International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 08 | August - 2022 Impact Factor: 7.185 ISSN: 2582-3930

IMPLEMENTATION OF IDENTITY BASED REMOTE DATA INTEGRITY CHECKING SCHEME FOR CLOUD STORAGE

T. Vamsi Vardhan Reddy[1],

[1]Assistant Professor, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India 524101, vvreddy.837@gmail.com

P. Varshitha[2], R. Sindhu[3], P. Rishitha[4], V. Pavani[5]

[2]Student, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India 524101, pydivarshitha2002@gmail.com

[3]Student, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India 524101, sindhuchinni66@gmail.com

[4]Student, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India 524101, pellururishitha630@gmail.com

[5]Student, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India 524101, pavani05a9@gmail.com

Abstract –In this paper, we executing Identity based (ID-based) far off remote data integrity checking (RDIC) convention by utilizing key-homomorphic cryptographic crude to decrease the framework intricacy and the expense for laying out and dealing with the public key verification structure in PKI based RDIC plans. We formalize ID-based RDIC and its security model including protection from a noxious cloud server and zero information security against an outsider verifier. The proposed ID-based RDIC convention releases no data of the put away information to the verifier during the RDIC cycle. The new development is demonstrated secure against the vindictive server in the nonexclusive gathering model and accomplishes zero information protection against a verifier.

Index Terms – Cloud storage, data integrity, privacy preserving, identity-based cryptography.

I. INTRODUCTION

Cloud computing [1], which has gotten significant consideration from research networks in scholarly world as well as industry, is a circulated calculation model over an enormous pool of shared-virtualized figuring assets, like capacity, handling power, applications and administrations. Cloud clients are provisioned and discharge recourses as they need in distributed computing climate. This sort of new calculation model addresses

another vision of giving processing administrations as open utilities like water and power. Distributed computing brings various benefits for cloud clients. For instance, (1) Users can diminish capital consumption on equipment, programming and administrations since they pay just for what they use; (2)Users can appreciate low administration upward and quick admittance to a wide scope of utilizations; and (3) Users can get to their information any place they have an organization, instead of remaining close by their PCs.

The size of the cloud information is gigantic, downloading the whole file to check the uprightness may be restrictive as far as data transmission cost, and thus, extremely unrealistic. In addition, conventional cryptographic natives for information uprightness checking, for example, hash capacities, approval code (MAC) can't have any significant bearing here straightforwardly due to being shy of a duplicate of the first file in verification. All in all, far off information uprightness checking for secure distributed storage is an exceptionally attractive as well as a difficult examination theme. Blum proposed a reviewing issue for the first time that empowers information proprietors to check the honesty of far off information without express information on the whole information [3]. As of late, far off information trustworthiness checking turns out to be increasingly more significant because of the advancement of circulated stockpiling frameworks and online stockpiling frameworks. Provable information ownership (PDP) [4], [5] at untrusted stores, presented by Ateniese et al., is an original procedure for "blockless approving" information honesty over far off servers. In PDP, the information proprietor creates some metadata for a file, and afterward sends his information file along with the metadata to a far off server and erases the file from its neighborhood stockpiling. To produce a proof that the server stores the first file accurately, the server figures a reaction to a test from the verifier. The verifier can confirm if the file keeps unaltered by means of really taking a look at the accuracy of the reaction. PDP is a useful way to deal with checking the trustworthiness of cloud information since it takes on a spot-really looking at method. Specifically, a file is separated into blocks and a verifier just difficulties a little arrangement of arbitrarily picked tickers for trustworthiness checking. As indicated by the model given by Ateniese et al. [4], for a file with 10,000 squares, on the off chance that the server has erased 1% of the squares, a verifier can identify server's trouble making with likelihood more prominent than almost 100% by requesting confirmation from ownership for just 460 haphazardly chosen blocks. Ateniese et al. proposed two cement PDP developments by utilizing RSA-based homomorphic direct authenticators. Because of its need and practicability, far off information respectability checking has drawn in broad examination interest [7]-[8][9][10][11], lately.

II. LITERATURE SURVEY

A. Provable data possession at untrusted stores.

We present a model for provable information ownership (PDP) that permits a client that has put away information at an untrusted server to check that the server has the first information without recovering it. The model produces probabilistic confirmations of ownership by examining arbitrary arrangements of squares from the server, which definitely decreases I/O costs. The client keeps a steady measure of metadata to check the confirmation. The test/reaction convention sends a little, steady measure of information, which limits network correspondence. Accordingly, the PDP model for far off information checking upholds huge informational collections in broadly circulated capacity framework.

We present two provably-secure PDP plans that are more proficient than past arrangements, in any event, when contrasted and plots that accomplish more fragile certifications. Specifically, the upward at the server is low (or even consistent), rather than straight in the size of the information. Tests utilizing our execution confirm the common sense of PDP and uncover that the presentation of PDP is limited by circle I/O and not by cryptographic calculation.

B. Remote data checking using provable data possession.

We present a model for provable information ownership (PDP) that can be utilized for far off information checking: A client that has put away information at an untrusted server can confirm that the server has the first information without recovering it. The model produces probabilistic confirmations of ownership by testing irregular arrangements of squares from the server, which definitely decreases I/O costs. The client keeps a steady measure of metadata to confirm the evidence. The test/reaction convention sends a little, steady measure of information, which limits network correspondence. Accordingly, the PDP model for far off information checking is lightweight and supports enormous informational indexes in conveyed capacity frameworks. The model is additionally strong in that it integrates systems for moderating inconsistent measures of information debasement. We present two provably-secure PDP plans that are more effective than past arrangements. Specifically, the upward at the server is low (or even steady), instead of straight in the size of the information. We then propose a nonexclusive change that adds strength to any far off information checking plan in view of spot checking.

C. ID-based Signature

A personality based signature (IDS) conspire comprises of four polynomial-time, probabilistic calculations depicted beneath. Setup(k). This calculation takes as information the security boundary

k and results the expert mystery key msk and the expert public key mpk. Separate (msk, ID). This calculation takes as info a client's personality ID, the expert mystery key msk and creates a mystery key usk for the client. Sign (ID, usk, m). This calculation takes as information a client's personality ID, a message m and the client's mystery key usk and creates a mark σ of the message m. Verify(ID, m, σ, mpk). This calculation takes as information a mark σ, a message m, a personality ID and the expert public key mpk, and yields on the off chance that the mark is substantial or not.

III. PROPOSED WORK

A. System Overview

Normally, information proprietors themselves can really look at the uprightness of their cloud information by running a two-party RDIC convention. Notwithstanding, the examining result from either the information proprietor or the cloud server may be viewed as one-sided in a twoparty situation. The RDIC conventions with public verifiability empower anybody to review the trustworthiness of the reevaluated information. To make the portrayal of the openly verifiable RDIC conventions obviously, we expect their leaves an outsider inspector who has ability and capacities to accomplish the verification work. Considering this, the ID-based RDIC engineering is delineated in Fig 1. Four distinct substances to be specific the KGC, the cloud client, the cloud server and the TPA are associated with the framework.

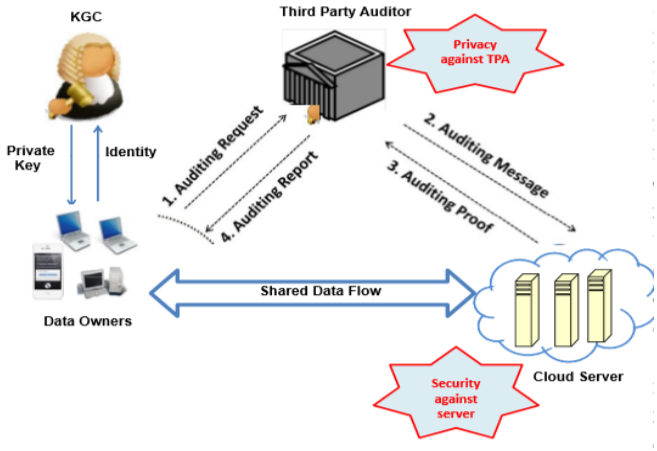

Fig. 1. System Overview

We provide a concrete construction of secure identity-based remote data integrity checking protocol supporting perfect data privacy protection. Our scheme works as follows. In the key extraction, we employ short signature algorithm due to Boneh et al. to sign a user's identity ID $\in\{0,1\}*$ and obtain the user's secret key. In TagGen, we invent a new algorithm to generate tags of file blocks which can be aggregated into a single element when computing a response to a challenge. In the challenge phase, the TPA challenges the cloud by choosing some indexes of the blocks and random values. In the proof generation, the cloud server computes a response using the challenged blocks, obtains the corresponding plaintext and forwards it to the TPA.

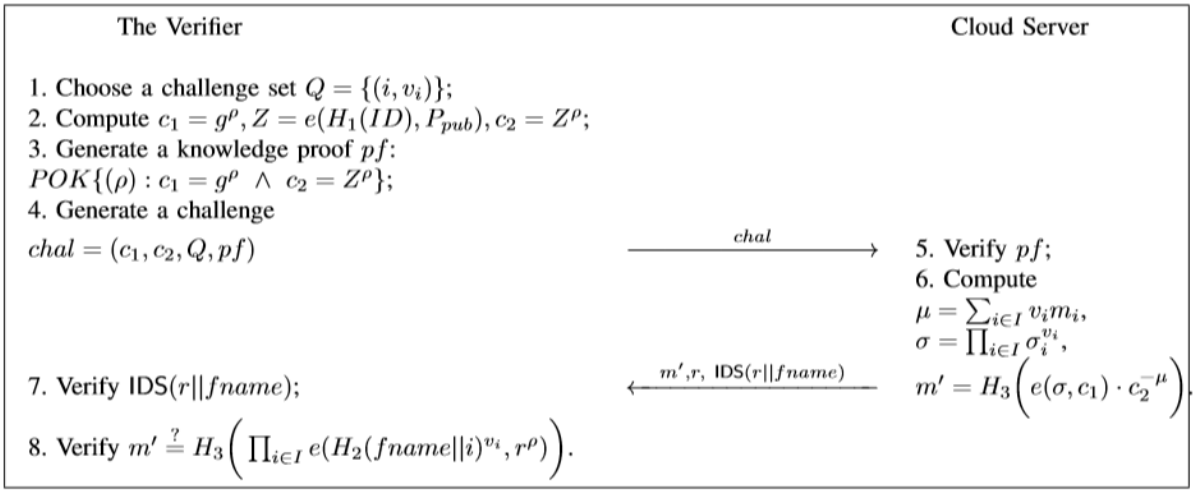

Fig. 2. Identity-based remote data integrity checking protocol

V. RESULTS

In our setting, the size of a data block is bounded by the group order p, i.e., 160 bits. Hence, we have 50,000 blocks in total. This implies that the timing results for Setup, Extract and TagGen steps are constant for this part. See Table I for more details.

SUMMERISE OF THE TIME COST FOR A 1 MB FILE

Setup	Extract	TagGen: off-line	TagGen: on-line	Challeng
4.8 ms	0.1 ms	241.9 second	20.3 second	351 ns per ch

TABLE I

We then increase the number of challenged blocks from 50 to 1000 with an increment of 50 for each test to see the time cost of Challenge, GenProof and CheckProof steps. As one shall see from Figure 3, the timing cost of those three parts increases with the increase of the number of challenges.

In the second part, we test the most expensive algorithm TagGen of the protocol by increasing the file size from 200 KB to 2 MB, that is, from 10,000 blocks to 100,000 blocks accordingly, and record the time for TagGen.

As expected, both on-line and off-line time to generate tags for a given file increases almost linearly with the increase of the file size. Figure 4 gives more details.

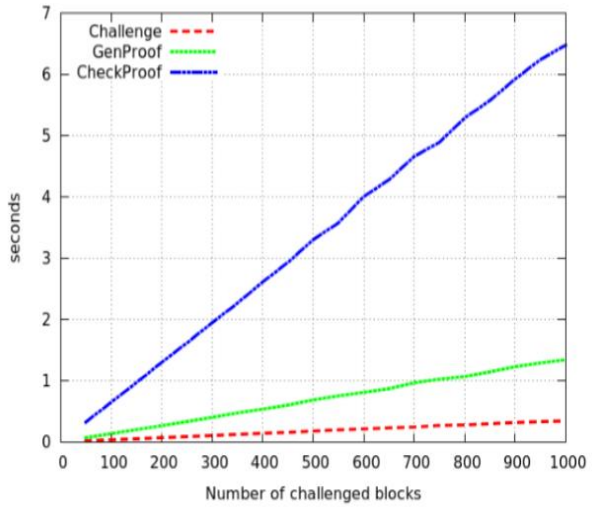

Fig. 3. Increasing number of challenges for fixed size of file

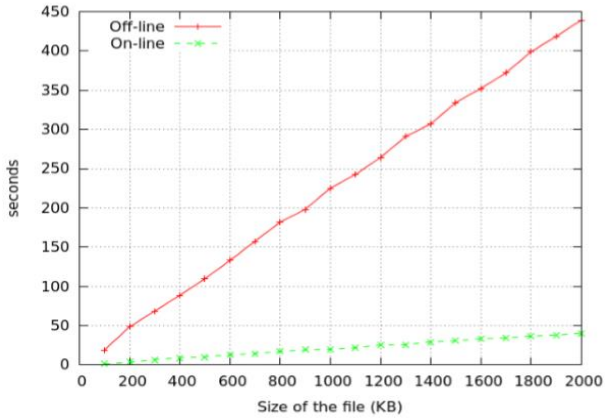

Fig. 4. Tag generation time for increased size of files

VII. CONCLUSION

In this paper, we investigated a new primitive called identity-based remote data integrity checking for secure cloud storage. We formalized the security model of two important propertiesofthisprimitive,namely,soundnessandperfect data privacy. We provided a new construction of this primitive andshowedthatitachievessoundnessandperfectdataprivacy. Both the numerical analysis and the implementation demonstrated that the proposed protocol is efficient and practical.

REFERENCES

1. P. Mell, T. Grance, Draft NIST working definition of cloud computing, Reference on June. 3rd, 2009. http://csrc.nist.gov/groups/SNC/cloudcomputing/index.html.
2. Cloud Security Alliance. Top threats to cloud computing. http://www.cloudsecurityalliance.org, 2010.
3. M. Blum, W. Evans, P.Gemmell, S. Kannan, M. Naor, Checking the correctness of memories. Proc. of the 32nd Anual Symposium on Foundations foVomputers, SFCS 1991, pp. 90–99, 1991.
4. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, D. X. Song, Provable data possession at untrusted stores. ACM Conference on Computer and Communications Security, 598-609, 2007.
5. P.Rajasekar & H.Mangalam (2015),"Design and Implementation of Low Power Multistage AES S Box", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 19 (2015) pp 40535-40540
6. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.

7. A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc. of CCS 2007, 584-597, 2007.
8. H. Shacham, and B. Waters, Compact proofs of retrievability. Proc. of Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.
9. G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphic identification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009.
10. A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensicsand Security, 10(3): 485–497, 2015.
11. J. Yu, K. Ren, C. Wang, V. Varadharajan, Enabling cloud storage auditingwith key-exposure resistance, IEEE Trans. on Information Forensics andSecurity, 10(6): 1167–1179, 2015.
12. Sruthi P.M, Parani T.K, P. Rajasekar, (2017) "An Efficient and Secured Data Transmission in WBAN Using U-Wear Technology", International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 3 Issue 5, May 2017 pp. 207– 217
13. Mandava Geetha Bhargava, Modugula TS Srinivasa Reddy, Shaik Shahbaz, P Venkateswara Rao, V Sucharita Potential of big data analytics in bio-medical and health care arena: An exploratory study, Global Journal of Computer Science and Technology 2017/8/5