focus on various parts of auditing, and achieve high bandwidth and efficiency is one of the crucial concerns. For that purpose, the Homomorphic[8] Linear Authenticator (HLA) technique that funds blockless certification is explored to reduce the overheads of estimation and transmission in auditing protocols. Auditor to verify the Reliability of data in cloud system. The resulting verification cannot be gathered, leading to unacceptably high estimation cost for the storage auditing. Auditing protocols are designed to ensure the privacy[2] of the client's data in cloud. Another method have been addressed in cloud storage auditing is how to support data dynamic operations.

Cloud service suppliers charge users provisional upon the space or facility provided in Research and Development, it is not always potential to have the genuine cloud organization for performing experiments. So it can be used to the cloud simulation tool, Modeling and simulation of large scale cloud computing data centers, data center network topologies and message passing applications, enery aware computational assets.

A. CLOUD COMPUTING

Cloud Computing is used to store, share and managing the data. Large number of computer that are joined to the real time communication network. Cloud computing and cargo space solutions provideusers and originalities with different abilities to store and process their data in third party data centers. Cloud provides various defense process in Auditing. And it can be navy of the Software, Platform and Transportation.

- Self-service provisioning: End users can revolve upcoming assets for almost any type of workload on-necessity.
- Elasticity: Companies can scale up as computing needs swell and then scale down again as demands lessen.

- Pay per use: Computing resources are considered at a granular level, allowing users to compensate only for the resources and capacities to use.

B. AUDITING

Auditing is a valuation of Person, Organization, System, Process, Enterprise, development or Product. The term refers to audits in secretarial. And it can be used to the confirmable auditing for outsourced data stored in cloud system. Two types of Auditing in an executing process, Correspondence audit, Fields audit. Audit can be used to classify and evaluating the user's data and verifies to the each levels then sending response to user. File Storage: Files can be stored to the cloud system and it can be performed to the Auditing process.

Advantages

(i)Save Time :Traditional methods of auditing is an instance to consuming where more interventions are compulsory on part of the auditors as they have to approve manual methods for subsequent the procedures.

(ii)Savings: The bucks and butter of all businesses are to look for venues for fiscal savings data of an cloud system.

II. Existing System

Auditing protocols[4] can also prop up dynamic data operations. Other aspects such as deputy auditing, user revocation and eliminating certificate managing in cloud storage auditing. Auditing protocols for cloud storage have fascinated more consideration and have been explored intensively. Most of the existing auditing protocols would become incapable to work. These protocols focus on several diverse aspects of auditing. Achieve high bandwidth and working efficiency is one of the vital concerns. Unfortunately prior auditing protocols did not deem this critical issue, and any revelation of the client's secret auditing solution would make most of the obtainable auditing protocols incapable to work correctly. Focus on how to trim down the damage of the client's key exposure [1]. How to do it efficiently under this problem setting brings in many challenges.

First of all, applying the traditional way out of key revocation to cloud storage auditing [4] is not practical. Whenever the client's secret key for auditing is uncovered, the client needs to produce two set of key for public key and secret key[1] and restore the authenticators for the client's data stored in cloud. This process involves the downloading data from the cloud, producing new set of key, and re-uploading the lot back to the cloud, all of which can be tedious and bulky. Moreover, it cannot always agreement that the cloud provides real data when the client restores new verification. Secondly directly adopting standard key evolving procedure is also not suitable for the new problem situation. It can lead to retrieving all of the genuine files blocks when the verification is preceded. This is partly as the technique is incompatible with blockless proof. The resulting authenticators cannot be aggregated, leading to incorrectly high working out and communication cost for the storeroom auditing.

Drawbacks

- Using Naïve explanation, The Authenticators of the data beforehand stored in cloud, on the other hand all need to be efficient because the old secret key is no longer protected. Does not finding the optimal answer.
- Two set of keys has to be very long and linear, Weak intelligence of refuge and low security situation at the client.
- Auditing protocols for cloud storage have fascinated much attention and have been researched intensively.
- Most of the auditing procedures would certainly become incapable to work. To realize high bandwidth and division helpfulness is one of the essential concerns.

III. Proposed Work

In These Paper, Focus on how to reduce the damage of the clients key contact in cloud storage auditing. So it is used to generating the method of a key generation. It can be strongly maintain the key

of an auditing process. So It should not affect damage of the client's innovative data in the cloud storage system. This client's wants to an additional user's content, they can send permission for the authorized user and get key for public key and secret key then admittance to view and download of an the user content. So Clients can be used to the traditional key for revocation method. In existing classifications used to procedure performs to the Output should be shorter than enter Blockless verification [9],Auditor can be checks to honor of certain files block in the cloud system. Hash procedure performs to the Output should be shorter than input.

IV. Architecture

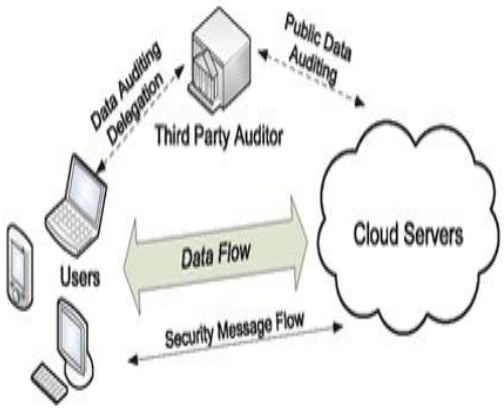


Fig1.Architecture

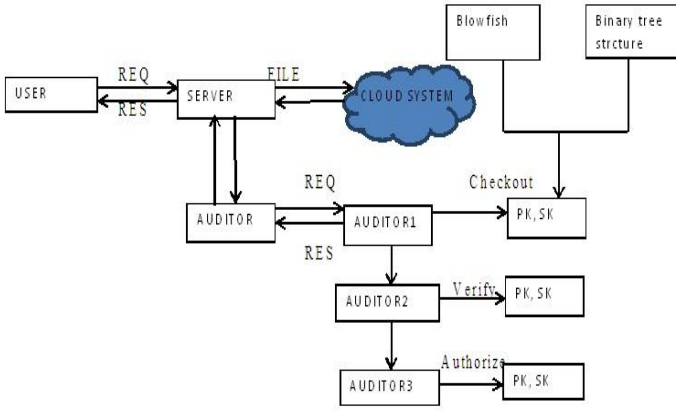


Fig2.BlockDiagram

HLA (Homomorphic Linear Authenticator) data can be send data by using Packet size. So it can be decrease overhead, transportation. Finally it can be follows to the Blockless verification[9],Auditor can be checks to honor of certain files block in the cloud system.

Cloud me is a luggage compartment tool for the cloud system. It can be an operated storage services by offers cloud storage space system. Cloud me is used to the cloud storage and sync solution for users to store, right of entry and share their user's content. Cloud me maintains to various features such as easy user interface, easy sharing, dynamic file storage of user's comfortable, and it can be provides mobility, media features, collaboration among the data. Sharing data can be email, text, message, facebook, google. In Cloud system, Server can be upload data in cloud storage system, diverse types of user's can

be send request to server, user wants any data from cloud system, send request to server, then pass demand to the auditing process verifies data are three levels User's details can be,

- Check
- Verify
- Authorization among user's data.

Blowfish algorithm have been used to key generation (Public key and Secret key), Binary tree structure is used to updating the Secret key. To Verifies the user's data then send response auditor to server and user. So these methods can be performed to the secure and efficient in an advanced manner. Various levels of data can be verifies to the cloud system have been storing files, checking, verifies, checks to the authorize person content, authenticate among the data using key.

ADVANTAGES

- The Binary tree structure [9], seen in a few prior works on different cryptographic designs to update an undisclosed keys for the client.

- The Homomorphic Linear Authenticator (HLA) [8] technique which support blockless substantiation is explored to decreases the expense of working out and messages in auditing protocols.

- The safety measures proof and the recital analysis show that our projected protocol is secure and capable. We allow the auditor and addict to view and download the file if they send appeal, Users will provide the key to them.

- Our protocol is maintaining to the Auditing process, checkout, agree and authenticate user's data to verify via key. So these method achieves sheltered and efficient.

A. KEY GENERATION

Key cohort[1] is the process of generating two set of keys for cryptography. These keys are used to both encrypt and decrypt, whatever records is being processed encrypted and decrypted that should be stored. They can provide increase productivity, effectiveness, cost saving, improve customer agreement. Generating the two set of keys, Public key ought to be constant and secret key generating between the every time.Syssetup(), Keyupdate(), Authgen(), Proofgen(), Proofverify().

Public key(): PK, should be constant.

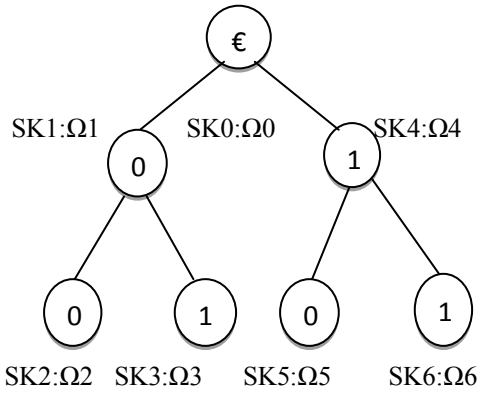
Secret key() :SK, Changing key for every time period.

B. BINARY TREE STRUCTURE

A Recursive non empty binary tree refers to triple(L,R,R). Binary tree structure has been two children, left and right and one root node. These methods can be used to first assigning values of an the each nodes, performing the stack operation used to the push and pop method. Tree structure have been various types as Perfect, full, routed, complete, balanced, unbalanced. Inserting the element or data in this method, so it can be generating two set of keys (public key and secret key).

Perfect l=2hn=2h+1-1

Leaf node l=(n+1)/2.



SK1:{(S0,R0),(S1,R1)}

SK2:{(S00,R00),(S01,R01),(S1,R1)}

SK3:{(S01,R01),(S1,R1)

SK4:{(S1,R1)}

SK5:{(S10,R10),(S11,R11)}

SK6:{(S11,R11),(S1,R1)}

S: Secret key

R: Cloud storage server

Binary tree structure specified by the S is secret key and R is server, used time period for 0 t 6. The changes of Ωj(0<=j<=6). Public key PK period j, user's secret key SKJ,file F=(m1,….,mn). Assigning PK and SK values of an the Ω0,1,….,6.

Ω0=0

Ω1=Ω0 U{R0}={R0}

Ω2=Ω1 U{R00}={R0,R00}

Ω3=Ω2 U{R01}={R0,R01 }

Ω4=Ω3 U{R1}-{R1,R01,R11}={R1}

Ω5={R1,R10}

Ω6={R1,R11}

C. TREE TRAVERSAL

Graph traversal refers to the process of visiting and updating each node in the binary tree. These types of traversal can be used to the two types operations, Stack and Queue. In our design is used to the Pre order traversal technique, first visiting root node of the element then left and right subtree can be recursive calling by using binary method. Stack: Last in first out, user's can be inserting an element in the binary structure by using Stack method is performed to the last inserting element eliminated to the first order.

D. PREORDER TRAVERSAL TECHNIQUE

Traversal is performed to three types of nodes such as Visit node, Left node, Right node are used to updating the secret key.

I. Display the data part of root element

II. Traverse by using left node.
III. Traverse by using right node.

V. Algorithm

A. BLOWFISH

Blowfish is a Symmetric key block cipher, Invented by Bruce Schneier at 1993. Replacement for the DES [3] or ID EA algorithm. Variable length key size has been 32bits to 448bits. Symmetric key is a Secret key [1], Asymmetric key is a Public key both key is used to domestic and exportable faster than DES. Fast implementation on 32bits, first secure block cipher and license free method of an the cryptography. This algorithm has been used to the generating set of pair-wise keys. Key can verifies to the four levels Checkout, Verify, Authorize and Approval of a user's files. Using these Algorithm achieve various benefits: they are Storage, Key generation, Authorization [4],Time and Power consumption. Using Blowfish algorithm Key can be used to encrypting and stored original files on the cloud system, Whenever user wants to accessing the same files by using key to decrypting the original file. Permutation and Combination is a method it uses same key for both encryption and decryption. Blowfish can be used to the key cause and key schedule algorithm, and these algorithm used to the Binary tree structure method based on key generation. Benefits of these algorithms are: Password-hashing method basedon OpenBSD uses.

Schneier intended Blowfish as a general-purpose algorithm, proposed as an alternative to the mature DES [3] and free of the troubles and restrictions related with other algorithms. At the time Blowfish was on the rampage, many other designs were exclusive, overloaded by patents or were feasible or management secrets. The algorithm is hereby placed in the public domain, and can be absolutely used by anyone.

VI. Implementation

Cloud storage system have been implemented to the Blowfish and Binary tree structure method through Auditing process. First initiate the key generation and producing two set of keys public key and secret key and providing resource of the client's.

State<- Initstate()

State<- Generatekey()

Repeat

State<-Generatekey(Public key)

State<-Generatekey(Secret key)

A. KEY GENERATION

Key should be generated to the different ways ofinstance, data initialization among the generator object and providing request and response object .

getInstance(): Return a key generator object in the user's data.

init() : Initialize the key generator with specific key.

generate Key() : Generate key and returns SK object.

generate Algorithm() : Return the algorithm.

get Provider() : Returns to the provider.

```
KeyGeneratorkg= KeyGenerator.getInstance(alg);

Kg.init(keysize);

SK key= kg.generatekey();
```

- File storage
- Key Generation
- Secret key update
- User's authorization
- Authentication

a. File Storage

User files can be stored on the cloud system[6], The file is provided the option to scrutiny and download based on the time phase keys.

b. Key Generation

User can be upload files in cloud system, two set of keys are generated (Public key and Secret key). Key can be used to securely maintained the User's data.

c. Secret Key Update

Public key should be constant, every time uploading files to the cloud system, generating new type of secret key [1]

d. User Authorization

Data can be send and receive to the cloud system, Auditor can be verifies the data can be used to check the Authorized person content.

e. Authentication

Cloud system involves the client and the cloud. The client produces files and uploads these files along with corresponding validator to the cloud.

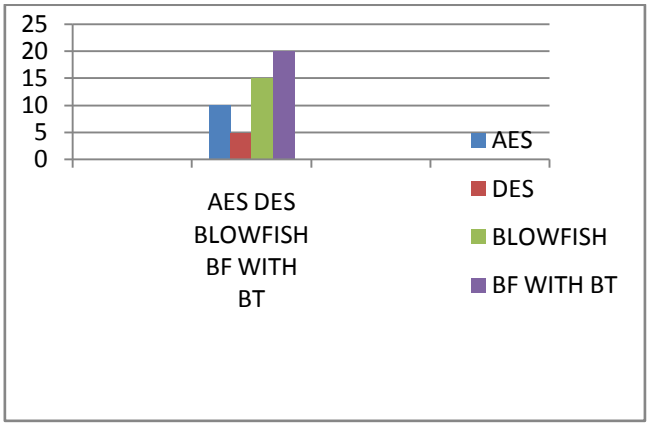
f. View and Download files

The files can be viewed and download based on the set of time period key used for Authentication process.

VII. Result and Discussion

By using Blowfish and Binary tree structure method is easy for generating key for auditing process. In cloud storage system is secure and efficient to managing the client's data with the help of various level of auditing and key generation process by using cloud me tool. User's data can verify to the various levels of auditing in cloud computing and it can be achieve high performance and security among the authorized data.

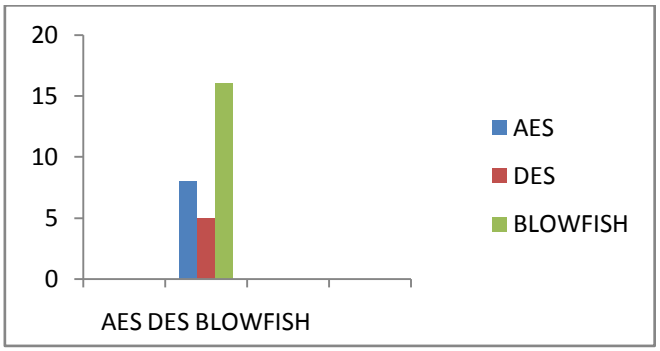
a. Throughput



Key generation [3] is using Blowfish with Binary tree Power Consumption structure method have been increase the level of Throughput, compare to the AES and DES.

Throughput= TP(Total Plain Text)/ Encryption Time.

b. Power Consumption



Power Consumption have been compared to AES, DES levels. Hence minimum amount of power can be used to the Blowfish algorithm based key generation in cloud storage auditing.

VIII. Conclusion

In this paper, it is understood how to store the client's data securely in the cloud using Auditing. Public Auditing system utilizes key generation. We offer a new method for cloud storage auditing with key generation algorithm. Finally it can achieve more security to the client's data and give high performance for generating the keys.

References

[1] Chunxuan Ye and Alex ReznikInter Digital Commuications Corporation King of Prussia,"Group Secret Key Generation Algorithms" 0701124v1 19 Jan 2007.

[2] C.Wang, S.S.M.Chow, Q.Wang, K.Ren, and W.Lou, "Privacy Preserving Public Auditing For Secure Cloud Storage," IEEE Trans. Comput. Vol.62, no.2, pp.362-375. 2013.

[3] I.Abd-ElGhafar, A.Rohiem, A.Diaa, F.Mohammed, "Generation of AES Key Dependent S-Boxes Using RC4 Algorithm." 13 International Conference On Aerospace Sciences &Aviation Technology, 26 May 2009.

[4] Po-Wen Chi and Chin-Laung Lei, Member, "Audit Free Cloud Storage Via Deniable Attribute-based Encryption" , IEEE Transaction on 2015.

[5] PriteeParwekarPrakash Kumar MayuriSaxenaSakshiSaxena, " Public Auditing: Cloud Data Storage"International Conference On 5th 2014.

[6] Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data" IEEE Tansaction on Parallel and Distributed systems,Vol No.1 2015.

[7] Ling Li Lin Xu Jing Li ChangchumZhang, "Study on the Third-Party Audit in Cloud Storage Service" Internnnational Conference on Cloud and Service Computing 2011.
[8] Jose M.Lopez, Thomas Ruebsamen, Dirk WesthoffHochschuleFurtwangen University Furtwangen, Germany, "Privacy-Friendly Cloud Audits With Somewhat Homomorphic and Searchable Encryption".
[9] Jia Yu, KuiRen, Senior Member, IEEE, Cong Wang, Member, IEEE, and Vijay Varsdharajan, Senior Member, IEEE, "Enabling Cloud Storage Auditing With Key Exposure Resistance" IEEE Transaction on Information Forensics and Security, , JUNE 2015.