Review of International Geographical Education | RIGEO | 2020

RIGEO

ISSN: 2146 - 0353

Review of International GEOGRAPHICAL EDUCATION

www.rigeo.org

DATA INTEGRITY VERIFICATION USING OPERATION RECORD TABLE IN CLOUD COMPUTING

[1] Eedunuri Muralidhar Reddy,[2] TSKS jyothirmayi, [3] Y Pavan Kumar Gupta, [4] B Sumalatha

[1,2,3,4] Assistant Professor, Department of Computer Science Engineering,

Pallavi Engineering College, Hayathnagar_Khalsa, Hyderabad, Telangana 501505

Article Info

Received: 03-09-2023 *Revised: 13 -10-2023* *Accepted: 23-11-2023*

Abstract

As crucial software in cloud computing, cloud garage offers consumer scalable, flexible and excessive first-rate statistics garage and computation offerings. A developing number of data owners pick to outsource information documents to the cloud. Because cloud garage servers aren't fully trustworthy, information owners need reliable approach to test the possession for his or her documents outsourced too far off cloud servers. To deal with this vital problem, a few faraway statistics ownership checking (RDPC) protocols were supplied. But many existing schemes have vulnerabilities in performance or facts dynamics. In this paper, we offer a new green RDPC protocol based totally on homomorphic hash function. The new scheme is provably relaxed towards forgery attack, replace attack and replay assault primarily based on an average security model. To guide facts dynamics, an operation file desk (ORT) is delivered to track operations on document blocks. We similarly deliver a brand new optimized implementation for the ORT which makes the cost of getting access to ORT almost constant. Moreover, we make the complete performance evaluation which suggests that our scheme has advantages in computation and verbal exchange costs. Information protection, from time to time shortened to InfoSec, is the exercise of stopping unauthorized get right of entry to, use, disclosure, disruption, modification, inspection, recording or destruction of facts. It is a general time period that may be used irrespective of the shape the information may take (e.g. Digital, bodily). Network protection consists of the rules and practices adopted to save you and monitor unauthorized get admission to, misuse, modification, or denial of a computer community and community-available resources. Network protection includes the authorization of get admission to information in a network, that's controlled by using the network administrator. Users choose or are assigned an ID and password or different authenticating facts that permits them get admission to statistics and packages inside their authority. Network protection covers a selection of laptop networks, both public and personal, which can be utilized in normal jobs; carrying out transactions and communications among groups, government businesses and individuals. Networks may be non-public, along with inside a enterprise, and others which is probably open to public get entry to. Network safety is worried in companies, businesses, and other sorts of establishments. It does as its name explains: It secures the community, as well as protective and overseeing operations being performed. The maximum not unusual and easy manner of protecting a network aid is by assigning it a unique call and a corresponding password.

Keywords: - SHA-256 algorithm, Hash Code for checking, RDPC, Operation Record Table.

1. INTRODUCTION

Cloud computing emerges as a unique computing paradigm subsequent to grid computing. By dealing with a great variety of dispensed computing assets in Internet, it possesses large virtualized computing capacity and storage space. Thus, cloud computing is extensively customary and used in many actual applications. As an crucial service for cloud computing, cloud service issuer elements dependable, scalable, and occasional-cost outsourced garage service to the customers. It affords the users with a greater flexible way referred to as pay-as-you-pass model to get computation and garage resources on-call for. Under this version, the users can rent necessary IT infrastructures in step with their requirement in place of purchase them. Thus, the up-the front funding of the users may be reduced greatly. In addition, it's far convenient for them to regulate the ability of the rented aid while the scale in their programs changes. Cloud service company tries to offer apromising carrier for data storage, which saves the users charges of funding and aid. Nonetheless, cloud garage additionally brings numerous protection problems for the outsourced information. Although a few protection problems had been solved, the critical challenges of statistics tampering and records lost still exist in cloud storage. On the one hand, the coincidence disk error or hardware failure of the cloud garage server (CSS) may also purpose the sudden corruption of outsourced documents. On the alternative hand, the CSS is not fully straightforward from the perspective of the facts proprietor, it may actively delete or modify files for great economic advantages. At the same time, CSS may also hide the misbehaviors and data loss accidents from statistics proprietor to preserve an awesome popularity. Therefore, it is vital for the information proprietor to utilize an efficient manner to test the integrity for outsourced information. Remote data ownership checking (RDPC) is an powerful approach to

make sure the integrity for facts documents saved on CSS. RDPC materials a way for facts owner to efficiently verify whether cloud provider issuer faithfully shops the original files without retrieving it. In RDPC, the records owner is able to assignment the CSS on the integrity for the goal report. The CSS can generate proofs to show that it keeps the entire and uncorrupted records. The essential requirement is that the information proprietor can perform the verification of file integrity without accessing the entire authentic record. Moreover, the protocol need to resist the malicious server which attempts to affirm the data integrity without gaining access to the entire and uncorrupted facts. Another preferred requirement is that dynamic statistics operations ought to be supported by using the protocol. In preferred, the facts proprietor can also append, insert, delete or adjust the record blocks as needed. Besides, the computing complexity and verbal exchange overhead of the protocol need to be taken under consideration for real applications.

2. RELATED WORK

Review of related work

Cloud provider issuer attempts to offer a promising carrier for statistics garage, which saves the customers costs of funding and useful resource. Nonetheless, cloud garageadditionally brings diverse s safety troubles forth outsourced records. Although some protection problems had been solved the important challenges of information tampering and information lost nevertheless exist in cloud storage. On the only hand, the coincidence disk blunders or hardware failure of the cloud garage server (CSS) might also motive the unexpected corruption of outsourced files. On the opposite hand, the CSS isn't completely trustworthy from the attitude of the statistics proprietor; it is able to actively delete or regulate files for first-rate financial blessings. At the same time, CSS might also cover the misbehaviors and records loss injuries from facts proprietor to maintain a great reputation.The main RDPC was proposed by Deswarte et al. [11] predicated on RSA hash work. The downside of this plan is that it requires to get to the whole document obstructs for each test. In 2007, the provable information ownership (PDP) display was introduced by Ateniese et al. [12], which used the probabilistic verification system for remote information uprightness checking without getting to the entire record. In reconciliation, they provided two solid plans (S-PDP, E-PDP) predicated on RSA. Yet these two conventions had great execution, it's a pity they didn't strengthen dynamic tasks.Another branch of remote information checking is confirmation of retrievability (PoR) which has additional capacity of recuperating record if there should arise an occurrence of disappointment contrasted and PDP. In 2007, Juels and Kaliski [13] proposed the idea for PoR and formalized the definition and security necessity. They displayed a PoR conspire utilizing sentinels and blunder adjusting code to demonstrate document uprightness and recoup target file. Shacham and Waters [14] gave two productive and minimized PoR conventions, which were based on BLS marks [15] and pseudorandom works individually. As of late, a few PoR conventions were proposed to upgrade the security and enhance the effectiveness.

In 2008, Curtmola et al. [16] first considered the remote honesty checking for various copies in cloud setting. They proposed a situation that the information proprietor put away certain reproductions of a considerable document on the server, it is required to check whether every one of these copies are kept flawless. To accomplish this objective, they exhibited a provable secure numerous imitations PDP plot. Hao and Yu [17] proposed a RDPC convention for the different copies with open undeniable nature and security protection. Mukundan et al. [18] introduced a dynamic numerous copies PDP, which braced unique tasks on reproductions while holding the highlights of various imitations respectability checking.

3. PROPOSED SYSTEM

It is important for records owners to affirm the integrity for the statistics saved on CSS before the usage of it. For instance, a large worldwide trading organization stores all the imports and exports report files on CSS. According to those files, the employer can get the important thing information including the logistics quantity, the alternate extent and so on. If any document file is discarded or tampered, the organization will suffer from a huge loss which might also reason awful have an effect on its commercial enterprise and improvement. To keep away from this sort of occasions, it's far obligatory to check the integrity for outsourced information files. Furthermore, considering the fact that those documents may consult with enterprise mystery, any facts exposure is unacceptable. If the company competitor can execute the report integrity checking, by often checking the documents they'll gain some useful facts which include when the record modifications, the boom fee of the document and so on, by way of which they can guess the development of the business enterprise. Thus, to keep away from this example, we don't forget the personal verification kind in our scheme, this is, the data owner is the particular verifier. In reality, the cutting-edge research direction of RDPC makes a speciality of the general public verification, wherein anyone can carry out the challenge of record integrity checking with the system public key. Although RDPC with public verification, appears better than that with non-public verification, but it's miles mistaken to the scenario stated above. Motivated by means of the above software eventualities, we gift a novel green RDPC scheme by using homomorphic hash feature, which has been used to construct RDPC schemes. Unfortunately, these schemes are either insecure or now not efficient enough. To conquer those drawbacks, we talk to the idea of and introduce a non-public key for every tag generation in our RDPC scheme. Simultaneously, a brand new construction of ORT is provided for records dynamic that can improve the performance of the protocol greatly. Compared with the previous ones, our scheme has higher performance in term of computation and communique. Our contributions are summarized as follows: We gift a singular efficient dynamics. The simple scheme makes use of homomorphic hash characteristic method, wherein the hash fee of the sum for two blocks is same to the product for two hash values of the corresponding blocks. We introduce a linear desk called ORT to record statistics operations for supporting information dynamics such as block modification, block insertion and block deletion. To enhance the performance for getting access to ORT, we make use of doubly related list and array to offer an optimized implementation of ORT which reduces the price to nearly steady stage. We prove the offered scheme is at ease against forgery attack, replay attack and replace attack based on atypical safety model. At ultimate we put in force our scheme and make thorough contrast with preceding schemes. Experiment consequences display that the new scheme has better overall performance and impractical for real applications.

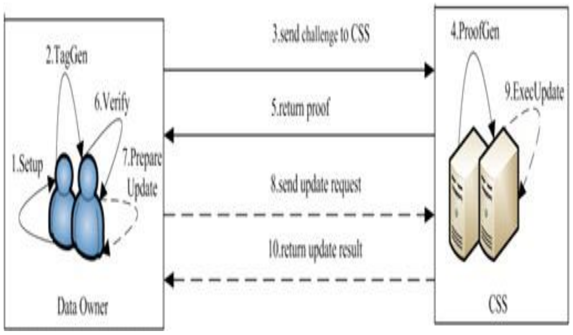

Fig.1 System Architecture

Data Owner: That can be an organization or a person in the beginning possessing Sensitive data to be shop inside the cloud. In proposed system statistics owner is industry proprietor.

CSS: Who manages Cloud Servers (CSs) and provide paid garage space on its infrastructure to stores documents. In proposed device CSP offer public cloud that may be offer by using Google, Rackspace, and so on.

Verifier:

It may be Data Owner or Third Party Auditor or Authorized User. In advocate system manager or proprietor or employee of industry may be the verifier

File Division:

User's document is split into data blocks of different sizes for enhancing the efficiency of garage and as well as to improve security of document.

Integrity Verification:

Verifier randomly sends a venture to the CSP to test integrity and consistency of report copies then CSP send proof of that undertaking and finally verifier take a look at is it accurate or not without downloading of documents copies.

ORT (Operation Record) Table:

To support dynamic operations on report blocks, we introduce a easy bendy facts structure named operation document table (ORT). The desk is reserved on the records owner facet and used to record all the dynamic behaviors on report blocks. ORT has a easy shape with most effective three columns, this is Block Position BP ( ), Block Index BI ( ) and Block Version ( ) BV. The BP represents the bodily index for the contemporary block inside the document; normally its cost is incremented by way of 1. The BI represents the logical index for the contemporary block, which isn't always vital equal to BP however relevant with the time when the block seems inside the document. The BV indicates the present day version for the block. If the statistics file is initially created, the BV values for all blocks are 1. When one concrete block is up to date, its BV cost is incremented by means of 1. It is stated that the use of the ORT desk will boom the garage overhead of the facts proprietor through O n ( ), in which n is the count of blocks.

Advantages:

1. We can reduce the storage space.

2. We can keep community round trips.

For locating reproduction record we use SHA-256 set of rules for producing Hash Code for checking cloud with any report is matched.

SHA-256 Algorithm:

SHA-256 both use six logical functions, where each function operates on 32-bit words, which are represented as x, y, and z.

The result of each function is a new 32-bit word.

$$
\begin{aligned}
Ch(x,y,z) &= (x\wedge y)\oplus(\neg x\wedge z)\\
Maj(x,y,z) &= (x\wedge y)\oplus(x\wedge z)\oplus(y\wedge z)
\end{aligned}
$$

$$
\begin{aligned}
\textstyle\sum_0^{\{256\}}(x) &= ROTR^{2}(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)\\
\textstyle\sum_1^{\{256\}}(x) &= ROTR^{6}(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)\\
\sigma_0^{\{256\}}(x) &= ROTR^{7}(x) \oplus ROTR^{18}(x) \oplus SHR^{3}(x)\\
\sigma_1^{\{256\}}(x) &= ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)
\end{aligned}
$$

4. RESULTS

Our plan is based on a safe homomorphic hash capacity and backings completely unique tasks about squares including addition, erasure and adjustment. Another light weight information structure called ORT is received to acknowledge dynamic activities. By presenting a novel advanced usage of ORT, we lessen the cost of getting to ORT to almost consistent level. In the mean time, our plan has no confinements on the confirmation times and tested square numbers, which can be set unreservedly by the information proprietors as indicated by their prerequisites. To exhibit the highlights of our plan, we list the complete productivity correlation for our plan with the best in class. Further, we will break down the point by point cost of our RDPC plot.

Calculation cost: The Calculation cost will performed tosecluded exponentiation, pseudo-arbitrary number age, change activity, hash task and expansion activity individually. Setup calculation keeps running on the information proprietor side, it is in charge of yielding homomorphic key and private key (key size minimum 512bits).The calculation cost of Setup can't be affirmed entirely on the grounds that it is identified with the methods for creating huge primes p , q and the vector g. Hence we can't give the particular hypothetical estimations of the Setup calculation cost, however we will demonstrate the continuous spend in the test later, which can give us a more clear learning than the hypothetical examination. Be that as it may, Setup will run just once in framework. Regardless of how much time it costs, the effect on the calculation overhead of the information proprietor is practically nothing. In this way, we disregard the Setup cost in the accompanying investigation about the calculations cost for the information proprietor.

Capacity cost: In our plan, the capacity cost of the information proprietor just contains homomorphic key, private key and the ORT, which is upper bound by 2 | p + (1) | m q +12n . With respect to the capacity cost of CSS, it incorporates two sections: document and labels, so the upper bound of the CSS stockpiling cost is nm q | + n p |.

Correspondence cost: In a total procedure of test, the information proprietor initially sends the test chal=(c, k1, k2) to CSS, at that point CSS restores the verification (F, T) to the information proprietor. So the correspondence cost for the test is log c + (m+2) |q| + |p|.

With a specific end goal to show the effectiveness of our cross breed information structure regarding square updates, we direct another 'embed squares' test on 1MB record. The measure of square is set to be 16KB the aggregate check of squares is 536. We understand the ORT by exhibit, connected rundown and our cross breed information structure individually. In view of these three sorts of ORT, we as often as possible embed squares to arbitrary places of the record. We run the trials 100 times for each condition, at that point we got the normal time cost. By Implementation of this paper it can achieve 95% security and integrity of cloud data.

5. CONCLUSION

In this paper, we observe the issue for integrity checking of information files outsourced to faraway server and recommend an efficient at ease RDPC protocol with records dynamic. Our scheme employs a homomorphic hash feature to confirm the integrity for the files saved on far off server, and reduces the storage prices and computation costs of the records owner. We design a new light-weight hybrid records shape to assist dynamic operations on blocks which incurs minimum computation costs with the aid of lowering the quantity of node shifting. Using our new statistics shape, the data owner can perform insert, adjust or delete operation on file blocks with excessive performance. In destiny paintings we're implementing de-duplication Technique for observed duplicate document have in cloud. Because within the above System we're doing RDPC Technique to Data integrity. So it's far degrade the gadget overall performance via doing for reproduction files. To enhance gadget performance we will locate reproduction document earlier than add in cloud, as soon as if we located any reproduction file from cloud then this enhancing device does now not permit to store in cloud.

6. REFERENCES:

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,“Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Gener. Comp. Sy., vol. 25, no. 6, pp. 599 – 616, 2009.

[2] H. Qian, J. Li, Y. Zhang and J. Han, “Privacy preserving personal health record using multi-authority attribute-based

encryption with revocation,” Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

[3] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, “Flexible and fine-grained attribute-based data storage in cloud computing,” IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, “KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage,” IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016. 2542813.

[5] J. Li, Y. Shi and Y. Zhang, “Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage,” Int. J. Commun. Syst., DOI: 10.1002/dac.2942.

[6] J.G. Han, W. Susilo, Y. Mu and J. Yan, “Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no.11, pp. 2150-2162, 2012

[7] Z. J. Fu, X. M. Sun, Q. Liu, L. Zhou, and J. G. Shu, “Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing,” IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.

[8] Z. J. Fu, K. Ren, J. G. Shu, X. M. Sun, and F. X. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE Transactions on Parallel and Distributed Systems, DOI: 10.1109/TPDS.2015.2506573, 2015.

[9] Z. H. Xia, X. H. Wang, X. M. Sun, and Q. Wang, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, 2015.

[10] Y. J. Ren, J. Shen, J. Wang, J. Han and S. Y. Lee, “Mutual verifiable provable data auditing in public cloud storage,” Journal of Internet Technology, vol. 16, no. 2, pp. 317-323, 2015.

[11] 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.

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable Data Possession at Untrusted Stores,’’ in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), 2007, pp. 598-609.

[13] A. Juels and B.S. Kaliski Jr., ‘‘PORs: Proofs of Retrievability for Large Files,’’ in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), 2007, pp. 584-597.

[14] H. Shacham and B. Waters, ‘‘Compact Proofs of Retrievability,’’ in Proc. 14th Int’l

Conf. on Theory and Appl. of Cryptol. and Inf. Security (ASIACRYPT), 2008, pp. 90-107.

[15] D. Boneh, H. Shacham, and B. Lynn, ‘‘Short Signatures From the Weil Pairing,’’ J. Cryptol., vol. 17, no. 4, pp. 297-319, Sept. 2004.

[16] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ‘‘MR-PDP: Multiple-replica provable data possession,’’ in Proc. 28th IEEE Conf. on Distrib. Comput. Syst. (ICDCS), 2008, pp. 411-420.

[17] Z. Hao and N. Yu, ‘‘A multiple-replica remote data possession checking protocol with public verifiability,’’ in Proc. 2th Int’l Symp. Data, Privacy, E-Comm. (ISDPE), 2010, pp. 84-89.

[18] A. F. Barsoum and M. A. Hasan, ‘‘Provable multicopy dynamic data possession in cloud computing systems,’’ IEEE Trans. Inf. Foren. Sec., vol. 10, no. 3, pp. 485-497, 2015.