Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 2, Issue 11, February 2019
Proceedings of Knowledge Discovery in Information Technology and Communication Engineering (KITE-2018), 4th May 2018

A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage

Santhrupthi C Goudappanavar, Shalini, Gujjalla Sahithi, Yashaswini A, K Komala devi

Dept.Of Information Science, East Point College Of Engineering And Technology, Bangalore

Abstract: ***As an essential application in cloud computing, cloud storage offers client versatile, adaptable and astounding data stockpiling and calculation administrations. A developing number of data proprietors outsource data records to the cloud. Since cloud storage servers are not completely reliable, data proprietors require tried and true intends to check the possession ship for their documents outsourced to remote cloud servers. To address this vital issue, some remote data possession checking (RDPC) conventions have been displayed. In any case, numerous current plans have vulnerabilities in effectiveness or data progression. In this paper, we give another proficient RDPC convention in light of homomorphic hash function. The new plan is provably secure against fraud assault, supplant assault and replay assault in light of a normal security demonstrate. To help data flow, an operation record table (ORT) is acquainted with track tasks on document squares. We additionally give another upgraded usage for the ORT which makes the cost of getting to ORT almost consistent. Also, we make the extensive execution investigation which demonstrates that our plan has focal points in calculation and correspondence costs and also provides data regain ability if it is found modified. Model execution and examinations show that the plan is practical for genuine applications.***

Keywords: Cloud storage, RDPC, data dynamics and integrity, homomorphic hash function, operation record table

I. INTRODUCTION

Cloud computing rises as a novel processing worldview consequent to lattice figuring. By dealing with an incredible number of dispersed processing assets in Internet, it has colossal virtualized registering capacity and storage room [1]. In this way, cloud computing is generally acknowledged and utilized as a part of numerous genuine applications [2]. As a critical administration for cloud computing, cloud specialist co-operate dependable, adaptable, and ease outsourced capacity administration to the clients. It furnishes the clients with a more adaptable way called pay-as-you-go model to get calculation and capacity assets on-request. Under this model, the clients can lease vital IT framework according to their requirement rather than buy them. In this manner, the in advance speculation of the clients will be diminished enormously.

Furthermore, it is advantageousfor them to modify the limit of the leased asset while the size of their applications changes. Cloud specialist co-op tries togive a promising support of data stockpiling, which spares the clients expenses of venture and asset. In any case, cloud storage likewise brings different security issues for the outsourced data. Albeit some security issues have been illuminated [3-10], the critical difficulties of data altering and data lost are as yet existing in cloud storage. From one viewpoint, the mischance circle blunder or equipment disappointment of the cloud storage server (CSS) may cause the unforeseen defilement of outsourced documents. Then again, the CSS isn't completely dependable from the point of view of the data proprietor, it might effectively erase or change records for colossal financial advantages. In the meantime, CSS may conceal the mischievous activities and data misfortune mishaps from data proprietor to keep up a decent notoriety. In this manner, it is significant for the data proprietor to use a proficient method to check the uprightness for outsourced data.

Remote data possession ship checking (RDPC) [11] is a powerful strategy to guarantee the uprightness for data documents put away on CSS. RDPC supplies a technique for data proprietor to productively confirm whether cloud specialist co-op loyally stores the first documents without recovering it. In RDPC, the data proprietor can challenge the CSS on the trustworthiness for the objective record. The CSS can produce verifications to demonstrate that it keeps the entire and uncorrupted data. The central necessity is that the data proprietor can play out the check of record uprightness without getting to the entire unique document. In addition, the convention must oppose the malignant server which endeavors to check the data trustworthiness without getting to the entire and uncorrupted data [12].Another coveted necessity is that dynamic data tasks ought to be bolstered by the convention. As a rule, the data proprietor may annex, embed, erase or change the document obstructs as required. Additionally, the registering many-sided quality and correspondence overhead of the convention ought to be considered for genuine applications.

II. RELATED WORK

A. Literature Survey

The principal RDPC was proposed by Deswarte et al. [11] in light of RSA hash work. The disadvantage of this

Conference held at Brindavan College of Engineering, Yelahanka, Bagalur Main Rd, Dwarka Nagar, Bengaluru - 560063

plan is that it needs to get to the whole record obstructs for each test. In 2007, the provable data possessionship (PDP) display was exhibited by Ateniese et al. [13], which utilized the probabilistic verification strategy for remote data honesty checking without getting to the entire document. Moreover, they provided two solid plans (S-PDP, E-PDP) in light of RSA. Despite the fact that these two conventions had great execution, it's a pity they didn't bolster dynamic activities. To defeat this weakness, in 2008, they displayed a dynamic PDP conspire by utilizing symmetric encryption [14]. In any case, this plan still did not bolster piece embed task. In the meantime, loads of research works [15-19] committed to develop completely powerful PDP conventions. For example, Sebé et al. [15] gave a RDPC convention to basic data foundations in light of the issue to factor vast whole numbers, which is effortlessly adjusted to help data progression. Erway et al. [16] first exhibited a completely dynamic PDP conspire (DPDP) by utilizing confirmed skip list, which enabled data proprietor to attach, erase, embed and refresh record obstructs at whenever. Wang et al. [17] utilized Merkle hash tree (MHT) to propose another dynamic strategy for remote data checking, in which each square was hashed to be a leaf hub of MHT. By arranging all leaf hubs from left to right, the MHT verifiably distinguished the piece position which is basic for dynamic activities. Nonetheless, utilizing MHT caused substantial calculation cost. In 2013, Yang and Jia [18] introduced a proficient plan, in which a list table was used to help dynamic activities. By the list table, the data proprietor recorded the legitimate area and adaptation number for each piece for the outsourced document. Be that as it may, to erase or embed one data obstruct, theverifier needed to discover the situation of the piece and move the rest of the passages to embed or erase a line in the list table, which still caused high calculation cost. In [19], Chen et al. given a dynamic RDPC conspire by utilizing homomorphic hash work characterized in [20]. Sadly, their plan was demonstrated shaky by Yu et al. [21]. To conquer the downside, Yu et al. [21] exhibited another RDPC convention in light of RDPC plot in [19] and demonstrated the security. They additionally utilized MHT to accomplish data dynamic tasks, which caused an indistinguishable inadequacy of wasteful from in [17].

In 2008, Curtmola et al. [22] first considered the remote uprightness checking for numerous copies in cloud setting. They accepted a situation that the data proprietor put away certain copies of an essential record on the server, it is important to confirm whether every one of these imitations are kept in place. To accomplish this objective, they introduced a provable secure various copies PDP conspire. Hao and Yu [23] proposed a RDPC convention for the different reproductions with open undeniable nature and security protection. Mukundan et al. [24] displayed a dynamic various copies PDP, which upheld dynamic activities on reproductions while holding the highlights of numerous imitations respectability checking. In 2015, Barsoum and Hasan [25] proposed a provable multi-duplicate dynamic datapossessionship conspire, which utilized guide adaptation table to do dynamic activities on multi-duplicate. Zhu et al. [26] gave a cooperative provable data possessionship (CPDP) conspire for uprightness confirmation in multicloud setting. Despite the fact that they guaranteed the CPDP had the security properties of culmination, learning soundness and zero-data, Wang and Zhang [27] demonstrated that the CPDP did not fulfill the learning soundness property. To maintain a strategic distance from the authentication administration, Wang [28] proposed a personality based appropriated PDP in multicloud capacity. Chen [29] connected logarithmic mark characterized in [30] to present another remote data checking convention, which was ended up being unreliable against replay assault and cancellation assault [31]. Hao et al. [12] introduced a remote data uprightness check convention supporting security protecting, open unquestionable status and data elements. In any case, Zhou and Li [32] brought up that Hao's convention squandered storage room and couldn't avoid dynamic enemy's assault. In 2015, Wang and Li [33] exhibited a declaration based remote data uprightness checking plan openly cloud, which wipes out the key escrow issue.

Another branch of remote data checking is proof of retrievability (PoR) which has additional capacity of recouping document if there should arise an occurrence of disappointment contrasted and PDP. In 2007, Juels and Kaliski [34] proposed the idea for PoR and formalized the definition and security necessity. They displayed a PoR plot utilizing sentinels and mistake remedying code to demonstrate record honesty and recoup target document. Shacham and Waters [35] gave two effective and minimal PoR conventions, which were based on BLS marks [36] and pseudorandom works individually. As of late, a few PoRconventions [37-39] were proposed to upgrade the security and enhance the effectiveness.

B. Inspiration And Contribution

out It is basic for data proprietors to confirm the honesty for the data put away on CSS before utilizing it. For instance, a major universal exchanging organization stores every one of the imports and fares record documents on CSS. As per these documents, the organization can get the key data, for example, the coordinations amount, the exchange volume and so forth. On the off chance that any record document is disposed of or altered, the organization will experience the ill effects of a major misfortune which may cause awful impact on its business and advancement. To evade this sort of conditions, it is obligatory to check the respectability for outsourced data records. Moreover, since these documents may allude to business mystery, any data presentation is unsuitable. On the off chance that the organization contender can execute the record uprightness checking, by as often as possible checking the documents they may acquire some valuable data, for example, when the document changes, the development rate of the document and so on, by which they can figure the improvement of the organization. Therefore, to dodge this circumstance, we consider the private confirmation write in our plan, that is, the data proprietor is the remarkable verifier. Truth be told, the ebb and flow look into heading of RDPC centers around general society confirmation, in which anybody can playthe errand of

document honesty checking with the framework open key. In spite of the fact that RDPC with open check appears to be superior to that with private confirmation, yet it is inadmissible to the situation said above.

Spurred by the above application situations, we show a novel effective RDPC plot by utilizinghomomorphic hash work [20], which has been utilized to build RDPC plans [19,21]. Tragically, these plans are either unreliable or not sufficiently productive. To conquer these disadvantages, we allude to the possibility of [35] and present a private key for each label age in our RDPC plot. At the same time, another development of ORT is introduced for data dynamic which can enhance the productivity of the convention significantly. Contrasted and the past ones, our plan has better execution in term of calculation and correspondence. Our commitments are compressed as takes after:

We display a novel effective RDPC plot with data work system, in which the hash estimation of the whole for two pieces is equivalent to the item for two hash estimations of the relating squares. We present a direct table called ORT to record data activities for supporting data elements, for example, square adjustment, piece inclusion and square erasure. To enhance the productivity for getting to ORT, we influence utilization of doubly connected rundown and cluster to present to an improved execution of ORT which decreases the cost to about steady level. We demonstrate the displayed conspire is secure against fraud assault, replay assault and supplant assault in light of a run of the mill security show. Finally we execute our plan and make exhaustive examination with past plans. Test comes about demonstrate that the new plan has better execution and is useful for genuine applications.

III. PROPOSED SYSTEM

In this segment, we present the preparatory learning utilized all through in our framework. The architecture design is done in the figure 4, which consists of three modules basically our RDPC protocol work with the flow of figure 4. The three modules are possession module, cloud server module and verifier module. Possession can upload the file to cloud and he/she can download the file from cloud. In verifier module the initial hash value and the new hash value will be compared and if it is not matching then it sends a email alert to the user through a registered mail id. And it is also responsible for maintaining a data base for the possession details. In the cloud serer the data is divided into number of blocks and encrypted and stored and it checks the data integrity by generating the hash value for given frequency and it will be sent to the verifier module.

A. Homomorphic Hash Function

Motivated by [19] and [21], our plan embraces the homomorphic hash work characterized in [20] as the premise, which is portrayed as following:

To start with, the calculation HKeyGen(λ_p, λ_q,m,s)→K is used to acquire the homomorphic key. It takes four security parameters as contributions, in which λ_p *and* $\lambda_q$are two discrete log security parameters, m is the area check of the message and s is an irregular seed. It yields the homomorphic key K=(p,q,$\vec{g}$),where p and q are two arbitrary huge primes with the properties of | p|= λ_p, |q|= λ_q and q|(p-1), $\vec{g}$=[$g_1, g_2, \ldots, g_m$]is a 1×m line vector making out of m irregular esteems in $Z_P^*$with arrange q. The point by point procedure of this calculation is appeared in Fig.1, in which the capacity f(x) is the pseudo-arbitrary number generator with seed s and yields the following number in its pseudo-irregular grouping, scaled to the range {0, … . ,x-1} [19]

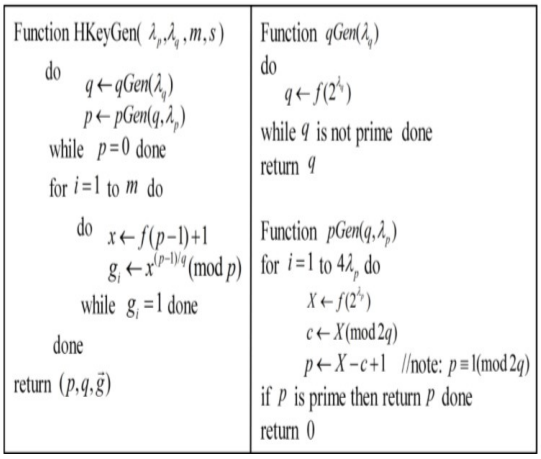

Fig 1. Homomorphic key generation algorithms

B. Operation Record Table

Allude to [18, 25], to help dynamic activities on document squares, we present a basic adaptable data structure named task record table (ORT). The table is saved on the data proprietor side and used to record all the dynamic practices on document squares. ORT has a basic structure with just three sections, that is Block Position(BP) , Block Index(BI) and Block Version (BV). The BP speaks to the physical list for the present piece in the document, typically its esteem is augmented by 1. The BI speaks to the legitimate record for the present square, which isn't important equivalent to BP however significant with the time when the piece shows up in the document. The BV demonstrates the present form for the square. On the off chance that the data record is at first made, the BV esteems for all pieces are 1. When one solid piece is refreshed, its BV esteem is augmented by 1. It is noticed that utilizing the ORT table will build the capacity overhead of the data proprietor by O(n) , where n is the check of pieces. In any case, this additional capacity cost is practically nothing. For instance, a 1GB-record with 16KB piece estimate just needs 512KB space to store an ORT acknowledged by connected rundown (< 0.05% of the document measure).

C. RDPC Protocol

In this paper, we research the cloud storage framework including two members: CSS and data proprietor. The CSS has intense capacity and calculation assets, it acknowledges the data proprietor's solicitations to store the

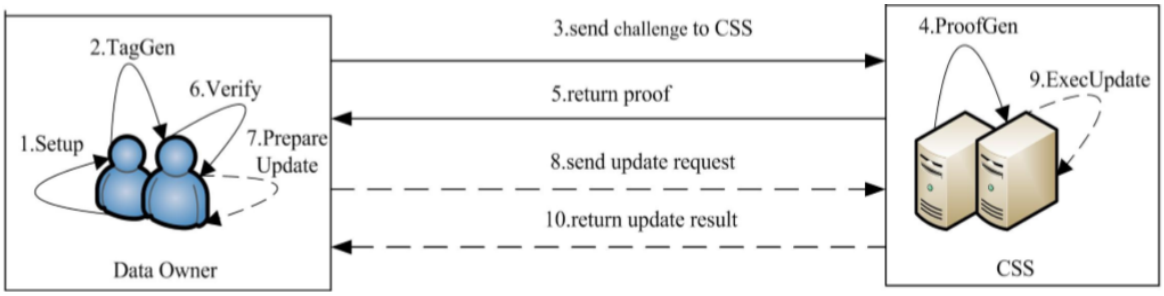

Fig 2. Work procedure of our RDPC protocol

outsourced data documents and supplies get to benefit. The data proprietor makes the most of CSS's administration and puts expansive measure of documents to CSS without reinforcement duplicates in nearby. As the CSS isn't thought to be trustable and once in a while get out of hand, for instance, adjusting or erasing incomplete data records, the data proprietor can check the trustworthiness for the outsourced data proficiently.

A RDPC conspire incorporates the accompanying seven calculations:

KeyGen(1^k,λ_p,λ_q,*m,s)*→*(K,s).*The data proprietor executes this calculation to instate the framework and create keys. It inputs security parameters k,λ_p,$\lambda_q$the message division number m and an irregular seed s , and yields the homomorphism key K and private key sk. Here the seed s fills in as a heuristic "proof", which the hash parameters are chosen truthfully[19].

TagGen(K,sk,F)→*T.*This calculation is executed by the data proprietor to create labels of the document. It inputs the homomorphic key K, private key sk and record F, and yields the label set T which is aconsecutive accumulation for tag of each piece.

Challenge(c)→*chal.*The data proprietor executes the calculation to create the test data. It takes the tested pieces consider c info and yields the test chal.

ProofGen(F,T,chal)→*P.*The CSS executes this calculation to create the honesty verification P. It inputs the record F, label set T and the test chal and yields the verification P.

Verify(K,sk,chal,P)→*{1,0}*. The CSS executes this calculation to produce the respectability confirmation P. It inputs the document F, label set T and the test chal and yields the verification P.

PrepareUpdate(F_i',*UT)*→*URI.*The data proprietor runs this calculation to plan dynamic data activities on data squares. It takes new document squareF_i' the piece position i and the refresh compose UT as sources of info, and yields the refresh ask for data URI. The parameter UT has three discretionary components: embed, change and erase.

ExecUpdate(URI)→{Success,Fail}.The CSS runs this calculation to execute the refresh activity. It inputs URI and Outputs execution result. On the off chance that the refresh activity is done effectively, it returns Success, generally returns Fail.

The entire work methodology of our RDPC convention is shown in Fig.2, in which strong linesand dash lines speak to the procedures of data honesty checking and data dynamic tasks individually.

IV. REQUIREMENT OF SECURITY

The CSS isn't completely trusted since it may take noxious practices on outsourced data and conceal data debasement events from data proprietor in order to keep great notoriety. As indicated by [18], the deceptive CSS may dispatch three sorts of assaults on RDPC, to be specific fashion assault, replay assault and supplant assault. Manufacture assault: the CSS fashions a legitimate tag for the tested piece to cheat the data proprietor.

Replay assault: the CSS picks a legitimate evidence for possession ship from past confirmations or other data, without getting to the genuine tested square and tag.

Supplant assault: the CSS uses the other legitimate combine for square and tag as the verification of the tested one, which may has been altered or disposed of.

A protected RDPC convention ought to be equipped for opposing every one of the assaults above, which ensures that any individual who can build up a legitimate evidence passing the confirmation ought to really have the whole document. Allude to [13, 19, 21], we utilize an data possessionship checking to receive the data possessionship characters which incorporates all the three assaults. The diversion which includes a challenger C filled in as data proprietor and an enemy A filled in as untrusted CSS is appeared as takes after

Setup: C executes KeyGen calculation to create the homomorphic key K and private key sk. The two are kept covertly by C.

Inquiry: A can make two kinds of questions with C:

1. Tag question: An adaptively picks measure of data squares and sends them to C for questioning the labels. C executes the TagGen calculation to acquire a legitimate tag of each square and returns every one of the labels to A.
2. Proof confirmation question: A creates data possessionship proofs for the hinders whose labels have been questioned and presents the evidences to C. C executes the Verify calculation to check the approval for the evidences and returns the

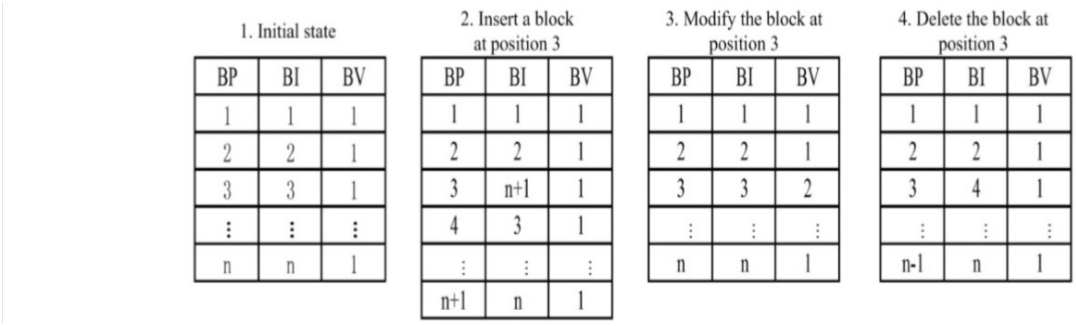

Fig 3. ORT operation

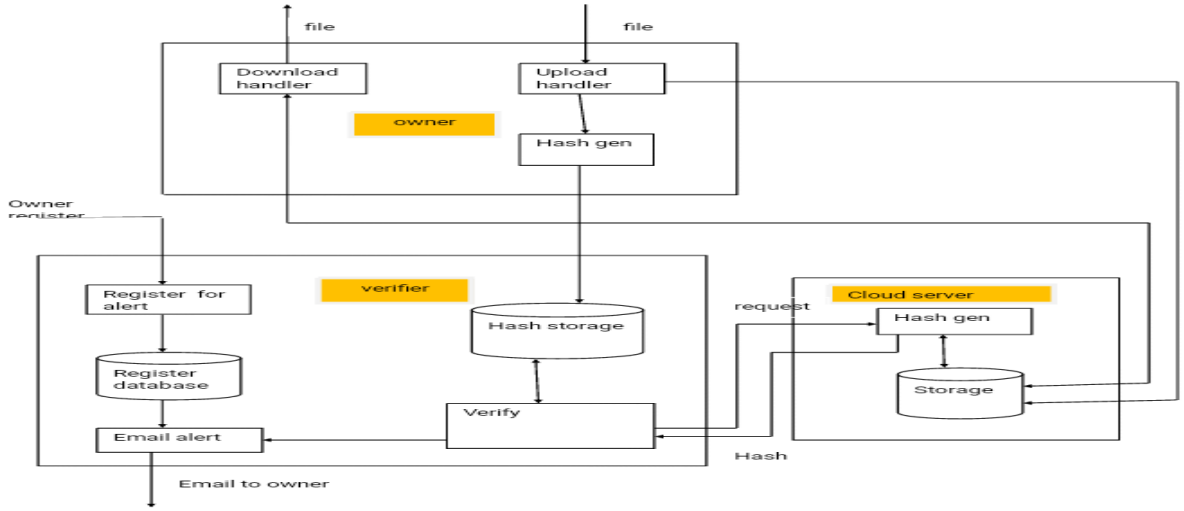

Fig 4. Architecture Module

outcomes to A. These inquiries can be rehashed polynomial circumstances.

Test: C submits challenge chal to An and requires A to answer data possession ship confirmation P of the tested pieces.

Manufacture: A registers a proof P and returns it to C. A wins if P is a right evidence.

Definition 1. A RDPC conspire is secure if any probabilistic polynomial-time (PPT) enemy can win the data possessionship diversion on an arrangement of pieces with non-irrelevant preferred standpoint, there exists a learning extractor which can extricate the tested squares with non-immaterial likelihood.

A. Dynamic RDPC Scheme

In genuine applications, outsourced data document is dynamic. This rouses us to develop dynamic RDPC plans with different data square activities. In this paper, we utilize ORT table as the helper device to help data dynamic activities. The comparable thought has been embraced by [18, 25]. To be a completely unique plan, we need to do another two works. Right off the bat, we have to make slight change on the calculation TagGen of the static plan. Besides, we should execute the calculations ExecUpdate and PrepareUpdate , which are the center capacities for data flow. At that point, we will exhibit these two works separately.

Adjustment on TagGen: In the new TagGen calculation, other than doing every one of the works in static plan, the data proprietor needs to introduce the ORT table and store the data for every one of the pieces to the ORT. As appeared in

Fig.3, in introduction stage all the BP esteems are the genuine records of squares with climbing request, the BI esteems are the same as BP, and the estimations of BV are instated to 1. At the same time, to improve the security of the dynamic RDPC convention, ω_i is refreshed toω_i=$F_{id}||m||BI_i||BV_i$, where BI_i and BV_i denote the BI esteem and the BV estimation of the piece F_i.This calculation is in charge of building up the pre-works for dynamic tasks. The data proprietor can execute three kinds of tasks on his outsourced record, in particular 'embed', 'erase' and 'adjust'.

B. Optimization Of ORT

The changing procedure of the ORT for various kinds of dynamic tasks. Clearly, ORT is a straight data structure.

So cluster and connected rundown are two conventional means for executing ORT [18, 25]. Be that as it may, utilizing exhibit has advantage over the component area however its awesome expenses on 'embed' and 'change' tasks, which need to duplicate and move every one of the components behind the embed or adjust list. Utilizing connected rundown to acknowledge ORT will expel the cost of component adapting and moving and simply require to move hub pointers which spends almost less cost. Be that as it may, it increments gigantic overhead on hubs area for recovering, embeddings and adjusting components particularly when the data estimate is bigger. In this manner, to show signs of improvement getting to productivity, we introduce a novel half and half data structure for acknowledging ORT, which is blend of exhibit and doubly connected rundown. We consolidate the exhibit's legitimacy to limit the scope of area, and the connected rundown's legitimacy to speed the embed or erase task. Accordingly, we can decrease the overhead of refresh ORT to about steady.

V. EXECUTION ANALYSIS

The execution for the proposed conspire is examinee in this segment. We first contrast our new plan and other RDPC plans for effectiveness. At that point we demonstrate the test comes about for our new plan.

A. Efficiency Evaluation

Our plan is create on a protected homomorphic hash capacity and backings completely unique tasks about squares including inclusion, cancellation and adjustment. Another light weight data structure called ORT is utilized to acknowledge dynamic tasks. By presenting a novel upgraded execution of ORT, we diminish the cost of getting to ORT to about consistent level. Then, our plan has no restrictions on the confirmation times and tested piece numbers, which can be set uninhibitedly by the data proprietors as per their prerequisites.

B. Experimental outcomes

In this paper, we execute the RDPC convention utilizing java programming dialect. We gave data respectability to the data document outsourced to cloud server utilizing Homomorphic hash capacity and task record table (ORT). At the point when the data gets undermined, email caution is sent to particular client. We will store the duplicate of unique data which won't be related with the tainted blocks. And the ruined data will be recovered by duplicate of data which was put away in cloud.

VI. CONCLUSION AND FUTURE WORK

In our work, we consider the issues for the data record outsourced to remote server by checking the respectability and we propose a capable secure RDPC tradition with data stream. In our arrangement to affirm the uprightness to the record set away in remote server we use homomorphic hash work, it cuts down the limit cost and estimation cost of data proprietor. We design another light weight data structure that sponsorships dynamic action on discourages that reveal slightest figuring cost by lessening number of center point moving. Using our new data structure, the data proprietor can perform exercises like install, eradicate and change on report blocks with high capability. It is exhibited that present model is secured by new arrangement. The execution is evaluated with respect to gather cost, estimation cost and limit cost. The exploratory results demonstrate that our arrangement is convenient in appropriated capacity.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud registering and rising IT stages: Vision, buildup, and reality for conveying figuring as the fifth utility," Future Gener. Comp. Sy., vol. 25, no. 6, pp. 599 – 616, 2009.

[2] H. Qian, J. Li, Y. Zhang and J. Han, "Protection safeguarding individual wellbeing record utilizing multi-expert quality based encryption with repudiation," Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

[3] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Adaptable and fine-grained trait based data stockpiling in cloud computing," IEEE Trans. Administration Comput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced property based encryption with catchphrase scan work for cloud storage," IEEE Trans. Administration Comput., DOI: 10.1109/TSC.2016. 2542813.

[5] J. Li, Y. Shi and Y. Zhang, "Accessible ciphertext-arrangement trait based encryption with repudiation in cloud storage," Int. J. Commun. Syst., DOI: 10.1002/dac.2942.

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

[7] Z. J. Fu, X. M. Sun, Q. Liu, L. Zhou, and J. G. Shu, "Accomplishing productive cloud seek administrations: multi-watchword positioned look over encoded cloud data supporting parallel registering," 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, "Empowering customized seek over encoded outsourced data with proficiency change," IEEE Transactions on Parallel and Cloud Systems, DOI: 10.1109/TPDS.2015.2506573, 2015.

[9] Z. H. Xia, X. H. Wang, X. M. Sun, and Q. Wang, "A safe and dynamic multi-watchword positioned seek conspire over scrambled cloud data," IEEE Transactions on Parallel and Cloud Systems, vol. 27, no. 2, pp. 340-352, 2015.

[10] Y. J. Ren, J. Shen, J. Wang, J. Han and S. Y. Lee, "Shared obvious provable data evaluating openly cloud storage," Journal of Internet Technology, vol. 16, no. 2, pp. 317-323, 2015.

[11] Y. Deswarte, J. J. Quisquater, and A. Saïdane, "Remote uprightness checking," in Proc. sixth Working Conf. Integr. Inside Control Inf. Syst. (IICIS), 2003, pp. 1– 11.

[12] Z. Hao, S. Zhong, and N. Yu, "A protection saving remote data uprightness checking convention with data flow and open irrefutability," IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432– 1437, Sep. 2011.

[13] G. Ateniese, R. Consumes, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Melody, "Provable Data Possession at Untrusted Stores," in Proc. fourteenth ACM Conf. on Comput. what's more, Commun. Security (CCS), 2007, pp. 598-609.

[14] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. fourth Int'l Conf.

Security and Privacy in Commun. Netw. (SecureComm), 2008, pp. 1-10.

[15] F. Sebé, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Productive Remote Data Possession Checking in Critical Data Infrastructures," IEEE Trans. Data and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[16] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in Proc. sixteenth ACM Conf. on Comput. what's more, Commun. Security (CCS), 2009, pp. 213-222.

[17] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847-859, May, 2011.

[18] K. Yang and X. Jia, "A productive and secure dynamic inspecting convention for data stockpiling in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717-1726, 2013.

[19] L. Chen, S. Zhou, X. Huang and L. Xu, "Data flow for remote datapossessionship checking in cloud storage, " Comput. Electr. Eng., vol. 39, no. 7, pp. 2413-2424, 2013.

[20] M. N. Krohn, M. J. Freedman and D. Mazieres, "On-the-fly confirmation of rateless eradication codes for proficient substance appropriation," in Proc. 2004 IEEE Symp. on Security and Privacy (S&P), 2004, pp. 226– 240.

[21] Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang and C. Xu, "Improved security of a dynamic remote datapossessionship checking convention for cloud storage," Expert Syst. Appl., vol. 41, no. 7, pp. 7789-7796, 2014.

[22] R. Curtmola, O. Khan, R. Consumes, and G. Ateniese, "MR-PDP: Multiple-reproduction provable datapossessionship," in Proc. 28th IEEE Conf. on Distrib. Comput. Syst. (ICDCS), 2008, pp. 411-420.

[23] Z. Hao and N. Yu, "A numerous imitation remote datapossessionship checking convention with open evidence," in Proc. 2th Int'l Symp. Data, Privacy, E-Comm. (ISDPE), 2010, pp. 84-89.