IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

A Security of Cloud Data Storage Using AF Crawler Algorithm in Cloud Computing Systems

N.Sheeba Pershi[1*], G.Sathish Kumar[2]

[1]*M.Tech Scholar, Department of Computer Science & Engineering, MNSK College of Engineering, Pudukkottai*
[2] *Head, Department of Computer Science & Engineering, MNSK College of Engineering, Pudukkottai*

www.ijcseonline.org

Received: Mar/23/2016 Revised: Apr /03/2016 Accepted: Apr/19/2016 Published: Apr/30/2016

Abstract— Gradually more furthermore, more associations are opting for outsourcing information to remote cloud administration providers (CSPs). clients can rent the CSPs capacity foundation to store furthermore, get back almost limitless sum of information by paying sum per month. On behalf of an improved level of scalability, availability, furthermore, durability, some clients may want their information to be virtual on distinctive servers over distinctive information centers. The more duplicates the CSP is asked to store, the more sum the clients are charged. As a result, clients need to have a solid assurance that the CSP is storing all information duplicates that are chosen upon in the administration contract, furthermore, all these duplicates are reliable with the most later changes issued by the clients. Map-based provable multi-copy dynamic information ownership (MB-PMDDP) technique is being proposed in this paper furthermore, comprises of the following features: 1) it affords an proof to the clients that the CSP is not degenerate by storing less copies; 2) it bolsters outsourcing of dynamic data, i.e., it bolsters block-level functions, such as square alteration, addition, deletion, furthermore, append; furthermore, 3) it licenses official clients to easily access the record duplicates stored by the CSP. In addition, we discuss the security against conspiring servers, furthermore, discuss how to perceive tainted duplicates by a little revising the projected scheme.

Keywords— *Cloud Computing, Dynamic Environment, Data Copy, Outsourcing Data Storage.*

I. INTRODUCTION

Outsourcing information to a remote cloud administration provider (CSP) licenses society to store additional information on the CSP than on private computer systems. Such Out sourcing of information capacity licenses society to focus on improvement furthermore, relieves the load of constant server updates furthermore, other registering matter. On one occasion the information has been outsourced to a remote CSP which may not be dependable, the information proprietors drop the direct control over their private data. This need of control raises new difficult furthermore, demanding tasks associated to information secrecy furthermore, respectability insurance in cloud computing. The secrecy issue can be feeling by encrypting private information before outsourcing to remote servers. As such, it is a vital demand, of clients to have solid proofs that the cloud servers still have their information furthermore, it is not being degenerate with or partially erased over time. As a result, numerous researchers have played consideration on the problem of provable information ownership (PDP) furthermore, proposed distinctive frameworks to audit the information stored on remote servers.

PDP is a technique for authenticating information respectability over remote servers. In a typical PDP model, the information proprietors produce some maintain formation for an information record to be utilized later for check purposes through a challenge-reaction protocol with the remote/cloud server. The proprietor sends the record to be stored on a remote server which may be untrusted, furthermore, erases the neighborhood duplicate of the file. One of the center plan ethics of outsourcing information is to provide dynamic behavior of information for a variety of applications. This means that the slightly stored information can be not only accessed by the approved users, but too effective furthermore, scaled Examples of PDP constructions that bargain with dynamic information -. The final are how-ever for a single duplicate of the information file. PDP technique has been obtainable for distinctive duplicates of static information –. PDP framework directly deals with distinctive duplicates of dynamic data. When proving distinctive information copies, generally framework respectability check fails if there is one or more tainted duplicates were present. To bargain with this issue furthermore, perceive which duplicates have been corrupted, a slight modification has been associated to the proposed scheme.

II. RELATED WORK: OUR CONTRIBUTIONS

Our contributions can be audit as follows:

i) We propose a map-based provable multi-copy dynamic information ownership (MB-PMDDP) method. This technique provides an sufficient ensure that the CSP stores all duplicates that are agreed upon in the administration contract. Additionally, the technique bolsters outsourcing of dynamic data, i.e., it bolsters block level capacities such as square alteration, insertion, removal, furthermore, append. The certified users, who have the right to access the owner's file, can easily access the duplicates gotten from the CSP.

ii) A thorough comparison of MB-PMDDP with a reference scheme, which one can obtain by expanding existing PDP models for dynamic single-duplicate data.

iii) We show the security of our framework against conspiring servers, furthermore, talk about a slight adjustment of the proposed plan to distinguish tainted copies. Remark 1: Proof of irretrievability (POR) is a adjusting approach to PDP, furthermore, is stronger than PDP in the sense that the verifier can revamp the entire record from answers that are consistently transmitted from the server. This is due to encoding of the information file, for case utilizing erasure codes, before outsourcing to remote servers. A range of POR frameworks can be found in the journalism, for case –, which focuses on static data. In this work, we do not instruct the information to be outsourced for the following reasons. Primarily, we are dealing with dynamic data, furthermore, consequently if the information record is encoded before outsourcing, modifying a segment of the record needs re-encoding the information record which may not be suitable in reasonable applications due to high calculation transparency. Secondly, we are permitting for economically-motivated CSPs that may challenge to use less capacity than essential by the administration agreement through cancellation of a few duplicates of the file. The CSPs have approximately no economic benefit by evacuating only a little segment of a duplicate of the file. Thirdly, furthermore, more significantly, unlike evacuation codes, duplicating information documents transversely distinctive servers attains adaptability which is a basic client constraint in CC systems. A record that is copied furthermore, stored deliberately on distinctive servers – situated at different geographic areas – can help decrease access time furthermore, correspondence fetched for users. In addition, a server's duplicate can be rebuilt indeed from a whole harm utilizing copied duplicates on other servers.

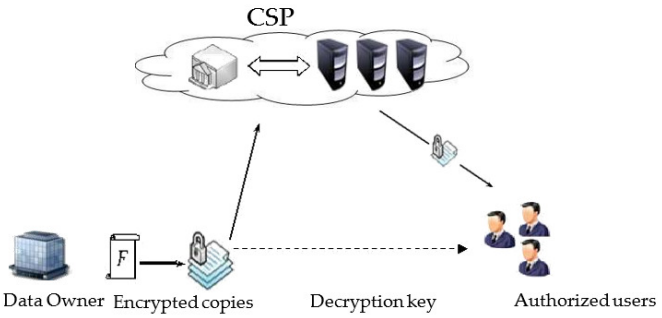

Figure: 1 Framework Architecture

A. Framework Components

The cloud registering capacity model measured in this work incorporates three main components as illustrated in Fig. 1:

(i) A information proprietor that can be an association initially possessing private information to be stored in the cloud.

(ii) A CSP who handles cloud servers (CSs) furthermore, offers paid capacity space on its foundation to store the owner's files.

(iii) Approved clients — a set of owner's clients who have the right to access the remote data.

The capacity model utilized in this work can be assumed by much reasonable requests. For example, e-Health applications can be predicted by this model where the patients' database that incorporates substantial furthermore, private information can be stored on the cloud servers. In these types of applications, the e-Health association can be measured as the information owner, furthermore, the physicians as the approved clients who have the right to access the patients' medical history. Numerous other reasonable applications like financial, scientific, furthermore, educational applications can be watched in similar settings.

B. Outsourcing, Updating, furthermore, Accessing

The information proprietor has a record F consisting of m squares furthermore, the CSP offers to store n duplicates *{ F1,F2, ……..,Fn}* of the Owner's record on distinctive servers — to prevent simultaneous disappointment of all duplicates — in exchange of pre-specified fees in the structure of GB/month. The number of duplicates depends on the nature of data; more duplicates are desired for basic information that cannot easily be replicated, furthermore, to attain a higher level of scalability. This basic information be

supposed to be recreated on distinctive servers over distinctive information centers. On the other hand, non-critical, reproducible information are stored at compact levels of redundancy. The CSP fetched model is connected to the number of information copies.

For information privacy, the proprietor encrypts their information before outsourcing to CSP. After outsourcing all n duplicates of the file, the proprietor may work together with the CSP to carry out block-level capacities on all copies. These capacities contains alter, insert, append, furthermore, remove particular squares of the outsourced information copies.

An approved client of the outsourced information throws a data-access request to the CSP furthermore, accepts a record duplicate in an encrypted structure that can be decrypted utilizing a mystery key shared with the owner. According to the load adjusting device utilized by the CSP to orchestrate the work of the servers, the data-access demand, is directed to the server with the lowest jamming, furthermore, as a result the client is not conscious of which duplicate has been received.

We imagine that the correspondence between the proprietor furthermore, the official clients to verify their identities furthermore, share the mystery key has previously been completed.

C. Threat Model

The respectability of customers' information in the cloud may be at danger due to the following reasons. Firstly, the CSP- whose goal is probable to make a profit furthermore, sustain a reputation-has an reason to hide information loss (due to hardware failure, management errors, different attacks) or get back capacity by evacuating information that has not been or is rarely accessed. Secondly, a dishonest CSP may store less duplicates than what has been chosen upon in the administration contact with the information owner, furthermore, try to induce the proprietor that all duplicates are correctly stored intact. Thirdly, to save the computational resources, the CSP may totally pay no consideration to the data update demands concerned by the owner, or not execute them on all duplicates leading to inconsistency between the record copies. The objective of the proposed plan is to distinguish (with high probability) the CSP misconduct by validating the number furthermore, respectability of record copies.

2.1 MB-PMDDP PLAN

A. Overview furthermore, Rationale

Produce unique differentiable duplicates of the information record is the center to plan a provable multi-copy information ownership scheme. Identical duplicates enable the CSP to simply deceive the proprietor by storing only one duplicate furthermore, pretending that it stores distinctive copies. Utilizing a simple yet effective way, the proposed plan generates particular duplicates utilizing the dispersion property of any secure encryption scheme. The dispersion property ensures that the output bits of the ciphertext depend on the input bits of the plaintext in a very complex way, i.e., there will be an unpredictable complete change in the ciphertext, if there is a single bit change in the plaintext. The interaction between the approved clients furthermore, the CSP is considered through this methodology of generating particular copies, where the former can decrypt/access a record duplicate gotten from the CSP. In the proposed scheme, the approved clients need only to keep a single mystery key (shared with the information owner) to decrypt the record copy, furthermore, it is not necessarily to perceive the record of the gotten copy.

In this work, we propose a MB-PMDDP plan permitting the information proprietor to update furthermore, scale the squares of record duplicates outsourced to cloud servers which may be untrusted. Validating such duplicates of dynamic information requires the knowledge of the square versions to ensure that the information squares in all duplicates are consistent with the most later changes issued by the owner. Furthermore, the verifier should be aware of the square records to ensure that the CSP has inserted or added the new squares at the requested positions in all copies. To this end, the proposed plan is based on utilizing a little information structure (metadata), which we call a map structure table.

B. Map-Structure Table

The map-structure table (MVT) is a little dynamic information structure accumulates on the verifier side to verify the reliability furthermore, uniformity of all record duplicates outsourced to the CSP. The MVT comprises of three columns: serial number (SN), square number (BN), furthermore, square structure (BV). The SN is an indexing to the record blocks. It point out the physical position of a square in a information file. The BN is a counter utilized to make a intelligent numbering/indexing to the record blocks. Therefore, the relation between BN furthermore, SN can be watched as a mapping between the intelligent number BN furthermore, the physical position SN. The BV specifies the current structure of record blocks. When a information

record is originally created the BV of each square is 1. If a particular square is being updated, its BV is incremented by 1.

Remark 2: It is significant to note that the verifier remain only one table for limitless number of record copies, i.e., the capacity condition on the verifier side does not depend on the number of record duplicates on cloud servers. For n duplicates of a information record of size | G|, the capacity condition on the CSP side is O (n| G|), while the verifier's overhead is O (m) for all record duplicates (m is the number of record blocks).

Remark 3: The MVT is associated as a connected list to make simpler the insertion cancellation of table entries. For actual achievement, the SN is not needed to be stored in the table; SN is considered to be the entry/table index, i.e., each table section contains just two integers BN furthermore, BV (8 bytes). As a result, the complete table size is 8m bytes for all record copies. We additionally note that indeed if the table size is linear to the record size, in practice the previous would be smaller by several orders of magnitude. For instance, outsourcing limitless number of record duplicates of a 1GB-record with 16KB square size requires a verifier to keep MVT of only 512KB (< 0.05% of the record size).

III. IMPLEMENTATION

Our usage of the presented schemes comprises of three modules: OModule (proprietor module), CModule (CSP module), furthermore, VModule (verifier module). OModule, which runs on the proprietor side, is a library that incorporates KeyGen, CopyGen, TagGen, algorithms. CModule is a library that runs on Amazon EC2 furthermore, incorporates Execute Update furthermore, Prove algorithms. VModule is a library to be run at the verifier side furthermore, incorporates the Verify algorithm.

In the experiments, we do not believe the framework preprocessing time to orchestrate the distinctive record duplicates furthermore, produce the tags set. This pre-processing is complete only once amid the life time of the plan which may be for tens of years. Furthermore, in the usage we do not think the time to access the record blocks, as the state-of-the-art hard drive

Proposed System

In proposed system, AF Crawler scheme is used for corruption of dynamic data .This scheme provides an adequate guarantee that the CSP stores all copies that are agreed upon in the service contract. Moreover, the scheme supports outsourcing of dynamic data, and it supports block-level operations such as block modification, insertion, deletion, and append. The authorized users, who have the right to access the owner's file, can seamlessly access the copies received from the CSP. AF Crawler technique can obtain by extending existing PDP models for dynamic single-copy data and data replication. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations on the data fragmentation. We also report our implementation and experiments using Cloud server. This provide the security of our scheme against colluding servers, and discuss a slight modification of the proposed scheme to identify corrupted copies.

Advantages:

- Utilization is very effective and efficiency.
- Proof for the utilization of the spaces allocated.
- It provides evidence to the customers that the CSP is not cheating by storing fewer copies.
- It supports outsourcing of dynamic data, and it supports block-level operations, such as block modification, insertion, deletion, and append.

System Architecture

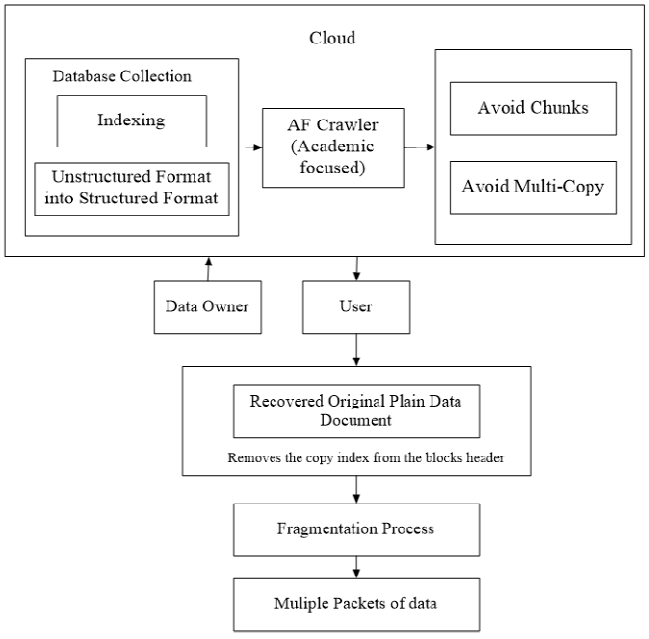

Figure 2. Proposed Architecture

IV. CONCLUSION

We have proposed a new AF Crawler algorithm, which supports outsourcing of multi-copy dynamic data, where the data owner is capable of not only archiving and accessing the data copies stored by the CSP, but also updating and scaling these copies on the remote servers. The interaction

between the authorized users and the CSP is considered in our scheme, where the authorized users can seamlessly access a data copy received from the CSP using a single secret key shared with the data owner. Moreover, the proposed scheme supports public verifiability, enables arbitrary number of auditing, and allows possession-free verification where the verifier has the ability to verify the data integrity even though he neither possesses nor retrieves the file blocks from the server. AF Crawler scheme significantly reduces the computation time during the challenge-response phase which makes it more practical for applications where a large number of verifiers are connected to the CSP causing a huge computation overhead on the servers.

A slight modification can be done on the proposed scheme to support the feature of identifying the indices of corrupted copies. The corrupted data copy can be reconstructed even from a complete damage using duplicated copies on other servers. Through security analysis, we have shown that the proposed scheme is provably secure.

Future Enhancement

In cloud data, user can be strong belief for his uploaded data for any future purpose or his any other related process without worry. Here complicated, internal, external and malevolent attack is known by our proposed scheme in efficient manner by storage data measurement (i.e., since there can be some modifications in cloud data). Thus our main idea is to give integrity to the cloud storage area with strong trustworthiness so that user can feel free of worry for his uploaded data in his allocated space. Here our scheme ensures for any extra inclusion of unwanted bits or related things in cloud area so that they can be so easily found out by our data measurement concepts in efficient manner. And it finds out how much of changes have occurred there in its cloud area.

References:

[1] Zhou Peng; Jinhua Zheng; Juan Zou, “A population diversity maintaining strategy based on dynamic environment evolutionary model for dynamic multi objective optimization”, 2014 IEEE Congress on Evolutionary Computation (CEC),Year: 2014, Pages: 274 – 281.

[2] Shivlal Mewada, Umesh Kumar Singh, Pradeep Sharma, “Security Based Model for Cloud Computing”, International Journal of Computer Networks and Wireless Communications Vol. 1(1), pp (13-19), December 2011.

[3] Ling Zhang; Yan-bin Liu, “The influence of dynamic environment and resource allocation on enterprises financial performance”, Management Science and Engineering (ICMSE), 2012 International Conference on, Year: 2012, Pages: 1314 – 1320.

[4] Inderjeet Singh Dogra; Ziad Kobti, “Improving prediction accuracy in agent based modeling systems under dynamic environment”, 2013 IEEE Congress on Evolutionary Computation, Year: 2013, Pages: 2114 – 2121.

[5] C. E. Campbell; G. McCulley, “Terrain reasoning challenges in the CCTT dynamic environment”, AI Simulation, and Planning in High Autonomy Systems, 1994. Distributed Interactive Simulation Environments, Proceedings of the Fifth Annual Conference on, Year: 1994,Pages: 55 – 61.

[6] Aameek Singh; Ling Liu, “Sharoes: A Data Sharing Platform for Outsourced Enterprise StorageEnvironments”, 2008 IEEE 24th International Conference on Data Engineering, Year: 2008, Pages: 993 – 1002.

[7] Shaheen Ayyub and Devshree Roy, "Cloud Computing Characteristics and Security Issues", International Journal of Computer Sciences and Engineering, Volume-01, Issue-04, Page No (18-22), Dec -2013,

[8] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "Security Enhancement in Cloud Computing (CC)", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Vol.-01, Issue-01, pp (31-37), Jan -Feb 2013

[9] Harsh Yadav; Mayank Dave, “Secure data storage operations with verifiable outsourced decryption for mobile cloud computing”, Recent Advances and Innovations in Engineering (ICRAIE), 2014, Year: 2014, Pages: 1 – 5.

[10] B.Subasri, P.Vijayalakshmi, P.Yurega and E.Revathi, "Improving Zero Knowledge in Cloud Storage Auditing System", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (204-207), Mar -2014

[11] Juan Camilo Corena; Anirban Basu; Shinsaku Kiyomoto; Yutaka Miyake; Tomoaki Ohtsuki, “Beyond proofs of data possession: Finding defective blocks in outsourced storage”, 2014 IEEE Global Communications Conference, Year: 2014,Pages: 2381 - 2386

[12] Ayad F. Barsoum; M. Anwar Hasan, “Provable Multicopy Dynamic Data Possession in Cloud Computing Systems”, IEEE Transactions on Information Forensics and Security, Year: 2015, Volume: 10, Issue: 3, Pages: 485 – 497.

[13] Qia Wang; Wenjun Zeng; Jun Tian, “A Compressive Sensing Based Secure Watermark Detection and Privacy Preserving Storage Framework”, IEEE Transactions on Image Processing, Year: 2014, Volume: 23, Issue: 3, Pages: 1317 – 1328.

[14] Xiuxia Tian; Ling Huang; Tony Wu; Xiaoling Wang; Aoying Zhou, "CloudKeyBank: Privacy and Owner Authorization Enforced Key Management Framework", IEEE Transactions on Knowledge and Data Engineering, Year: 2015, Volume: 27, Issue: 12, Pages: 3217 – 3230.

[15] Ankita Lathey; Pradeep K. Atrey; Nishant Joshi, "Homomorphic Low Pass Filtering on Encrypted Multimedia over Cloud", Semantic Computing (ICSC), 2013 IEEE Seventh International Conference on, Year: 2013, Pages: 310 – 313.

