International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Provable Dynamic Data in Cloud Computing Systems

SHAIK NAGUL IMRAN
M.Tech, Software Engineering
JJ Institute Of Information Technology
M. Omprakash
Associate Professor & HOD, Department Of CSE JJ
Institute Of Information Technology

Abstract: Steadily more and more companies are picking out outsourcing data to remote cloud service vendors (CSPs). Clients can appoint the CSPs storage infrastructure to store and get again close to endless amount of data through paying amount per month. On behalf of an improved level of scalability, availability, and sturdiness, some customers may want their data to be virtual on more than one servers throughout multiple data centers. The data owner stores the data in cloud service provider after the encryption. For securing the information Elliptic curve cryptography and Blowfish algorithms are used which is more secured than the advanced Encryption commonplace algorithm. By way of using at ease Hash Algorithm-1 owner can verify the integrity of the data. The data owner update probably the most copies from Cloud service provider and the rest data ought to be updated by using the Cloud service provider. By the way Message Authentication Code can be been up to date after which the client can send the request and receive the data from the Cloud service provider. With the aid of utilising the secure Hash Algorithm-1 the client can determine the integrity of the data, whether it is updated or not.

Key Words: Provable data possession (PDP), storage security, Cloud Service Provider(CSP), Cloud Computing, Dynamic Data.

I. INTRODUCTION

Cloud service provider (CSP) is allows for retailer more data on exclusive computer approach. The data storage infrastructure to store and retrieve data and it store unlimited amount of data. That is from of cloud computing that provides virtualized computing resources over the web. This model is thirdparty supplier hosts hardware, program, server, storage and different infrastructure element on behalf of its users. The clients pay on a per-use basis, commonly through the hour, week or month. Some provider also charge customers based on the quantity of virtual machine space they use. In remote data integrity checking protocols, the client can mission the server in regards to the integrity of a special data file, and the server generates responses proving that it has access to the complete

and uncorrupted data. The basic standards are that the client does now not have got to access the complete common data file when performing the verification of data integrity, and that the client will have to be ready to verify integrity for an limitless quantity of occasions. Juels et al describe a "proof of retrievability" (PoR) model and provides a extra rigorous proof of their scheme. In this model, spot-checking and errorcorrecting codes are used to make sure each "possession" and "retrievability" of data files on archive service systems. Specifically, some distinctive blocks called "sentinels" are randomly embedded into the data file F for detection purpose and F is additional encrypted to look after the positions of these specified blocks. Nevertheless, like [10], the number of queries a client can participate in is PDP is system for validating remote data integrity checking is a vital technology in cloud computing. The two provably-comfortable PDP schemes which might be extra effective than previous options, even in comparison with schemes that gain weaker ensures. In exact, the overhead at the server is low (and even steady), as opposed to linear in the size of the data. Experiments making use of our implementation confirm the practicality of PDP and disclose that the performance of PDP is bounded by way of disk I/O and not through cryptographic computation. Additionally a fixed priori and the introduction of pre-computed "sentinels" prevents the development of realizing dynamic data updates. In addition, public verifiability isn't supported of their scheme. Even though schemes with personal verifiability can attain larger scheme effectivity, public verifiability makes it possible for any individual, no longer just the purchaser (data owner), to task the cloud server for correctness of data storage at the same time maintaining no confidential data.

II. RELATED WORKS

Our contributions may also be overview as follows: i) We propose a map-centered provable multi-copy dynamic data possession (MB-PMDDP) procedure. This system presents an ample assurance that the CSP outlets all copies that are agreed upon within the provider contract. Moreover, the approach helps outsourcing of dynamic data, i.e., it helps blocklevel functions similar to block alteration, insertion, removing, and append. The certified users, who've the correct to access the owner's file, can with ease access the copies acquired from the CSP.

ii) a radical evaluation of MB-PMDDP with a reference scheme, which you can acquire by way of expanding existing PDP models for dynamic single-reproduction data.

iii)We show the safety of our method against colluding servers, and speak a couple of moderate alteration of the proposed scheme to establish corrupted copies.

III. PROPOSED METHOD

The cloud computing data storage model considered in this work consists of three predominant components as illustrated in Fig. 1: (i) a data owner that can be an institution outsourcing data to the cloud server (ii) a CSP who manages cloud servers (CSs) and it presents paid space for storing on its infrastructure to retailer owner's files and (iii) licensed users a collection of owner's clients who've the right to access the remote data seamlessly. The storage model used in this work can be adopted through some of the sensible applications. For instance, e-bank applications will also be picturized by means of this model where the customer's database that involves large and sensitive data can be protected on the cloud servers. In these types of functions, the e-financial institution may also be considered as the data owner, and the employees as the licensed users who have the correct to access the clients' banking historical past.

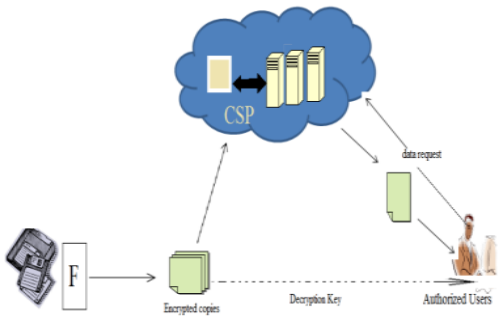

Fig 1: cloud computing data storage model

A. Protocol Design

i) **Data Owner:-**

- Data owner generates keys that are required for sessions.
- It divides the files into blocks.
- These blocks are encrypted.
- These blocks are outsourced to the CSP.
- It receives location tags from the CSP and maintains the location details in it.
- It challenges the CSP to provide proof. It sends challenge to the CSP to verify whether the agreed number of copies are stored in the CSP.

Proof is received by the data owner from different locations that are specified in the tags.

- After receiving the proof, proof is verified. If proof is correct then the exact copies of the files are maintained in the CSP. Then the data owner confirms reliability with the CSP.
- When the authorized users request to grant permission to access the file, data owner will share a key with the user
- and user will access the file with it.

ii) Cloud Service Provider:-

- CSP receives the file blocks outsourced to it.
- CSP creates multiple copies that agreed with the data owner.
- It sends the file copies to the location.
- After sending the file to location, tags are created with the details of the location.
- These created location tags are send to data owner.

- CSP receives a challenge from the data owner.

When challenge is received, it is passed to the locations where the copies are stored. Each location computes a proof and these proofs are passed to the data owner with interactive zero data protocol.

- Operations like insertion, deletion, modification, append are performed in the CSP on file blocks according to data owners' request. Insertion insert a block anywhere in the file. Deletion deletes the block completely. Modification modifies the block content. Append operation adds a new block at the end of the blocks.

- After the operation change must be updated to all the copies present in the CSP.
- Request for accessing the file is received from the authorized users.
- After checking the authenticity encrypted blocks are send to the authorized users.

iii) Authorised Users:-

Authorized users request the data owner to grant permission to access the file from the CSP.

- It will receive a key from the data owner.
- After receiving the key, it will request for the file to the CSP.
- User will receive the encrypted blocks of the file in an unordered manner.
- Blocks are decrypted using the Shared secret key. These blocks are rearranged to get a complete file. Every file can be decrypted with the same key. Users can seamlessly access the file from the CSP.

B. Data Owner Registration:

Data owner need to register the details. After which prefer the data. then it is splitted. A data owner that may be an group will have to preserve the data stored in the clouds database. A Cloud service provider maintains the cloud servers and presents paid storage space to the user. A user is a collection of owner and clients having the right to access the remote server and its data.

C. Data uploading

MAC generated for the splitted data then the data are encrypted and uploaded into the cloud service provider's storage space. The data owner has a file which include multi blocks and the CSP presents to store the multi copies of the owner file on various servers. The vital data must be replicated on multiple servers. On the other hand, non-crucial, reproducible data are saved at diminished levels of redundancy. For data confidentiality, the owner encrypts his data earlier than outsourcing to CSP.

D. Clients Request

Clients send the request to the cloud service provider. Cloud provider vendors send the associated data to the user. An approved user sends a data-access request to the CSP and receives a file replica in an encrypted type. Decryption is done by using using a secret key shared with the owner. The work of the servers will have to be organized utilising the weight balancing mechanism.

D. Users Accessing Data

The data-access request is directed to the server with the bottom congestion clients gaining access to data user get the important thing from the data owner and get the encrypted data from the cloud service provider then decrypts the data. The licensed users have the rights to access the owner file stored on the CSP. A new PDP scheme supports outsourcing of multi-copy dynamic data. Knowledge owner having the potential to updating, scaling and access the data copies stored in the remote servers.

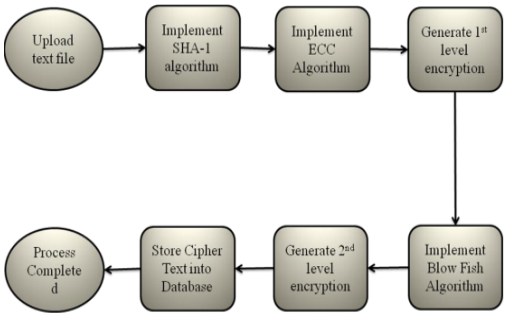

Fig. 2. Multilevel Encryption

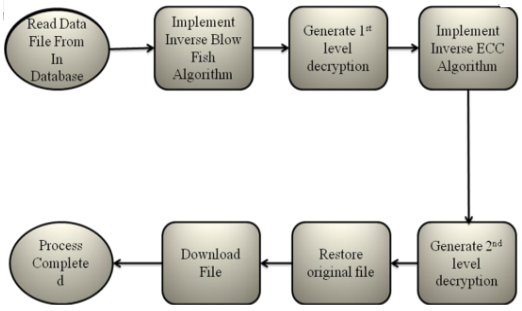

Fig3. Multilevel Decryption

E. Secure Hash Algorithm 1:

SHA1 was developed by the NSA for NIST as part of the Secure Hash Standard (SHS). SHA1 is similar in design to MD4. The original published algorithm, known as SHA, was modified by NSA to protect against an unspecified attack; the updated algorithm is named SHA1.

Step 1:-Padding

Add Padding to the end of the genuine message length is 64 bits and multiple of 512.

Step 2:- Appending length

In this step the excluding length is calculated

Step 3:- Divide the Input into 512-bit blocks

In this step we divide the input in the 512 bit blocks

Step 4:-Initialize chaining variables

In this step we initializing chaining variables here we initialize 5 chaining variables of 32 bit each=160 bit of total.

Step 5:-Process Blocks

1) Copy the chaining variables
2) Divide the 512 into 16 sub blocks
3) Process 4 rounds of 20 steps each [2].

The fig.2 shows one SHA iteration

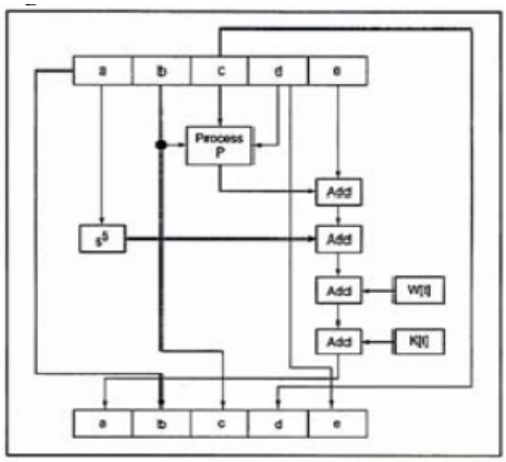

Fig 4:-One SHA iteration

F. The Blowfish algorithm

Blowfish is a symmetric encryption algorithm, which means that it uses the same secret key to both encrypt and decrypt messages. Blowfish can also be a block cipher, which means that it divides a message up into fixed size blocks for the period of encryption and decryption. The block size for Blowfish is 64 bits; messages that don't seem to be a more than one of eight bytes in dimension ought to be padded.

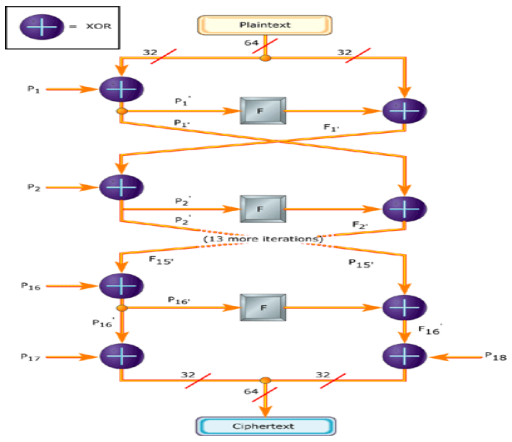

Fig.5: Blowfish algorithm

Blowfish requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 clock cycles. (Not-so-careful implementations, like Kocher, don't increase that time by much.) Longer messages increase computation time in a linear fashion; for example, a 128-bit message takes

about (2 x 12) clocks. Blowfish works with keys up to 448 bits in length.

G. Elliptic Curve Cryptography

It is Elliptic Curve Cryptography. ECC was introduced by Victor Miller and Neal Koblitz in 1985.It uses Asymmetric Key Algorithm. It uses 224 bit key length. For DSA, RSA we need larger key length.ECC requires significantly smaller key size with same level of security as DSA & RSA. Although it has smaller Key length, it provides higher Security equivalent to RSA. Since it is asymmetric, it has greater efficiency. Having Smaller Key Size, it has faster computations and needs less storage space.

IV. CONCLUSION

Data proprietor may additionally affirm that the data copies are stored within the correct numbers and in different vicinity. Approved clients can interact with CSP, the place the authorized users can seamlessly access a data reproduction received from the CSP utilizing a single secret key shared with the data owner. Proposed scheme supports public verifiability, permits auditing, and allows possession free verification the place the verifier has the ability to affirm the data integrity despite the fact that he neither possess nor retrieved the file block from the server. The TB-PMDDP needs excessive storage. So it leads to storage overhead. The remote method needs excessive computation for entire the mission. The MBPMDDP scheme reduces the computation time. The data owner retailers the data within the cloud service provider. Multi copies are generated for the data stored in the cloud service provider. with the helip of Blowfish algorithm and Secure Hash Algorithm 1.

REFERENCES

[1] Ayad F. Barsoum and M. Anwar Hasan, "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems,"2015.

[2] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," 2010.

[3] A. F. Barsoum and M. A. Hasan. "On verifying dynamic multiple data copies over cloud servers," 2011.

[4] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," 2007.

[5] Kochumol Abraham, Win Mathew John, "Proving Possession and Retrievability within a Cloud Environment: A Comparative Survey", 2014.

[6] A. F. Barsoum and M. A. Hasan. "Provable possession and replication of data over cloud servers," 2010.

[7] G. Ateniese et al., ―Provable data possession at untrusted stores,‖ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[8] K. Zeng, ―Publicly verifiable remote data integrity,‖ in Proc. 10th Int. Conf. Inf. Commun. Secur. (ICICS), 2008, pp. 419–434.

[9] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, ―Remote integrity checking,‖ in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[10] D. L. G. Filho and P. S. L. M. Barreto, ―Demonstrating data possession and uncheatable data transfer, IACR (International Association for Cryptologic Research) ePrint Archive, Tech. Rep. 2006/150, 2006.

Author's Profile

SHAIK NAGUL IMRAN pursing M.Tech in Software Engineering from **JJ INSTITUTE OF INFORMATION TECHNOLOGY**

M.OMPRAKASH working as Associate Professor & HOD, Department of CSE in **JJ INSTITUTE OF INFORMATION TECHNOLOGY**