January-February 2020
ISSN: 0193-4120 Page No. 15034 - 15038

ID-based Public Audit Protocol to Check Data Integrity with Privacy Preservation and Cloud Batch Audit

[1] Arjun U, [2]Vinay S.
[1]Asst. Professor, PESITM Shivamogga, ,[2]Professor, PESCE, Mandya.
[1]arjuninformation@gmail.com,[2]vinaymanyan@gmail.com.

Article Info
Volume 82
Page Number: 15034 - 15038
Publication Issue:
January-February 2020

Article History
***Article Received**: 18 May 2019*
***Revised**: 14 July 2019*
***Accepted**: 22 December 2019*
***Publication**: 28 February 2020*

Abstract:
with the advance and huge development in the cloud services, Cloud Storage service gives the huge storage where we can store the local data remotely with the minimum computing power and limited storage as we delete the locally present data. However, Cloud Service provider (CSP) may cause damage or make unauthorized alterations to the data for benefits. For this purpose, the cloud user must periodically check the integrity of remote data. Public auditing method used for the cloud data integrity verification on behalf of the user. ID-based public auditing protocol (IDPA) for cloud data integrity verification is proposed. Even existing methods can not protect the privacy of the user, as the third party auditor obtains data from the user when auditing.. In this paper, we propose a IDPA for data integrity verification, privacy preserving and effective batch verification. Furthermore we compare our proposed protocol with other IDPA methods**.**

***Keywords:** —Identity-based public auditing protocol, Remote Data auditing, data integrity, privacy, batch auditing*

I. INTRODUCTION

With the advance and huge development in the cloud services, users with the limited storage space can store the locally presented large amount of data to the cloud[3][4]. As Cloud is service oriented and many users use the cloud system it leads to security threat. Once data stored remotely in the remote cloud server, cloud service provider may delete or tamper the data knowingly or unknowingly hence the integrity of the data is violated[6][7]. As data stored remotely Cloud user cannot check the data integrity locally or by using any conventional method. Thus, cloud users need to periodically check the integrity of the large data stored in the remote cloud server.Public auditing methods are preferred to do the data integrity verification in which data integrity can be verified without downloading all the data.Several public audit protocols based on a public key cryptographic scheme were proposed after the implementation of the concept of public auditing. Then ID based cryptographic system are proposed to eliminate the burden of public key management but ID bases method leads to forgery attack and also for frequent auditing methods cannot preserve the privacy of the user.[8][9][10].Based on the study, We proposed an IDPA for data integrity verification. ID-based public auditing protocol which optimizes the time taken to generate the tag and verify, also reduce the computational cost of the batch verification. Furthermore, IDPA protocol has privacy-preserving functionality as third party auditors are unable to render or manipulate data blocks for the cloud users. We show the proposed protocol can withstand forgery attack . We also compare the proposed protocol with other IDPA. The proposed audit protocol is proven Secure and more efficient by comparing with the computation cost.

II. LITERATURE WORK

Ateniese [1] model that allows a cloud user to verify the integrity of the original data by taking the sample from the random set of blocks without downloading it from the untrusted server. [2] Efficient and provably secure PDP technique which allows outsourcing dynamic data and technique supports operations such as modification, deletion and append but not insertion on the outsourced data.[3][6] An efficient and privacy preserving public auditing protocol which supports dynamic operations. [7] a secure storage, auditing and verification of the outsourced data which are includes the deduplication framework and Kerberos authentication protocol with identity based remote data verification and authentication.[8] An approach based on index based i.e relative index and time stamped merkle-hash tree ensure that outsourced data is not been pouted as well as recent copy is maintained. Supports public auditing of data and efficiently supports data dynamic operations. [9] MAC mode of encryption and concrete including VDBC scheme to achieve the desired security properties. [10][11] users random masking technique to protect external threats and also prevent the altering verified results from the auditor audited which leads to the auditor overhead.[12][13] SecCloud which helps client to generate the number of data tags before uploading which reduced communication cost of the file uploading and auditing phases. Public auditing figured out the collusion attack and [14] public integrity auditing scheme with vector based commitment and generating the verifier local revocation group signature this method also supports the count ability and traceability.[15] IBDO scheme which gives authorization to proxies to upload the data and it also supports the comprehensive auditing and also regular integrity auditing of the outsourced data. [16] ID-based public key cryptography methods were used and Where Proxy server is used to upload data and remotely check data integrity in the public cloud.

III. PRELIMINARY

In this preliminary section, discuss the properties of bilinear pairings (BP) and Computational Diffie-Hellman (CDH) problem.

A. Properties of Bilinear pairings

Let G and G_T be a group of Cyclic Additives and multiplicative group with the same q number. Bilinear pairs are called G and G_T.ee: $G \times G \rightarrow G_T$ is a bilinear map. If the following properties are met:

(1) Bilinear:

$\forall X,Y,Z \in G, \forall a,b \in z,$

$ee(Y,X+Z)=ee(X+Z,Y)=ee(X,Y)\cdot ee(Z,Y)$

$ee(aX,bX)=ee(X+bX)a =ee(aX,X)b =ee(X,X)ab$

(2) non-degeneracy: $X,Y \in G$ $ee(X,Y) \neq 1$ GT

(3) Computability $e(X,Y)$for any $X,Y \in G$ can be efficiently computed.

Properties of Computational Diffie-Hellman problem (CDH)

Problems with calculating g_{xy} , $g_x,g_y \in G$ where G be a Cyclic group with generator g.

IV. SYSTEM MODEL

As shown in Fig 3.1, an IDPA system for cloud data storage normally includes CSP-cloud storage provider, DO-Data Owner, TPA-Third party auditor and PKG-Public key generator.

-Cloud Service Provider Provides substantial storage space and computing power on request.

-Data Owner create and upload the locally present large amount of data to cloud server.

-Third Party auditor Trusted party that, upon request, offers the auditing service by checking the data integrity on behalf of the data owner.

-Public Key generator to generate the security or system parameters like master key and private keys for the users.

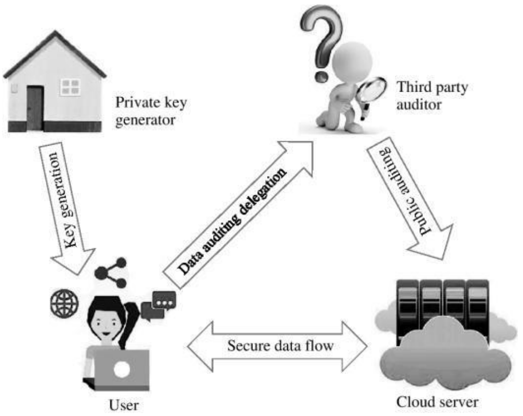

Fig 3.1: System model for cloud data storage audit

V. PROPOSED METHOD

We propose an IDPA in this section using signature based protocol. It includes four stages, Setup ,key generation ,, tag generation , Challenge and Prove ,.

Setup: Following security parameters are provided by public key generator :

1. Selects G1 and a cyclic multiplicative group (G_1,G_2) of the same order q > 2_k using the security parameters k
2. Let e: G_1*G_2->G_2 . Let H_1 :{0,1}*→Zq, H_2 :$\{0,1\}^{n}{}_{v}$ hash functions where n_v € Z.
3. Randomly chosen s belongs Z_q as a master key and compute public key $P_{pub}=g^{a}$.

These System parameters are generated (G_1, $G_{2,}$e,q,g,h,H_1,h,g2,P_{pub}).

Key Extraction: To get the Key, Data Owner sends a request with his ID to the Public Key Generator. Then Send the ID to PKG, PKG computes K = h(ID) € G1,Set the private key S= s*K where s is the master Key of PKG.Tag Generation: With the file M, With the data owner ID split M into n blocks each block has s sectors. Such that M=m1||m2||m3….||m_n. Then randomly select WORD from $z^{q}{}_{*}$ and s+1 random values r0,r1,rs belongs to R.Zq to compute $u_i=g_2^{ri}$ for each 0 ≤ i≤ s.

Following step used to tag generation:

1. Compute (Pk_s,Sk_s)-> using secure signatures algorithms S KGen(x^k) where x=1 to get a pair of public keys and private keys.
2. Compute Y=∑.sign(SK_s,τ_0) to obtain the signature $\tau_{0.}$ Where τ_0 =WORD||n|| u_o||u_1||….$U_{n.}$
3. for each data block b_i 0 ≤ i≤ n. calculates

$$\acute{\omega}_i = r_{0}H_1(WORD\|\, i) + {}^{s}_{j=1}\, rjmij$$

4. Compute authentication tag

$$t_i = (t_{i1} = d_{j1}{}^{\delta_i}(v' \prod v_i), t_{i2} = d_j g^{\ r}$$

The data owner sends the M file along with all the ti authentication tags to the cloud storage services.

Challenge and Prove:

Challenge and prove phase consisting of 3 steps:

(1) TPA → CSP($Chall$, $IDAU$, ω, G, T)

To test the integrity of the outsourced data file M, Third party Auditor randomly selects a set $I \subseteq [1, n]$ and a number $a \in Zq$ to generate the challenging information $Chall = [IDDU, \tau, a, I]$ and sends $Chall$and ($IDAU$, ω, G, T) to Cloud service provider

(2) CSP → : (σ', μ) On receipt $Chall = [IDDU, \tau, a, I]$ and ($IDAU$, ω,,T), Cloud Server checks the formula.

$e\ (G, P) = e\ (h\ \ (\tau\ \ \| \omega\ \ \| T)\, Ppub\ \ + T, QDU)$. (15)

If the equation satisfies, CS finds ($IDDU$, M, τ, $\sigma m1$ ⋯ ,σmn, R) , produces set $\omega = \{(i,\ bi)\}$, $i \in I$. Here, $bi = ai$ mod q. with $M = m1 \| \cdots \| mn$ and ($\sigma m1$ ⋯ ,σmn), Cloud Server computes

$$\sigma' = \sum_{i \in I} b_i \sigma_{m_i},$$

$$\mu = \sum_{i \in I} b_i (m_i + h(m_i))$$

(3) After obtaining the cloud storage proof (σ', μ), based on stored information FA, DU, AU computes

$$z = \sum_{i \in I} b_i z_i,$$

$$R' = \sum_{i \in I} b_i R_i.$$

Then Auditor reviews the equation below: $e\,(\sigma', P) = e\,(zQDU + \mu P, Ppub) \cdot e\,(R', QDU)$

Where the equation applies, the auditor accepts the proof.

VI. RESULTS AND DISCUSSIONS

To validate the efficiency of our audit service, We Simulated the computational cost of our proposed protocol and of the protocol of Zhang et al. [12] on a linux machine with Intel i5 2450 CPU @2.50 Ghz and 16-GB RAM. We used version 0.5.14 of the Pairing-based cryptography (PBC) library. We measure the performance of our proposed audit protocol with regard to security features, communication cost and computation costs, are shown, respectively, in Table 1. Computation costs of our proposed protocol in Key extraction phase is 2HC+2SC+1 , Block tag generation step is (6n+8)HC+(7n+10)SC+13BC, prove and verify step is —I—HC +I—SC—EC and —I—SC+5BC-HC. When the file is 1024 Bytes, When the number n of the blocks of the file is 48, Figure 2 shows a comparison of the cost of computation between our IDPA proposed protocol and Zhang et al.'s protocol. When the file is large and the number of its blocks is correspondingly large, The result shows that our IDPA protocol needs significant low cost computation.

Table 6.1: Comparison of computation costs.

	key extraction	block tag generation	Prove	Verify
Zhang et al. [12]	2HC+2SC	4nHC+6nSC+3nBC+nEC	—I—HC+2—I—SC+I—EC	—I—HC+2—I—SC+3BC
Ours protocol	HC+SC+1	(6n+8)HC+(7n+10)SC+13BC	—I—HC +I—SC—EC	—I—SC+5BC-HC

E: Exponential operation , S: scalar multiplication, H: hash computation , B: bilinear pairing with Computation cost.

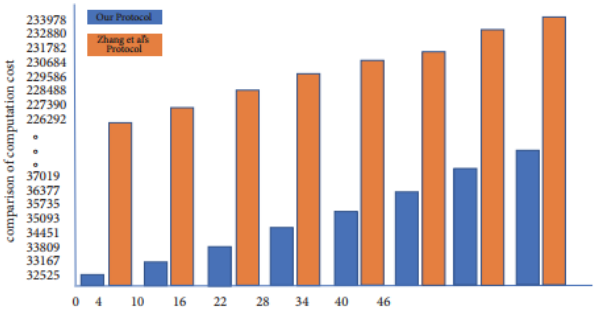

Fig 6.1: Comparison of computation cost

CONCLUSION

In this paper, we propose an IDPA for cloud data integrity verification with preserving privacy. IDPA proposed protocol which optimizes the time taken to generate the tag and verify, also reduce the computational cost of the batch verification. Furthermore, IDPA has privacy features, since the auditor cannot render or tamper the cloud user data blocks. We prove that the proposed IDPA protocol can withstand the attack of forgery on the assumption that the problem with Diffie-Hellman is difficult. We also compare the proposed IDPA protocol with other existing ID-based auditing methods. It is shown that the proposed audit protocol is Secure and more efficient in comparing with the cost of the computation.

REFERENCES

1. G. Ateniese, R. Burns, R. Curtmola et al., ―Provable data possession at untrusted stores,‖ in Proceedings of the 14th ACM Conference on Computer and Communications Security(CCS '07), pp. 598–609, Virginia, Va, USA, November 2007
2. G. Ateniese, S. Kamara, and J. Katz, ―Proofs of storage from homomorphic identification protocols,‖ in Proceedings of International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology,pp.319–333, Springer-Verlag, London, UK,2009.
3. G. Yang, J. Yu,W. Shen, Q. Su, Z. Fu, and R. Hao, ―Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability,‖ The Journal of Systems and Software, vol. 113, pp. 130–139, 2016.
4. R. Swathi and T. Subha, ―Enhancing data storage security in Cloud using Certificateless public auditing,‖ in Proceedings of the 2nd International Conference on Computing and Communications Technologies, ICCCT 2017, pp. 348–352, India, February 2017.
5. L. Wu, J. Wang, N. Kumar, and D. He, ―Secure public data auditing scheme for cloud storage in smart city,‖ Personal and Ubiquitous Computing, vol. 21, no. 5, pp. 949–962, 2017.
6. M. Swapnali and C. Sangita, ―Third Party Public Auditing Scheme for Cloud Storage,‖ in Proceedings of International Conference on Communication , Computing and Virtualization, ICCCV, vol. 79, pp. 69–76, 2016.

7. Aujla G S, Chaudhary R, Kumar N, Das A K, Rodrigues J. SecSVA: secure storage, verification, and auditing of big data in the cloud environment. IEEE Communications Magazine, 2018, 56(1): 78–85
8. [8] Garg N, Bawa S. RITS-MHT: relative indexed and time stamped Merkle hash tree based data auditing protocol for cloud computing. Journal of Network and Computer Applications, 2017
9. Chen X, Li J, Weng J, Ma J, Lou W. Verifiable computation over large database with incremental updates. IEEE Transactions on Computers, 2016, 65(10): 3184–3195
10. Li J, Xie D, Cai Z. Secure auditing and deduplicating data in cloud. IEEE Transactions on Computers, 2016, 65(8): 2386–2396
11. Zhang Y, Xu C X, Li H W, et al. HealthDep: an efficient and secure deduplication scheme for cloud-assisted ehealth systems. IEEE Trans IndInf, 2018, 14: 4101–4112
12. Zhang J H, Dong Q C. Efficient ID-based public auditing for the outsourced data in cloud storage. InfSci, 2016, 343: 1–14
13. Zhang Y, Xu C X, Liang X H, et al. Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation. IEEE Trans Inf Forensic Secur, 2017, 12: 676–688
14. Zhang Y, Xu C X, Li H W, et al. Cryptographic public verification of data integrity for cloud storage systems. IEEE Cloud Comput, 2016, 3: 44–52
15. Jiang T, Chen X F, Ma J F. Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Trans Comput, 2016, 65: 2363–2373
16. Wang Y J, Wu Q H, Qin B, et al. Identity-based data outsourcing with comprehensive auditing in clouds. IEEE Trans Inf Forensic Secur, 2017, 12: 940–952
17. Wang H Q, He D B, Tang S H. Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud. IEEE Trans Inf Forensic Secur, 2016, 11: 1165–1176
18. Zhang Y, Xu C X, Yu S, et al. SCLPV: secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors. IEEE Trans ComputSocSyst, 2015, 2: 159–170
19. Sookhak M, Gani A, Talebian H, et al. Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues. ACM ComputSurv (CSUR), 2015, 47: 65
20. Yu Y, Au M H, Ateniese G, et al. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Trans Inf Forensic Secur, 2017, 12: 767–778
21. Li Y N, Yu Y, Min G Y, et al. Fuzzy identity-based data integrity auditing for reliable cloud storage systems. IEEE Trans Depend Secure Comput, 2017. doi: 10.1109/TDSC.2017.2662216