International Conference On Emerging Trends in Engineering and Management Research
NGSPM's Brahma Valley College of Engineering & Research Institute, Anjaneri, Nashik(MS) (ICETEMR-16)
23rd March 2016, www.conferenceworld.in ISBN: 978-81-932074-7-5

PRIVACY-PRESERVING PUBLIC AUDITING DATA INTEGRITY FOR SHARED DATA IN THE CLOUD

Pooja Doshi[1],Gayatri Sarag[2]

[1,2]Computer Science, DYPIEMR(SPPU),India)

ABSTRACT

With cloud data administrations, it is typical for data to be put away in the cloud, as well as shared over numerous clients. Sadly, the integrity of cloud data is liable to suspicion because of the presence of equipment/programming disappointments and human blunders. A few components have been intended to permit both data proprietors and open verifiers to effectively review cloud data integrity without recovering the whole data from the cloud server. On the other hand, open auditing on the integrity of shared data with these current components will definitely uncover secret datacharacter privacyto open verifiers. In this paper, we propose a novel privacypreserving component that backings open auditing on shared data put away in the cloud. Specifically, we endeavor ring marks to process check metadata expected to review the accuracy of shared data. With our component, the endorser's character on every piece in shared data is kept private from open verifiers, who have the capacity to proficiently confirm shared data integrity without recovering the whole document. Also, our instrument has the capacity perform different auditing undertakings all the while as opposed to checking them one by one. Our trial results show the adequacy and proficiency of our component when auditing shared data integrity.

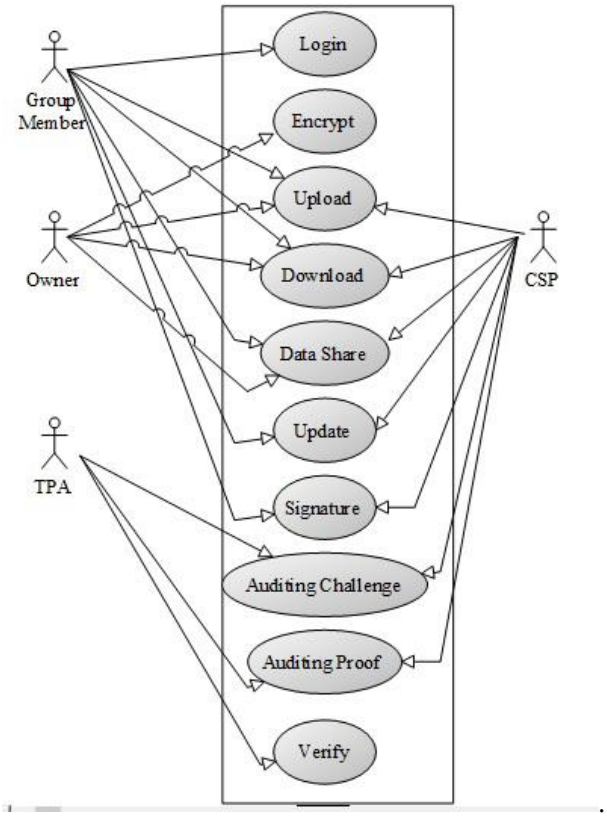
Keywords: Cloud computing, Privacy-preserving ,Public auditing, Shared data

I. INTRODUCTION

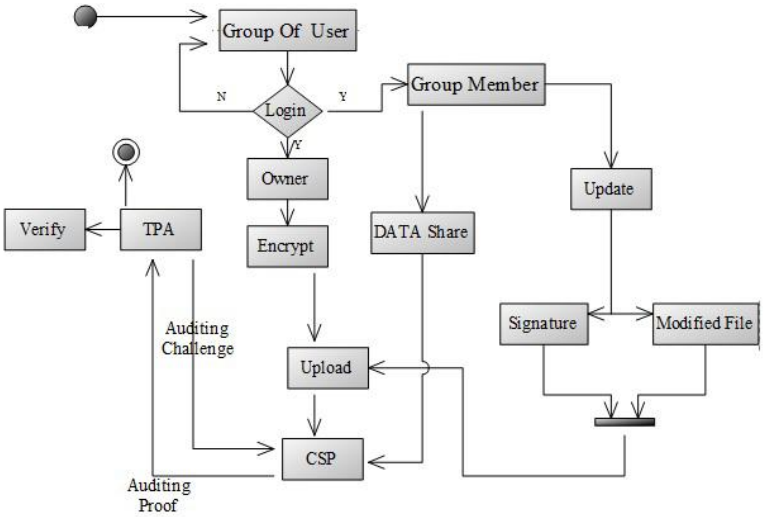
In this paper, we propose the first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.

 ISBN: 978-81-932074-7-5

II. FIGURES AND TABLES



Use case diagram



Activity diagram

III. CONCLUSION

In this paper, we propose Oruta, the first privacypreserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphic authenticators, so the TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity

privacy. To improve the efficiency of verification for multiple auditing tasks, we further extend our mechanism to support batch auditing. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor

IV. ACKNOWLEDGEMENTS

It gives us great pleasure in presenting the preliminary project report on ' PRIVACYPRESERVING PUBLIC AUDITING DATA INTEGRITY FOR SHARED DATA IN THE CLOUD'.

I would like to take this opportunity to thank my internal guide Prof. NareshKumar Mustray for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

I am also grateful to Prof. P. P. Shevtekar, Head of Computer Engineering Department,DYPIEMR for her indispensable support, suggestions. In the end our special thanks to Prof. P.P.Halkarnikar. for providing various resources such as laboratory with all needed software platforms, continuous Internet
connection, and constant support and guidence for Our Project.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM Conference on Computer and Communications Security(CCS), 2007, pp. 598–610.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications(INFOCOM), 2010, pp. 525–533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application ofCryptology and Information Security (ASIACRYPT). Springer- Verlag, 2001, pp. 552–565.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432