Hindawi
Scientific Programming
Volume 2021, Article ID 8533995, 5 pages
https://doi.org/10.1155/2021/8533995

Research Article

Public Auditing Scheme for Integrity Verification in Distributed Cloud Storage System

K. Mahalakshmi,[1] K. Kousalya,[2] Himanshu Shekhar,[3] Aby K. Thomas,[4] L. Bhagyalakshmi,[5] Sanjay Kumar Suman,[6] S. Chandragandhi,[7] Prashant Bachanna,[8] K. Srihari,[9] and Venkatesa Prabhu Sundramurthy[10]

[1] *Department of Computer Science Engineering, SSM College of Engineering, Namakkal, India*
[2] *Department of Computer Science Engineering, Kongu Engineering College, Erode, India*
[3] *Department of Electronics and Communications Engineering, Hindustan Institute of Technology and Science, Kelambakkam, Chennai 603103, India*
[4] *Department of Electronics and Communications Engineering, Alliance College of Engineering and Design, Alliance University, Bengaluru-562106, Karnataka, India*
[5] *Department of Electronics and Communications Engineering, Rajalakshmi Engineering College, Chennai, India*
[6] *Department of Electronics and Communications Engineering, Bharat Institute of Engineering and Technology, Hydrabad, India*
[7] *Department of Computer Science Engineering, Jct College of Engineering and Technology, Coimbatore, India*
[8] *Department of Computer Science Engineering, SNS College of Technology, Coimbatore, India*
[9] *Department of Electronics and Communications Engineering, Bharat Institute of Engineering and Technology, Hyderabad, Telangana 501510, India*
[10] *Department of Chemical Engineering, Addis Ababa Science and Technology University, Addis Ababa, Ethiopia*

Correspondence should be addressed to Venkatesa Prabhu Sundramurthy; venkatesa.prabhu@aastu.edu.et

Received 25 October 2021; Revised 8 November 2021; Accepted 6 December 2021; Published 22 December 2021

Academic Editor: M Pallikonda Rajasekaran

Cloud storage provides a potential solution replacing physical disk drives in terms of prominent outsourcing services. A threaten from an untrusted server affects the security and integrity of the data. However, the major problem between the data integrity and cost of communication and computation is directly proportional to each other. It is hence necessary to develop a model that provides the trade-off between the data integrity and cost metrics in cloud environment. In this paper, we develop an integrity verification mechanism that enables the utilisation of cryptographic solution with algebraic signature. The model utilises elliptic curve digital signature algorithm (ECDSA) to verify the data outsources. The study further resists the malicious attacks including forgery attacks, replacing attacks and replay attacks. The symmetric encryption guarantees the privacy of the data. The simulation is conducted to test the efficacy of the algorithm in maintaining the data integrity with reduced cost. The performance of the entire model is tested against the existing methods in terms of their communication cost, computation cost, and overhead cost. The results of simulation show that the proposed method obtains reduced computational of 0.25% and communication cost of 0.21% than other public auditing schemes.

1. Introduction

The cloud storage behaves as a modern paradigm in cloud computing services that is considered proven to deliver extraordinary services to the management and data storage capabilities. The individuals and cloud enterprises tend to outsource their personal or official data to the cloud server via a pay-as-you-go model. The storage services developed to collect the outsourced data reduce their services greatly that affects the local storage essentialities of users. The integrity of data while verifying it is considered as a significant challenge in case of cloud computing [1, 2].

The data offloading and downloading, on the contrary, are often considered as a major consideration for testing the integrity of outsourced data, and this will increase dramatically the processing and connection overhead. The cloud devices used for storage, on the contrary, are often attacked by the hackers, where the data might get stolen while it is been outsourced. Hence, it is essential for the cloud service provider (CSP) to conceal the outsourced data against loss or corruption in order to maintain the trust of the users. The CSP further may reserve more storage spaces by proper removal of redundant information or the data that are accessed less [3] in order to avoid data leaks or leak of private confidential information. It is hence necessary for the CSP to develop an effective protocol that should validate the data integrity in cloud storage environment.

Various methods are developed in conventional literatures that support the verification of private and public information in handling large data. The verification of data allows the cloud users to validate the integrity of their outsourced data. However, such substantial computing poses a serious burden to the CSP, where the cloud resources are of constrained one. The publication verification of outsourced data reduces the computing cost of the client with the optimal usage of third-party authority (TPA) that helps in checking the data integrity. With such optimal processing and reduced user of resources, the public verification in recent past gained an increased attention [4–14].

In order to support the update of dynamic data, the researchers developed several models [3, 15–18] to update the outsourced data without affecting the completion of download. Certain techniques allow the data to be update dynamically using the cryptographic encryption model, and this requires optimal usage of cloud resources. This would increase the computational and communication cost in significant manner.

There exist various pitfalls that still need to be identified. There exist multiple storage spaces that are explicitly required for the storage of the outsourced data. The storage activities involve the deletion and insertion of the data that may result in increased cost of computation and communication since the movement of data in dynamical way cannot be forfeited. Furthermore, the lack of communication links poses a serious challenge in locating the required outsourced data. This system poses increased severity over forgery attack, replay attack, and replacement attack. In order to mitigate such challenges, an integrity verification is suitably designed in the proposed method that uses cryptographic algorithm to verify the sources.

In this paper, an integrity verification mechanism is formed that enables the utilisation of cryptographic solution with algebraic signature. The model utilises elliptic curve digital signature algorithm (ECDSA) to verify the data outsources. The study further resists the malicious attacks including forgery attacks, replacing attacks, and replay attacks. The symmetric encryption guarantees the privacy of the data.

The outline of paper is as follows. Section 2 provides the related works. Section 3 discusses the proposed method. Section 4 evaluates the entire works, and Section 5 concludes the work with possible direction of future work.

2. Related Works

Wang et al. [6] developed an auditing model combining privacy-preserving approach. The model is developed with a homomorphic random mask in order of preventing the TPA from obtaining the data collection without the outsourced data.

Shacham et al. [12] develop an integrity model using public verification scheme that consists of a BLS signature. The BLS [13] tends to use limited resources for its communication and processing requirements.

Chen et al. [14] developed an algebraic solution that is developed to check the integrity of the model. This model improves the efficiency of verification without a public key.

Sookhak et al. [18], on the contrary, develop a limitless verification model, but it suffers mostly from the security flaws. This model computes the secret key based on the signature with the tags and data blocks even if the tags gets attacked.

Juels et al. [19] proposed an identity verification model that helps in preserving the data privacy, where the cloud leverages the user identity to validate the integrity.

Ateniese et al. [20] developed a model that checks the data integrity in the cloud with a technique that combines the block tags with the homomorphic encryption.

3. Proposed Method

We begin by illustrating the system model with ECDLP algorithm.

3.1. System Model

3.1. System Model. The suggested public verification approach uses a three-party model, as depicted in Figure 1. The following are the roles in this model:

(i) Users who rely on the cloud to store the data
(ii) A CSP is a company that sells users a lot of storage and computing power
(iii) TPA checks the data integrity in response to user requests

In Figure 1, the proposed verification scheme shows the communication between the third-party administrator and cloud service provide in terms of proof information and challenge information between them. The user and TPA process between the version information and verification request and result. The data are only transmitted to CSP after a confirmation is obtained from the TP to CSP.

We present each user ability to implement the proposed paradigm. To begin with, the TPA is thought to be trustworthy yet suspicious. The TPA is truthful in its data integrity checks. Furthermore, the CSP is untrustworthy since it has the option of concealing data loss or corruption in order to maintain the user trust. As a result, the CSP can carry out the following attacks: forgery attack, replay attack, and replacing attack.

A data structure is designed in this part to facilitate dynamic data updating. It combines the benefits of a linked list and hash table in TPA. The ECC is made up of a hash

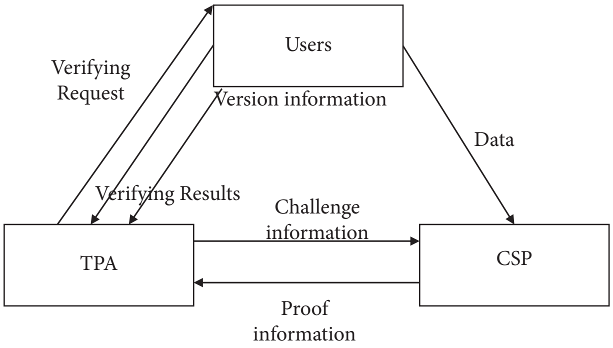

Figure 1: Proposed verification scheme.

table and several linked lists. The user organises the data into groups that compute the group based on its length. Each group index and length are saved in the hash table. Pointers are linked to data version information.

3.2. Verification Scheme. To begin, the TPA merely has to change the list pointer when inserting and deleting items. Second, the group index may be stored and managed using only a continuous space, which is very practical in practise. Third, if operations such as insertion or deletion are considered frequent, the TPA can change the ECDSA flexibly. As a result, the data format can lower the computational and communication costs of updating procedures dramatically.

3.2.1. Key Initiation. For encrypting data blocks, the user first produces a symmetric key dk. He then chooses $x\ Zq$ at random and calculates

$$\mathrm{GA} = xG, \tag{1}$$

where G is an element that is known by TPA and user.

The public key is computed as follows:

$$Q(x, y) = d \times G(x, y), \tag{2}$$

where d is the scalar.

A two different integers, namely, s and r, are used to compute the signature with proper computation of integer r from a base point G (x, y) and random number k:

$$\begin{aligned}(x_1, y_1) &= k \times G(x, y) \bmod p,\\ r &= x_1 \bmod n.\end{aligned} \tag{3}$$

Meanwhile, with an algebraic signature, the user selects a secure element. The secret key is (dk, x) and the public key is GA in this case.

In order the signature to be a valid one, the integer r should be treated as null. This helps in the generation of a random number (k), and after this, the integer r is computed again. Once the successful completion of integer r, the integer s is computed as below:

$$s = (k - 1(h(m) + d * r) \bmod n, \tag{4}$$

where h (m) is the message digest, d and r are the private key, and k is the random number.

3.2.2. Data Blocks' Encryption. To encrypt each data block Mi, the user uses the symmetric encryption method Enc () with the key dk to acquire the encrypted Mi.

3.2.3. Tag Initiation. For each encrypted data block, the user computes the data block tag i:

$$Mi\sigma i = \mathrm{Sig}\,\alpha(x(Mi + H(vi\,kti))). \tag{5}$$

The user then deletes the information that was previously saved locally. The TPA is in charge of launching a verification challenge to ensure that the outsourced data are accurate. It is worth to note that the technique uses dk for data protection and tag initiation using x which is used for public verification. It is difficult for attackers to extract x and the public key GA by exploiting an ECDSA characteristic:

$$x(Mi + H(vi\,kti)). \tag{6}$$

3.2.4. Challenge. The user tends to forward the verification request to TPA. The TPA selects the data from the pool of data blocks. The TPA further forwards the challenge information to CSP, which initiates a challenge.

3.2.5. Proof Generation. Once receiving the information on challenge, the CSP estimates the following:

$$M0 = \sum Mi \text{ and } \sigma = \sum \sigma i. \tag{7}$$

3.2.6. Proof Verification. The TPA is used to estimate the hash value sum.

3.2.7. Signature Verification. The verification of signature is considered as a counterpart while computing the signature. This verifies the authenticity of the message after proof verification using the public key of the authenticator. A secure has algorithm in the formation of signature and helps in computation of authenticator's signed message digest. This is essentially computed using the components of digital signature r and s and public key Q (x, y).

4. Results and Discussion

In this section, the simulation is conducted in a CloudSim software tool on a high-end computing engine that consists i9 processor with 8 GB RAM. The study transferred image files from the user module to CSP module after getting a verification from TPA. The CSP consists of 10 Virtual Machine (VM) running with 24 cores. The simulation has taken place to assess the communication and computation cost at various ends.

Figure 2 shows the storage computational cost between the proposed public auditing scheme and other methods. The results of simulation show that the proposed method achieves reduced storage cost than other methods. The use of ECDSA helps in reducing the computation cost than other methods.

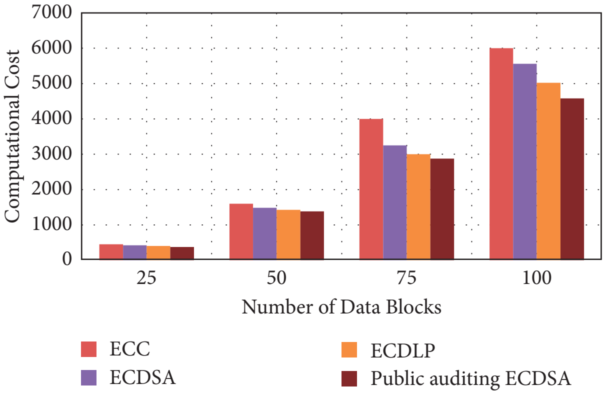

Figure 2: Storage computational cost.

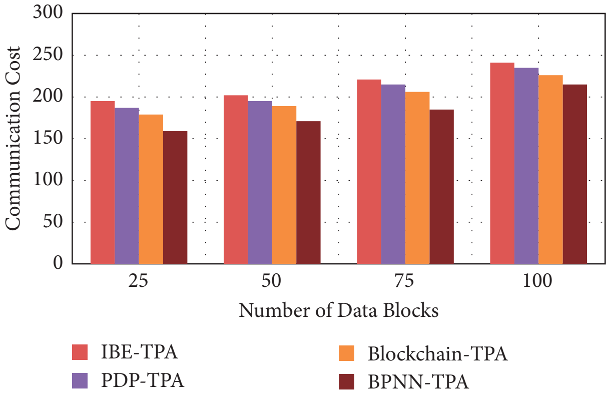

Figure 3: Storage communication cost.

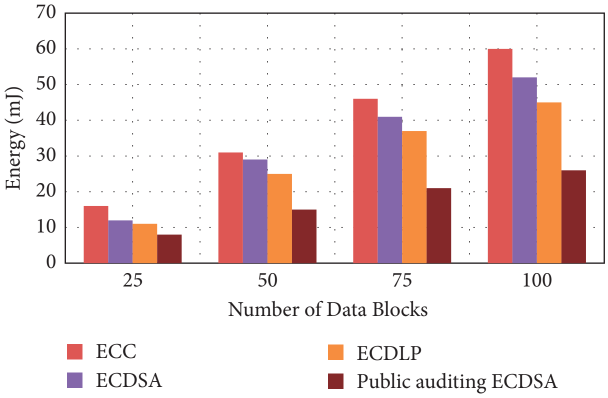

Figure 4: Data communication cost.

Figure 3 shows the storage communication cost between the proposed public auditing scheme and other methods. The results of simulation show that the proposed method achieves reduced storage communication cost than other methods. The use of ECDSA helps in reducing the computation cost than other methods.

Figure 4 shows the data communication cost between the proposed public auditing scheme and other methods. The results of simulation show that the proposed method achieves reduced data communication cost than other methods.

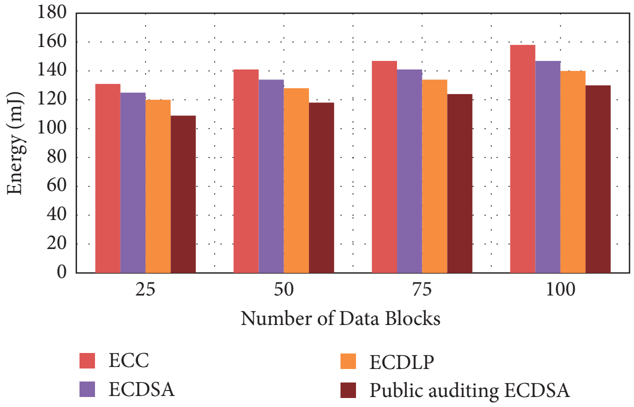

Figure 5: Data computation cost.

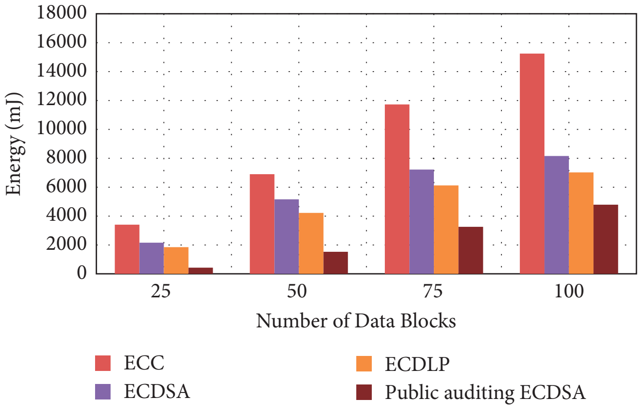

Figure 6: Control overhead cost.

The use of ECDSA helps in reducing the communication cost than other methods.

Figure 5 shows the data computation cost between the proposed public auditing scheme and other methods. The results of simulation show that the proposed method achieves reduced data computation cost than other methods. The use of ECDSA helps in reducing the computation cost than other methods.

Figure 6 shows the control overhead cost between the proposed public auditing scheme and other methods. The results of simulation show that the proposed method achieves reduced control overhead cost than other methods. The use of ECDSA helps in reducing the overhead cost than other methods.

5. Conclusions

In this paper, we develop an integrity verification mechanism that enables the utilisation of cryptographic solution with algebraic signature. The model utilises elliptic curve digital signature algorithm (ECDSA) to verify the data outsources. The study further resists the malicious attacks including forgery attacks, replacing attacks, and replay attacks. The symmetric encryption guarantees the privacy of the data. The simulation is conducted to test the efficacy of the algorithm in maintaining the data integrity with reduced cost. The results of simulation show that the proposed method obtains reduced computational and communication cost than other public auditing schemes. In future, the utilisation of advanced cryptographic encryption models is deployed to improve the rate of reducing the computational and communication cost in cloud systems.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Ethical Approval

No participation of humans has taken place in this implementation process.

Disclosure

No violation of human and animal rights is involved.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security & privacy*, vol. 9, no. 2, pp. 50–57, 2010.

[2] T. Wu, G. Yang, Y. Mu, R. Chen, and S. Xu, "Privacy-enhanced remote data integrity checking with updatable timestamp," *Information Sciences*, vol. 527, pp. 210–226, 2020.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2010.

[4] 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*, pp. 598–609, Virginia, VA, USA, October 2007.

[5] C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," *ACM Transactions on Information and System Security*, vol. 17, no. 4, pp. 1–29, 2015.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2011.

[7] S. S. Abdul-Jabbar, A. Aldujaili, S. G. Mohammed, and H. S. Saeed, "Integrity and security in cloud computing environment: a review," *Journal of Southwest Jiaotong University*, vol. 55, no. 1, 2020.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1717–1726, 2012.

[9] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.

[10] Y. Zhu, G. J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. J. Hu, "Dynamic audit services for outsourced storages in clouds," *IEEE transactions on services computing*, vol. 6, no. 2, pp. 227–238, 2011.

[11] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2231–2244, 2012.

[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proceedings of the Advances in Cryptology-ASIACRYPT 2008. In International Conference on the Theory and Application of Cryptology and Information Security*, pp. 90–107, Springer, Melbourne, Australia, December 2008.

[13] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[14] L. Chen, "Using algebraic signatures to check data possession in cloud storage," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1709–1715, 2013.

[15] H. Tian, Y. Chen, C. C. Chang et al., "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 701–714, 2015.

[16] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, 2017.

[17] M. Sookhak, "Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing," *Information Sciences*, vol. 380, pp. 101–116, 2015.

[18] M. Sookhak, A. Akhunzada, A. Gani, M. Khurram Khan, and N. B. Anuar, "Towards Dynamic Remote Data Auditing in Computational Clouds," *The Scientific World Journal*, vol. 2014, Article ID 269357, 12 pages, 2014.

[19] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks*, pp. 1–10, Istanbul, Turkey, September 2008.

[20] A. Juels and B. S. Kaliski, "PORs: proofs of retrievability for large files," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 584–597, New York; NY, USA, October 2007.