Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage

B Nareshkumar[1] Mr. G. Ananthanath[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Applications
[1,2]KMM Institute of PG Studies, Tirupati, India

Abstract— Distributed computing is an emanate worldview to present dependable and bendy framework empowering the clients (records owners) to store their facts and the statistics consumers (clients) can get to the information from cloud servers. This worldview diminishes capacity and support value of the information owner. In the meantime, the information owner loses the physical manipulate and ownership of information which activates sever a safety risks. Along these strains, inspecting management to test data respectability inside the cloud is fundamental. This issue has turned into a take a look at as the possession of information ought to be confirmed whilst keeping up the privacy. To address those troubles this work proposes at ease and efficient privacy preserving provable information possession (SEPDP). Further, we stretch out SEPDP to assist diverse owners, information elements and cluster affirmation. The maximum appealing component of this plan is that the evaluator can verify the ownership of facts with low computational overhead.

Key words: Integrity Verification, Storage-as-a-Service, Privacy Preserving, Dynamic Auditing, Batch Auditing

I. INTRODUCTION

Storage-as-a-service has emerged as a commercial alternative for local data storage due to its characteristics include less initial infrastructure setup, relief from maintenance overhead and universal access to the data irrespective of location and device. Though it provides several benefits like cost saving, accessibility, usability, syncing and sharing, it raises several security threats as data is under the control of the cloud service provider (CSP). CSP can discard the rarely accessed data to save space and earn more profit, or it can lie about the data loss and data corruption, as a result of software/ hardware failure to protect its reputation. Therefore, it is necessary to check the possession of data in the cloud storage. Traditional cryptographic solutions for integrity checking of data, either need a local copy of the data (which the data users (DUs) do not have) or allow the DUs to downloads the entire data. Neither of these solutions seems practical as earlier one requires extra storage and later alternative increases the file transfer cost. To address this issue, several schemes are proposed which employ blockless verification to verify the integrity without downloading the entire data. One of the attractive features of these works is to allow the public verifier to verify. With public auditability, DUs can recourse the auditing task to a third party auditor (TPA). It has expertise and capabilities to convince both the CSP and the DU. These schemes use provable data possession (PDP) technique, which gives probabilistic data possession guarantee by randomly verifying few blocks for ensuring possession of data in the un-trusted cloud storage.

In this work, we propose a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase. Most attractive feature of SEPDP is that it does not use any intensive computation like pairing based operation. Further, we extend SEPDP to support multiple data owners, batch auditing, and dynamic data operations. A probabilistic analysis to detect the integrity of the blocks stored at CSP. We evaluated the performance of the proposed scheme and compared with some of the existing popular mechanisms. We observe that the total time for verification carried out by TPA in the proposed scheme is less than that of the existing schemes. This signifies that SEPDP is efficient and suitable to implement the verification at the low powered devices.

II. RELATIVE STUDY

A. Privacy-Preserving Public Auditing for Secure Cloud Storage

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

B. Certificateless public auditing for data integrity in the cloud

Due to the existence of security threats in the cloud, many mechanisms have been proposed to allow a user to audit data integrity with the public key of the data owner before utilizing cloud data. The correctness of choosing the right public key in previous mechanisms depends on the security of Public Key Infrastructure (PKI) and certificates. Although traditional PKI has been widely used in the construction of

public key cryptography, it still faces many security risks, especially in the aspect of managing certificates. In this paper, we design a certificateless public auditing mechanism to eliminate the security risks introduced by PKI in previous solutions. Specifically, with our mechanism, a public verifier does not need to manage certificates to choose the right public key for the auditing. Instead, the auditing can be operated with the assistance of the data owner's identity, such as her name or email address, which can ensure the right public key is used. Meanwhile, this public verifier is still able to audit data integrity without retrieving the entire data from the cloud as previous solutions. To the best of our knowledge, it is the first certificateless public auditing mechanism for verifying data integrity in the cloud. Our theoretical analyses prove that our mechanism is correct and secure, and our experimental results show that our mechanism is able to audit the integrity of data in the cloud efficiently.

C. Data Storage Auditing Service in Cloud Computing: Challenges, Methods And Opportunities

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is moving data into the cloud: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. In this paper, we investigate this kind of problem and give an extensive survey of storage auditing methods in the literature. First, we give a set of requirements of the auditing protocol for data storage in cloud computing. Then, we introduce some existing auditing schemes and analyze them in terms of security and performance. Finally, some challenging issues are introduced in the design of efficient auditing protocol for data storage in cloud computing

III. PROPOSED SCHEME

In this section, we present the proposed secure and efficient data possession scheme (SEPDP). SEPDP achieves all the design goals discussed in previous section. SEPDP consists of three phases, namely, key generation phase, signature generation phase, and audit phase. The operations of these phases are depicted in and discussed below. For the sake of simplicity, we describe the scheme with a single DO and extend the scheme to support multiple DOs in Section 5. Notations used in this work are stated in Table 1. G, g, p and H(.)(.) are system wide parameters and available to all the entities.

Notations	Meaning
p	Large prime in Z_p^*
g	Primitive Element in G
$H_{(k)}(:)$	Keyed-hash function
$x \leftarrow^R X$	x is randomly selected from X
a‖b	a is concatenated with b

Table 1: Notations used in proposed SEPDP

A. Key Generation Phase

DO chooses a large prime number p such that computing discrete logarithm problem (DLP) is intractable in Z_p^*. Let G be a group of large prime order p and g 2 G is the primitive element. DO chooses a keyed-hash function, denoted as $|H|_{(k)}(:)$, defined as $\{0,1\}^* \times K \rightarrow Z_p^*$. She shares the key k∈K with TPA through a secure channel. Also, she selects a random number $x \leftarrow^R Z_p^*$ as private key (SK), calculates $Y(= g^x)$ as public key and publishes.

B. Signature Generation Phase

In this phase, DO splits the file M into n blocks as $M = (m_1, m_2, ..., m_n)$, where $m_i \in Z_p$. She signs all the n blocks after choosing a secret random number $r \leftarrow^U Z_p$. The signature hR; s_ii is computed as

$R=g^r$

$s_i = (m_i H_k(Rjji)x)r^{1}$; i = 1,2,... n

and uploads M and to the CSP.

C. Auditing Phase

In this phase, TPA randomly selects a subset (with c elements) of set [1; n]. This set is represented as Q. For i 2 Q it will generate a random v_i 2 Z_q where q << p. Now, TPA sends $f(i; v_i)g_{i2Q}$ to the cloud server as challenge.

After receiving the challenge message from TPA, CSP-computes , and as

$\alpha = R\Sigma i \in Q v_i s_i$

$\beta = \Sigma i \in Q v_i m_i$

$\gamma = g^\beta$

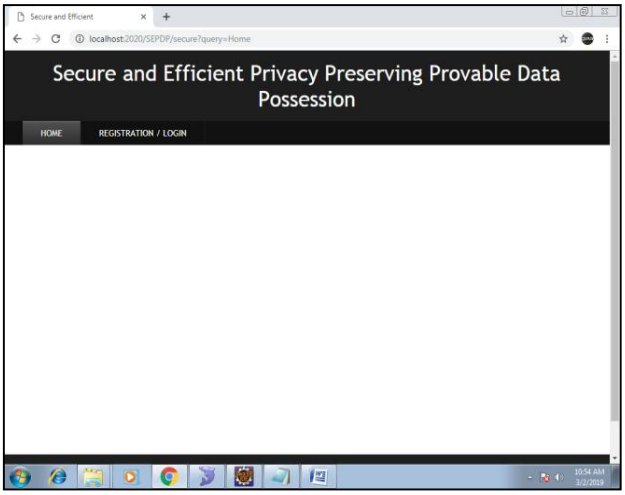
and returns ({α, γ, R}) as response.

TPA assures the integrity of M using below Equation .

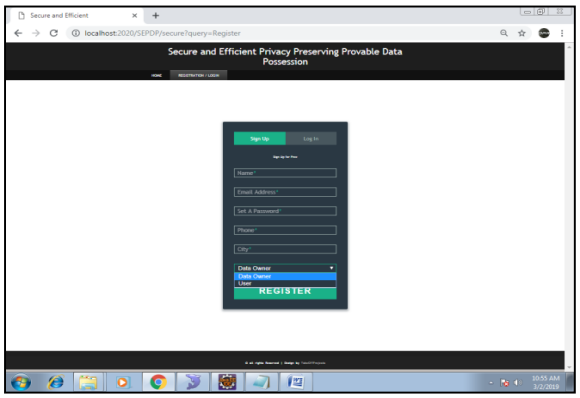
$\gamma =? \alpha Y^P{}_{i2Q} H|_k(R||i)v_i$

IV. SCREEN SHOTS

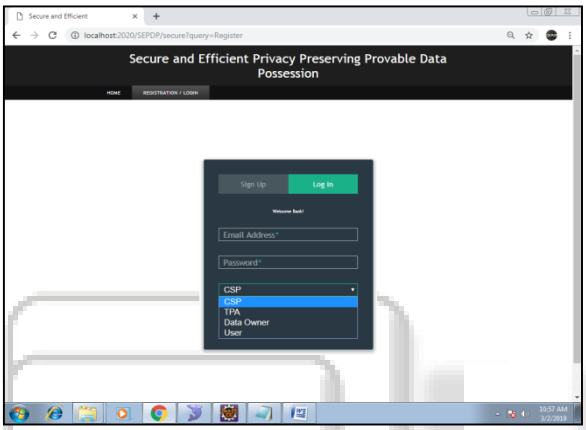
A. Home Page



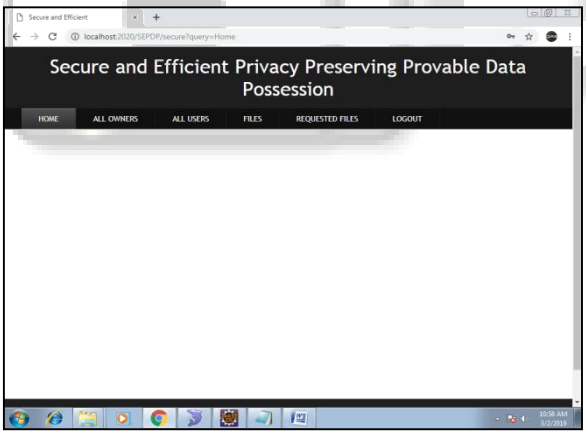
B. Data Owner/User Registration Page



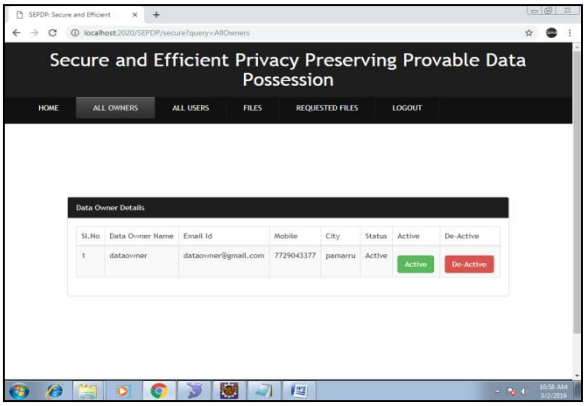
C. CSP/TPA/Data Owner/User Login Page



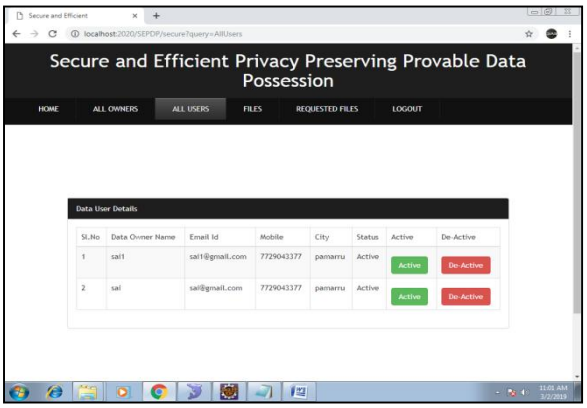
D. CSP Home



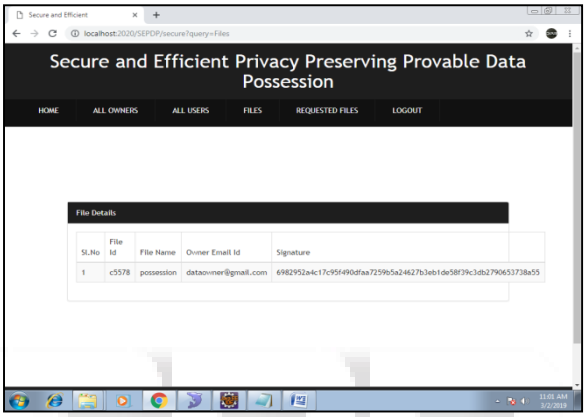
E. All owners



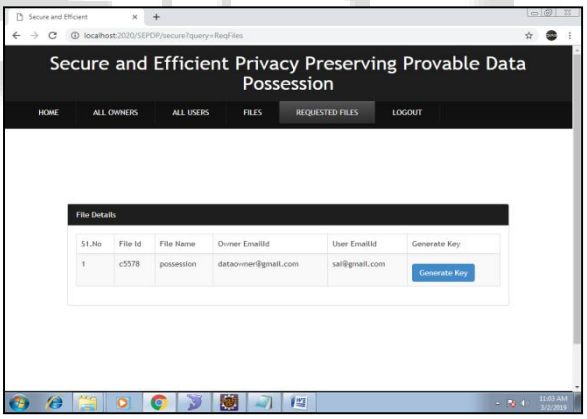
F. All users



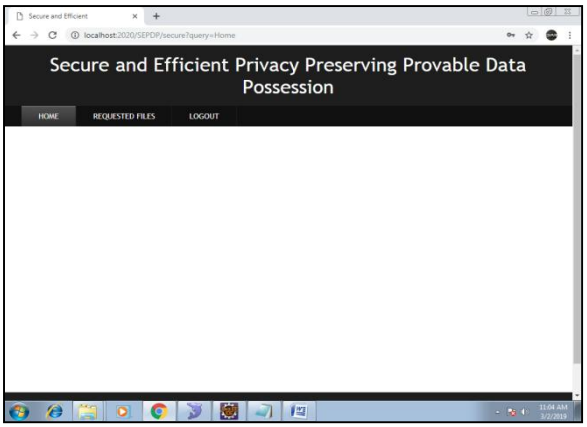
G. Files



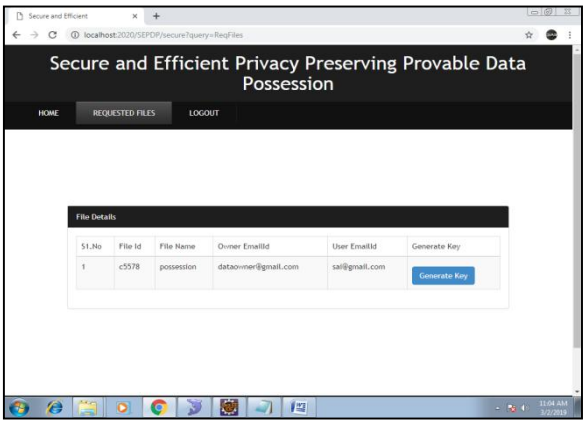
H. Requested files



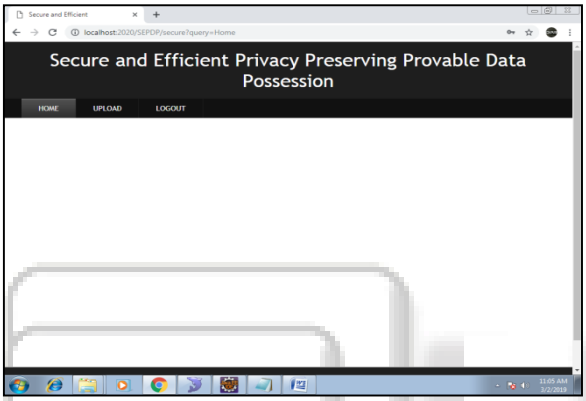
I. TPA Home



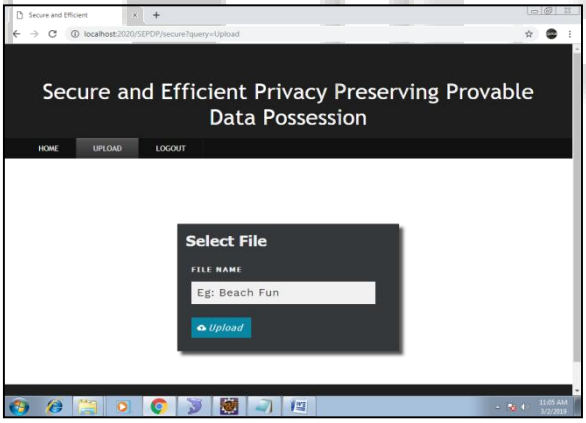
J. Requested files



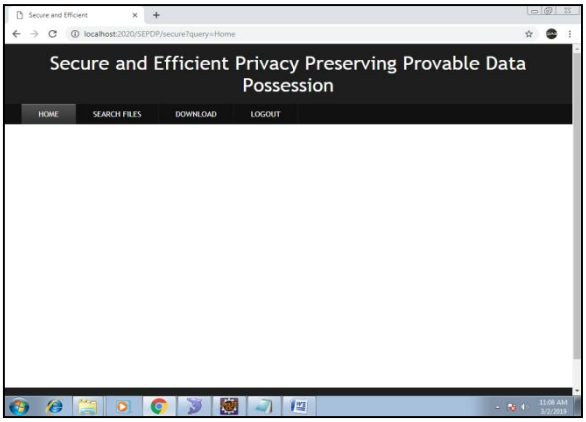
K. Data Owner home



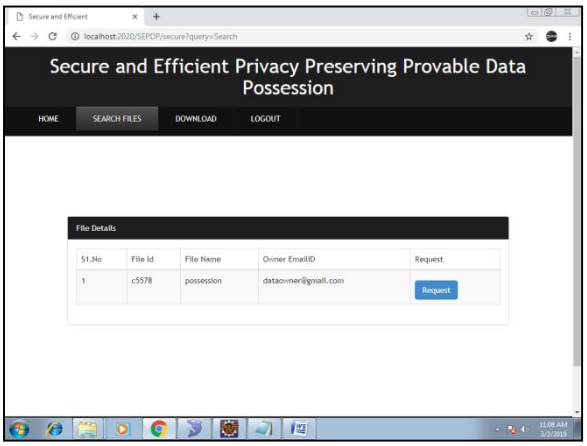
L. Upload File



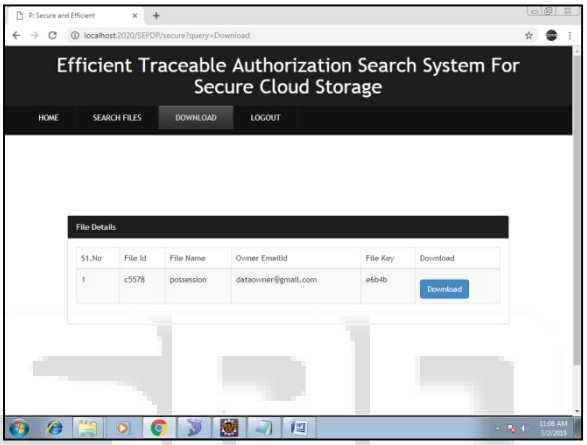
M. User Home



N. Search Files



O. Download



V. CONCLUSION

In this paper, privacy maintaining provable statistics possession scheme (named SEPDP) for untrusted and redistributed stockpiling framework is exhibited. Further, SEPDP is stretched out to help dynamic statistics updation by way of severa owners and clump evaluating. Security of the scheme is investigated and demonstrated that SEPDP shields statistics privacy from TPA whilst infeasible for CSP to manufacture the response without placing away the right squares. The most enticing highlights of the proposed scheme is to help all the important highlights including blockless confirmation, privateness retaining, bunch inspecting and statistics factors with lesser calculation overhead.

REFERENCES

[1] 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.
[2] B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing for data integrity in the cloud," in Proceedings IEEE Conference on Communications and Network Security (CNS), 2013, pp. 136–144.
[3] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proceedings of 14th ASIACRYPT, 2008, pp. 90–107.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM), 2010, pp. 1–9.
[5] L. Yuchuan, F. Shaojing, X. Ming, and W. Dongsheng, "Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage," China Communications, vol. 11, no. 11, pp. 114–124, 2014.
[6] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, 2015.
[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 598–609.
[9] B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient public verification on the integrity of multi-owner data in the cloud," Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, 2014.
[10] 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.
[11] 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, 2013.
[12] H. Wang, "Proxy provable data possession in public clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.
[13] "Identity-based distributed provable data possession in multicloud storage," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328–340, 2015.
[14] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
[15] 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, 2013.
[16] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 1550–1557.
[17] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and ´ J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1034–1038, 2008.
[18] D. L. Gazzoni Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer." IACR Cryptology ePrint Archive, vol. 2006/150, 2006.
[19] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE transactions on Knowledge and Data Engineering, vol. 23, no. 9, pp. 1432–1437, 2011.
[20] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proceedings of 7th ASIACRYPT, 2001, pp. 514–532. VLDB Endowment, 2007.

