International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Remote Data Integrity Check

A. Nagesh, Javeria Qurratul Ain

Abstract: ***In Cloud Storage Server, data integrity plays an important role, given cloud clients might not be aware whether the data is safe or has been tampered with. This system introduces identity-based signature algorithms to protect data that belongs to the data owner and gets the status of cloud data by means of verification through signatures. Since it is practically not possible for the data owner to be available online all the time for checking cloud data integrity, Third party auditor is tasked with verifying the data integrity every time instead of data owner. The Third party auditors should not read the cipher text data while verifying and must authenticate itself to cloud server by performing Proof of Knowledge operation; then cloud server can reveal the sensitive data as block wise and the third party auditor can verify the signature without knowledge of cipher text data. Finally, an audit report is sent to the data owner. This work demonstrates data security and integrity in the cloud..***

Keywords: ***Data integrity, data security, CSP, KGC, Cloud Storage.***

I. INTRODUCTION

In cloud computing [1], the cloud service provider allows cloud users to store their sensitive data with less cost. This allows willing users to save their data in the cloud, unlike the traditional storage spaces where a user needs to own a server which becomes a maintenance overhead with all the hardware and operating system costs. In addition, traditional systems are unable to store data for long time in local server because when storage device is full, they need to make space available for storing future data. Given the boundaries set by the traditional computing practices, users are very limited with what they can access, and remote access capabilities become very limited. But once the cloud user registers with a cloud storage server, users can access data remotely, provided they deploy an application in cloud and there is no need to maintain hardware and software. The cloud user just uploads their sensitive data in cloud then remaining process is carried out by the cloud service provider. The cloud user can upload sensitive data at any time and everywhere, as well as they can access the cloud data, but cloud users do not know whether their data is stored securely. It may lead to loss of security [2] because the data is stored in the third-party storage server. Hence there is no chance to know the activities carried out at the cloud service providers (CSP) unless a mutual trust is established. Data should be converted from plain text to cipher text by using cryptographic techniques which is not readable by unauthorized users. But the cloud user can decrypt the cipher text with privileges keys which are recommended to store sensitive data in cloud storage. In cryptography technology they have Symmetric and Asymmetric algorithms to transform the data into cipher text data. However, Symmetric algorithm can provide a single key for encryption and decryption whereas Asymmetric algorithm provides couple of key, referred as public key and private key, allowing public key to encrypt the data and with secret key, the data can be decrypted. For more security the second method Asymmetric algorithm can be used but is time consuming process and complex of key management. Therefore, Signature techniques can be used to overcome the drawback. There still exists auditing problem for Cloud users as Cryptography techniques provides security but no data Integrity [3] or Data Auditing. which increase the chances to access the corrupted data by Cloud User if not aware of data being corrupted or not. To overcome above limitations the proposed system contributes data integrity checking protocol with zero knowledge proof. In this system data owner can select file and make it signature with Identity-based signature algorithm and store into cloud storage, he/she can verifying their data with sending request to third party auditor then auditor first generate the challenge value with help of zero proof of knowledge, later send to cloud server then it can verify the proof if it is valid then cloud server can return signatures to third party auditor he can verify the signatures and return auditing report to cloud users or data owner if cloud data or signature is not matched then it can generate corrupted status and replace that corrupted data with original data by data owner. Here blocks wisely [4] it generates signature and store into cloud as well as verify the signature also blocks wisely which reduces complexity of comparing with full data. Key management can be done by private key generator, when cloud user register in this system then request sent to be private key generator then he/she can generate private key to user with identity. For preserving data security, cloud data becomes a signature with private key and for data integrity the signature can be verified with public key. So here there is a no chance of lose of security as well as cloud users can know the cloud data status by checking protocol with help of third party auditor.

Revised Manuscript Received on June 09, 2020.
* Correspondence Author
Dr A Nagesh*, Professor, Department of CSE, MGIT, Hyderabad India, E-mail: ans@mgit.ac.in
Javeria Qurratul, M- Tech in Computer Networks and Information Security at MGIT, Hyderabad, India E-mail: rahamaaz@gmail.com

II. RELATED WORK

The author G. Ateniese and R. D. Pietro [5] introduces data integrity with provable data possession, which is like cloud users can use symmetric encryption for encrypting the cloud data and using hash functions for data integrity as well as it can perform security operations like insertion, deletions and modifications. This system is secure but they have to be applying limited queries and limited blocks only divided.

The author S. Tang [6] implemented enhancing remote data integrity checking protocol. This system working on public key infrastructure which is cloud data can be encrypt by public key algorithm which is lead to lose the security if any malicious user get the knowledge of public key then easily they can generate private key and access the cloud so it is not signature based data integrity as well as it doesn't support block wisely data insertions and time consuming for performing encryption operations.

The author H. Rong [7] implemented enhancing for regenerating-code-based cloud storage, which is explain about data can be divided into three parts and store in different servers, if any server was corrupted then using of remaining of servers it can generate new server with cloud data and it can be done by proxy server. This system more security and flexible to generate codes but there is no proof of knowledge and it heavy expensive to maintain many servers for storing data and it is not following of identity based signature scheme for generating signature by PKI.

The author J. Wang [8] implemented Verifiable auditing for outsourced database where the data owner can access the database management which means they can encrypt table columns for performing the correct and completeness of searching outputs even if any attacker try to access the cloud data they unable to know the name of columns, so that SQL injections attacks cannot perform at cloud database side, it can preserving better privacy but it is difficult to encrypt for every column as well as decryption for every search query. For data integrity this system used bloom filter which is store the integer value in array index format, in this process there is a chances to get false positive results when user search with queries. Because when data user search with a keyword in cloud then first that keyword can be convert to hash code with hashing techniques and this hash code can be change to as integer then this integer value can be become position of array, at that index position it can filled with true value by default it filled up with false. When each keyword gets different position then that index position filled up true value but sometimes it can give false positive also when user sends a search request to cloud.

The author J. Ahn [9] implemented Audit Service Outsourcing for Data Integrity which is depicts about to overcome the security risks providing provable data possession and auditing data records for data integrity as well as it has used zero proof of knowledge for third party auditor make it authenticate himself for retrieve data files from cloud server. But for achieving they added diffie-hellman cryptography system for converting plain text to cipher text which is not easy to checking data integrity as well as for getting secret key a group of people should be involved and if any key compromised then there is a chances to lose the security and key updating also a tedious work.

III. IMPLEMENTATION

Identity based remote data integrity checking protocol with actors like Key Generation Centre can generate private keys to data owner and data owner can generate tags, sending an auditing request to Third Party Auditor as well as to get the auditing report from Third Party Auditor.

Architecture

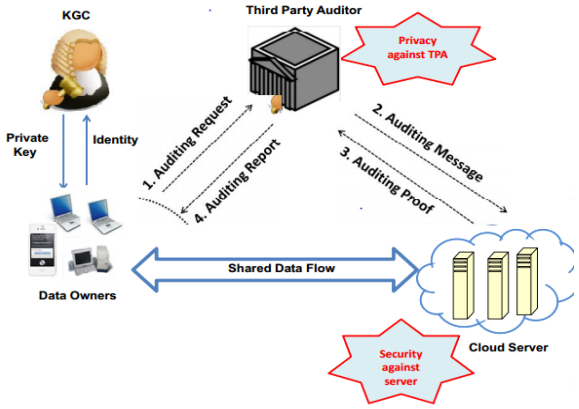

Fig.1. Identity based RDIC

The Third Party Auditor can audit the reports in Cloud Data which is send by Data Owner and it can sends back the audited report. The Cloud Server can monitor Cloud Storage data which is uploaded by Data Owner and can even sends the tags to Third Party Auditor for auditing the reports. When authentication is valid then it can reveal the file tags to Third Party Auditor.

KGC

The Key Generation Center can login and generate public key and master key by calling setup operation as well as it can generate private key to data owner for generating the Tags of files.

Data Owner

The data owner can register and login later he/she can generate file tags by using of identity based signature algorithm with help of input value file with blocks, private key then get tags and storing into cloud as well as he/she can verify their data with TPA by sending the request for data integrity checking and they can download their data form cloud storage server.

TPA

The Third Party Auditor can login and get data owner request then performing zero knowledge proof protocol for authenticate to cloud server later cloud can return to file tags to TPA if proof is valid then TPA can verify file signature and send auditing report to data owner.

Cloud Server

The cloud server can login and view the storage files and get the proof request from TPA then it can send file tags to TPA when proof is valid as well as it can modified the cloud data for data integrity checking protocol.

Proposed Algorithm for RDIC System

Functions used

Retrieval Number: E9780069520/2020©BEIESP
DOI: 10.35940/ijeat.E9780.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Initial Setup ()
This operation execute by Third Part Auditor for generating system public key and master secret key.
Extract ()
This operationexecute by Third Part Auditor for generating private key for data owner with input as public key, master key and user identity then it returns private key.
TagGen ()
This operationexecute by data owner which takes inputs public parameter, private key of data owner and file then it returns file tags for each block and store into cloud storage including with file data.
Challenge ()
This operation execute by TPA for generating challenge value with help of zero proof of knowledge algorithm with takes as inputs public parameter, user identity and file name then it returns chalvalue as output.
ProofGen( )
This algorithm is run by cloud server for proof generation with inputs as system parameters,data owner identity, challenge value, the file, the tags then it returns output as data possession proof to TPA.
Proof Check ()
This algorithm runs by the TPA which takes input as system parameter, data owner identity, data possession proof and file data then it returns output as signature True or False.
Zero Knowledge Proof

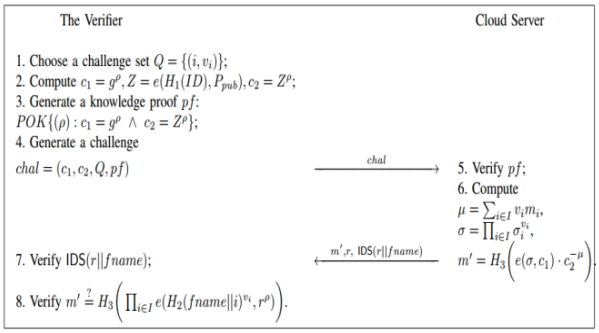

Fig.2.Remote Data Integrity checking protocol

The Fig.2 illustrates Proof of Knowledge protocol (POK) that is generated between TPA and Cloud Server when TPA can generates chalvalue. When this is sent to server and the cloud server proves that chalvalue authenticates then it returns file tags to TPA and it can verify the file tags and send to auditing report to data owner like cloud data is corrupted or not.

IV. EXPERIMENTAL RESULTS

The following page consists of register inputs and all the details are given by user and click on the register that should be stored in database for it to be used for login.

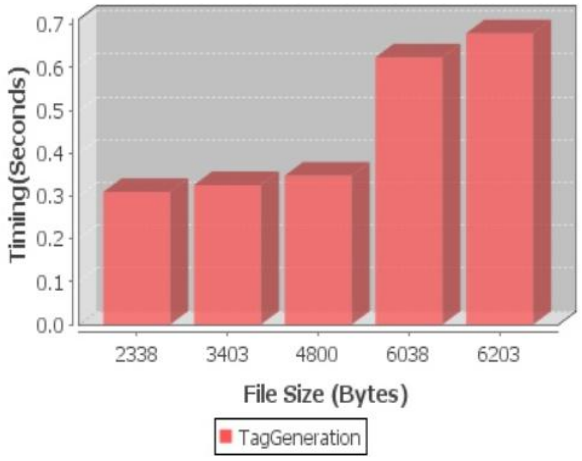

Fig.3 Calculate Tag Generation time

In Figure.3 it shows the calculate tag generation time by increasing the file size from 2338 bytes to 6203 bytes and the timing is displayed in seconds.

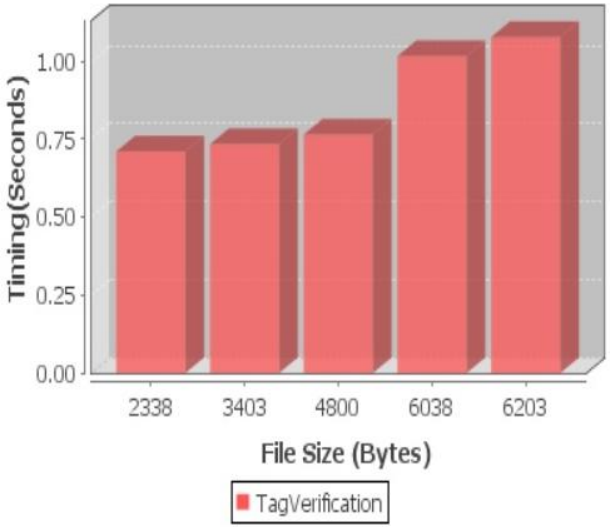

Fig.4 Calculate Tag Verification time

In Figure.4 it shows the calculate tag verification time by increasing the file size from 2338 bytes to 6203 bytes and the timing is displayed in seconds.

V. CONCLUSION

This research uses identity based signature for data integrity which is known by data owner the status of cloud data whether the data is corrupted. In addition, we implemented proof of knowledge algorithm for third party auditor, in case there is a need for authentication with cloud server for fetching cloud results. This is done by verifying the tags, and later it can update auditing reports to data owner. If it is corrupted then the data owner can replace with original data. This is how the system achieves security and data integrity.

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.cloudsecurityallianc e.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. G. Ateniese, R. D. Pietro, L. V. Mancini, G. Tsudik, Scalable and efficient provable data possession, Proc. of SecureComm 2008, Article No. 9 ,doi:10.1145/1460877.1460889.
6. Y. Yu, M H Au, Y. Mu, S. Tang, J. Ren, W. Susilo, and L. Dong, Enhanced privacy of a remote data integrity checking protocol for secure cloud storage, International Journal of Information Security, 14(4): 307– 318, 2015.
7. J. Liu, K. Huang, H. Rong, H. M. Wang, Privacy-preserving public auditing for regenerating-code-based cloud storage, IEEE Trans. On Information Forensics and Security, 10(7): 1513–1528, 2015.
8. J. Wang, X. Chen, X. Huang, I. You, Y. Xiang, Verifiable auditing for outsourced database in cloud computing, IEEE Transactions on Computers, 64(11), 3293-33032015.
9. Y. Zhu, H. Hu, G. J. Ahn, S. S. Yau, Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software, 85(5):1083-1095, 2012.

AUTHOR PROFILE

Dr A Nagesh is working as a professor in Department of CSE at MGIT, Hyderabad India. His research areas of interest include data mining, web technologies and database security. He has published in multiple national and international journals and conferences. Email: ans@mgit.ac.in

Javeria Qurratul Ain is currently purusingM.Tech in Computer Networks and Information Security at MGIT, Hyderabad, India. Her areas of interest include cyber security and forensics. Email: javeriamgit@gmail.com