International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

Securing Multi-copy Dynamic Data in Cloud Using AES

Arockia Panimalar.S[1]

[1]*Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamil Nadu*

Abstract - *Most of group vendors store unlimited quantity of their data in cloud with the facility of retrieving. Users pay costs for storing data. Most of the users are in collaborative relationship, at that time data sharing and dynamic operations are useful to make robust productive benefits. Uploading the data in multi server is to avoid the data loss from hacking and server crash. In this paper, we introduce a brand new method is Map based provable multi copy dynamic data that has the aspects like uses multi copy of data, file security and preventing data corruption. In this paper, there are three polynomial algorithms for protecting the data - Keygen, Copygen and Taggen. AES algorithm is used for data security. The authorized user to seamlessly entry the file copies saved through the CSP.*

Keywords: Provable Data Possession (PDP), Storage Security, Cloud Service Provider (CSP, Multi-Copy, Multi-Owner.

1. INTRODUCTION

An emergent amount of clients group use cloud to store data which has end up configuration [1]. Cloud service provider (CSP) makes it possible for storing far more data than private PC. As soon as data stored in remote server, authorizer can entry all data from any geographical location. Most of the time organization store foremost data in cloud, without leaving a duplicate in neighbourhood computer. Once data is stored in cloud they are probably not reliable due to losing control on data. So, it's predominant to ensure data isn't misplaced or corrupted by means of checking data integrity. In data integrity checking, patron challenge remote server and server response by way of proving that. Many researchers have motivated about this drawback and discover specific techniques.

PDP is among the techniques for validating data integrity. In this model, don't need to store all file to nearby computer to validating data integrity. It creates metadata expertise of each file and that store it in neighbourhood laptop without storing entire file. On the time of verification of data integrity it sends the metadata to the verifier facet. PDP model used each static data and dynamic data. In static PDP schema used data which cannot alternate, it only retailer and access with the aid of authorize users [2][3]. In dynamic PDP schema stored data may also be adjust via performing operation like modify, insert, delete and so on. And additionally it can be scaled through inserting more knowledge [4] [5] [6]. The MB-PMDDP of a database procedure is its constitution described in a formal language. This schema specifies, founded on the database administrator's capabilities of viable functions, the truth that can enter the database or those of interest to the possible end-client. A model of this "concept" carefully corresponds to a database, which can be obvious at any on the spot of time as a mathematical object.

2. LITERATURE SURVEY

A. Provable Data Possession (PDP)

Ateniese [7] has discussed a provable data possession technique the place a PDP protocol checks whether or not the data outsourced to the CSP is retained as per the service agreement. The client pre methods the file, generating a metadata which is stored locally and transmits the file to the CSP and he may delete his local replica of file. The server stores the file and responds to the assignment issued by the client. The client can alter the data in the file which is to be saved in the server. The client can execute data possession project to make certain that the server has retained the file earlier than deleting his local reproduction of file. Before outsourcing the data to the CSP the client can encrypt the file for the security purpose however metadata does now not contain any encryption keys. At any time when the client desires to confirm the integrity of the file data possession task is issued for which the server has to compute response, using the metadata which is stored locally the client can verify whether or not the server has successfully retained the file. The server has to reply to the challenges issued through the client failing to take action indicate that there may be a data loss and the server could not be relied on. Although the file is partly or fully missing the server might try to persuade the client that it possess the original data. The intention of this scheme is to realize the misbehaviour of the server. The difficulty of this scheme is it conveniently applies to the only static records.

B. Dynamic Provable Data Possession (DPDP)

Chris Erway and Alptekin Kupcu [8] have proposed an efficient way of proving the integrity of data saved within the CSP. In the PDP model the client pre-techniques the data and then retailers it within the server by using maintaining the metadata and the server responds to the project issued through the client. Nevertheless this model applies only to static records [9]. For that reason in the DPDP model the PDP model is accelerated to support dynamic updates to the saved data. Within the PDP model the file that's outsourced can in no way be converted whereas in the DPDP model dynamism is supported the place the client can insert, adjust

or delete the stored blocks. Such scheme is important in practical scenario [10]. In this DPDP scheme an efficient development for dynamic provable data possession is proposed which extends the PDP model to help provable updates on the saved data.

Given a file F such as n blocks, update is outlined as either insertion of a brand new block, or modification of an existing block, or deletion of any block. For that reason update operation is the most common type of modifications a client may just want to participate in on a file. In this scheme the rank understanding is used to prepare dictionary entries. As a consequence it is able to help effective authenticated operations. This scheme supplies an efficient entirely dynamic PDP solution. However the scheme does not guarantee that a couple of copies of the data file are virtually maintained [11].

C. Multiple Replica Provable Data Possession (MRPDP)

Reza Curtmola [12] has proposed multiple-replica provable data possession (MR-PDP) system. In an effort to toughen the data availability and reliability of a single replication PDP method the data copies are replicated and saved throughout a couple of servers.

With the aid of storing the data files on a couple of servers throughout special places, despite the fact that if one of the copies are destroyed, the data can nonetheless be recovered from the remainder copies. The replication methods can tolerate failures only if the failure modes of the replicas are independent. Think if the failure mode of replicas is stylish then all of the replicas may fail at the same time that is in view that all the replicas are saved within the same geographical location or considering data dependencies exist among replicas. The primary aim of the replication methods is to tolerate independent, unintended and non-malicious failures comparable to hardware disasters.

When the storage servers are non-malicious, storing data in different geographic areas can be certain failure independence. The drawback is exclusive when the servers are untrusted, i.e., servers are malicious and might collude. The failure independence cannot be assumed within the replication programs which rely on untrusted servers, such servers are not able to present the equal stage of assurance as an approach counting on trusted servers. At the beginning the replicas probably stored on servers in exceptional geographic locations, however later the servers can transfer the entire replicas to one place and access them from that place when client demands. An additional principal open hindrance is starting bodily vicinity of data.

The typical obstacle faced through the replication systems is to prove the data availability, upon client's assignment, the servers can produce replicas however this does not show that the precise replicas are saved all of the times. The malicious servers may introduce dependencies amongst replicas stored across different geographic areas, with the aid of encrypting them before storing. Replicas can also be decrypted and served whenever they are requested through clients. The malicious servers can effectively lessen the reliability enhancements completed by means of storing the replicas at unique places with the aid of storing the encryption key in single vicinity. Lack of the encryption key approach loss of the entire replicas. The efficient multiple-duplicate provable knowledge possession (MR-PDP) scheme is mentioned that ensures that the storage servers are storing more than one specific replica. Nevertheless the problem of the scheme is allowed client side difficulty in having access to the file copies from the CSP.

D. Effective Multicopy Provable Data Possession (EMCPDP)

Possession (EMC_PDP) Ayad F.Barsoum and M.Anwar Hasan [13] have proposed secure and effective protocol to provide powerful proof to the customers that CSP is storing the entire data copies as per the service contract. The effective Multi-replica Provable data Possession (EMC-PDP) scheme is proposed which utilizes BLS Homomorphic Linear Authenticators (HLAs) [14].

The HLAs finger prints each block of file in one of these approach that it satisfies any mission vector issued through the purchaser, with the aid of authenticating worth the server can homomorphically assemble the tag. The important task in designing a multi-copy provable data possession model is to generate special distinguishable copies of data file, a simple and effective process is used to generate these copies.

The EMC-PDP model adapts to the diffusion property of any secure encryption scheme. Diffusion implies that the output bits of the cipher text must rely upon the enter bits of the plaintext in an extraordinarily elaborate means. In an encryption scheme with robust diffusion property, if there's a change in one single little bit of the plaintext, and then there shall be drastic exchange within the cipher text content in an unpredictable way [15]. This technique of generating distinctive copies is efficient, and likewise successful in solving the approved user's hindrance of the MRPDP scheme to access the file copy obtained from the CSP. In this scheme, the data owner or the approved users need most effective to hold a single secret shared key to decrypt the file reproduction. It is a secure, complete, and effective protocol that addresses the storage integrity of multiple data copies over cloud computing.

3. METHODOLOGY

We prescribe a map based provable multi-duplicate dynamic data possession (MB-PMDDP) scheme. This scheme gives an

abundant guarantee that the CSP outlets all copies which are settled upon in the service contract. Also, the scheme bolsters outsourcing of dynamic data, i.e. it enables block level operations practically equivalent to block amendment, insertion, deletion, and append. The authorized clients, who've the right to access the owner's file, can seamlessly access the copies acquired from the CSP. A radical comparison of MBPMDDP with a reference scheme, which we possibly can obtain by using extending current PDP items for dynamic single-reproduction data, is given. We also report our implementation and experiments utilising Amazon cloud platform. The security of our scheme against colluding servers is discussed. In the proposed system AES algorithm is used for data protection.

4. ALGORITHMS

(PK, SK) ← KeyGen (): This algorithm is run by means of the data owner to generate a public key PK and a private key SK. The exclusive key SK is stored secret through the owner, while PK is publicly identified.

Ẽ← CopyGen (CNi, E)1≤i≤n: This algorithm is run through the data owner. It takes as input a replica quantity CNi and a file F, and generates n copies Ẽ= Ẽi 1≤i≤n. The owner sends the copies Ẽ to the CSP to be saved on cloud servers.

Φ← TagGen (SK, Ẽ): This algorithm is run by way of the data owner. It takes as input the personal key SK and the file copies Ẽ, and outputs tags/authenticators set Φ, which is an ordered collection of tags for the data blocks. The owner sends Φ to the CSP to be stored along with the copies Ẽ.

A. Advanced Encryption Standard (AES)

AES is a block of cipher algorithms beginning from Rijndael algorithms. It is a symmetric key encryption algorithm that encrypts a block of elements (set of bits) in the meantime, not at all like stream ciphers that encode each single item independently.

AES works with a 128-Bit Block cipher and, wishes to structure the plain text in matrices form of 4 rows and 4 columns (4x4 bytes = 128bit s) i.e 16bytes which are called states ("states"). The AES encryption separates the encryption stage ("round") in indistinguishable stages, each stage has its own particular session key or sub key that is extracted from the master key utilizing the accompanying procedure: The AddRoundKey – Each byte of the block is encrypted with the session key, the session key is calculated from the key manager. The number of stages changes at the variety of the key size being used, for instance, there are 14 phases or rounds for a 256 piece encryption key. Each phase comprises of four strategies that, connected to blocks (states), enact a progression of operations that work to acquire the cipher text. All the encryption process can be summarized in the following steps:

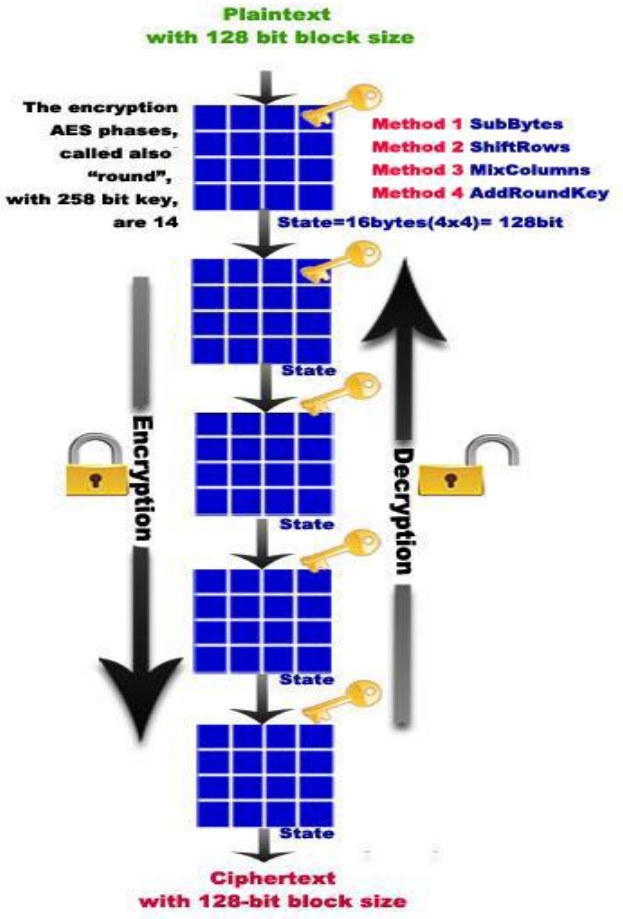

Fig 1: AES Flow Model

5. CONCLUSION

The proposed scheme is the first to handle multiple copies of dynamic data. The communication between the authorized users and the CSP is measured in our method, where the authorized users can simply enter a data reproduction got from the CSP making use of a single secret key shared with the data owner. Additionally, the proposed scheme supports public verifiability, allows for arbitrary quantity auditing, and allows for possession-free verification where the verifier has the potential to verify the data integrity even although they neither possesses nor retrieves the file block from the server.

6. REFERENCES

[1] R. Buyya, C.S. Yeo, S.Venugopal, J. Broberg , and I.Brandic, "Cloud computing and emerging IT platforms", Future generation computer system, vol. 25, no. 6, pp. 599-616, 2009.

[2]. Giuseppe Ateniese, Randal Burns,RezaCurtmola, Joseph Herring, LeaKissner, Zachary Peterson, and Dawn Song, "Provable data possession at untrusted stores".

[3]. F. Sebé, J. Domingo- Ferrer, A. Martinez-Balleste, Y.Deswarte and J.-J. Quisquater,"Efficient remote data possession checking in critical information infrastructures".

[4]. Giuseppe Ateniese, Roberto Di Pietro, Luigi V.Mancini and Gene Tsudik, "Scalable and Efficient Provable Data Possession".

[5]. C. Wang, Q. Wang, K. Ren, and W. Lou.(2009)."Ensuring data security in cloud computing".

[6]. C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession".

[7] G. Ateniese "Provable data possession at untrusted stores".

[8] C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia "Dynamic provable data possession. Cryptology".

[9] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik Scalable and efficient provable data possession".

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus "Scalable secure file sharing on untrusted storage.

[11] B.-G. Chun, F. Dabek, A. Haeberlen, E. Sit, H. Weatherspoon, M. F. Kaashoek, J. Kubiatowicz, and R. Morris "Efficient replica maintenance for distributed storage systems".

[12] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession".

[13] Ayad F.Barsoum and M.Anwar Hasan "Provable possession and replication of data over cloud servers".

[14] H. Shacham and B. Waters "Compact proofs of retrievability".

[15] C. E. Shannon "Communication theory of secrecy systems".