A Framework for Protecting Cloud Users from Third Party Auditors

Saif Khalid Musluh
Department Of Ms.C.IS
Osmania University, India
Foundation of Technical Education, Iraq
saifalkhaldi@gmail.com

Mr. T. Ramdas Naik
Assistant Professor (B.E, MCA, M. Tech, Ph.D)
Department Of It Nizam College
Hyderabad, Telangana, India
ramdas_teja@gmail.com

Abstract--Cloud computing has merged to be a now computing paradigm that lets public to access shared pool of resources without capital investment. The users of cloud need to access resources through Internet in pay per use fashion. Thus there is increased use of storage services of cloud in the real world. This service is known as Infrastructure as a Service (IaaS). However, there are security concerns as this service runs in entrusted environment. To ensure data integrity many public verification or auditing schemes came into existence. Nevertheless, there is a concern when the so called Third Party Auditor (TPA) has malicious intentions. In such cases, protection is required against malicious TPAs. Towards this end, recently, Huang et al. proposed a scheme in which users can directly check the integrity of stored data using a feedback based audit scheme. TPA takes process proof from cloud server and gives feedback to cloud user. The feedback is unforgivable and the TPA cannot make any malicious attacks. Based on this scheme, in this paper, we implemented a prototype application that demonstrates the proof of concept. The empirical results are encouraging.

Index Terms – *Cloud computing, storage security, public auditing, and protection from malicious TPA*

*****

I. INTRODUCTION

Cloud computing is the new computing model which provides on-demand access to computing resources in pay per use fashion. The cloud computing technology makes use of virtualization and parallel processing power of Graphical Processing Units (GPUs) in order to provide scalable services. Its services include Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). There are many benefits of cloud computing as the system can provide plethora of services in affordable fashion. Users in all sectors started using cloud service in one way or other.

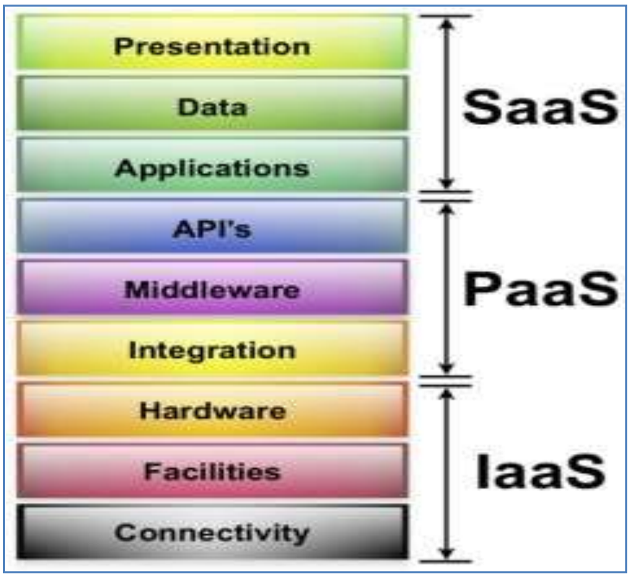

Figure 1 – Illustrates the cloud service layers

As can be seen in Figure 1, it is evident that the SaaS layer provides applications, data and presentation related services. The PaaS layer provides APIs for cloud application development, middleware and integration services. The IaaS layer on the other hand provides connectivity services, hardware and other facilities. These services are rendered on demand. It does mean that the cloud users need to subscribe for the services and pay as they use. Moreover, the cloud computing offers plethora of benefits that are realized in the form of cloud based applications like Drop Box, Google Docs and so on.

Cloud computing has many deployment models. They include private cloud, public cloud and community cloud. The private cloud is the cloud infrastructure that is pertaining to a single organization. Only the users of that organization can use the cloud. Public cloud is the cloud that is accessible any organization or individual globally in pay per use fashion. Community cloud is the cloud that is made by multiple organizations. These organizations only can access such cloud. There is one more deployment model which is the combination of two or more models. It is known as hybrid cloud. Hybrid cloud is very useful. For instance, the combination of private cloud and public cloud can be called as hybrid cloud. The private cloud can exhaust in resources and then it can access public cloud for scalability and business continuity. This way plenty of benefits are possible with hybrid cloud besides providing scalable and reliable services to cloud consumers.

In this context, the users of cloud outsource their data to it. However, there are many security concerns as the cloud servers are untrusted. For this reason many researchers contributed to develop some sort of auditing mechanism that ensures that the data stored in cloud is safe and the integrity of data is preserved. Most of the mechanisms enable a Third Party Auditor (TPA) who can involve in auditing. However, there might be scenarios in which the TPA might behave malicious. Therefore there is need for protecting cloud users from such malicious TPAs. Towards this end, Waung et al. proposed a scheme that makes use of feedback and aggregation of feedback in such a way that the TPA can not involve in malicious attacks. This is because the data owner himself can verify the integrity of data from time to time with the help of the feedback obtained from TPA. The feedback is unforgeable and the cloud computing mechanism is safe in this context. In this paper we implement this approach and built a prototype application that demonstrates the proof of concept. The empirical results are encouraging.

Our contributions in this paper are described here. First of all we investigate into the TPAs and the vulnerabilities of the cloud storage services when TPA turns into malicious. Then we implemented a prototype application that demonstrates the mechanism explored in [25] in order to prove the concept of protecting cloud users from malicious TPAs. The remainder of the paper is structured as follows. Section 2 reviews literature on TPA and the issues with TPA. The section 3 presents the proposed system. Section 4 presents the experimental results while section 5 concludes the paper and provides recommendations for future work.

II. RELATED WORK

This section provides review of literature on cloud storage related issues. When cloud users outsource data, they do not have physical possession of data. Therefore it is imperative that there should be fool proof security. However, in the wake of reports on attacks in 2011, cloud users are worried about the security of outsourced data [4]. This kind of problem is highlighted in many research papers such as [20], [18], [21], 19], and [15]. Some researchers introduced distributed protocols that are used to protect the outsourced data. These protocols were explored in [27], [26], [25] and [22]. Remote integrity checking with public verifiability is explored in [23], [14] and [13].

The data integrity verification protocols were required in order to protect data from malicious changes in the cloud servers. Towards this end many protocols or techniques came into existence. Third party auditing has been around for many years besides provable data possession where the data integrity is given high importance. Privacy preserving public auditing concept was first introduced by Wang et al. [13]. All the TPA schemes that came into existence in the literature assume that the TPA is trustworthy. However, in [28] Xu, for the first time, used a protocol that can audit TPA. This mechanism also defends collude and frame attacks with improved performance in protecting outsourced data. Recently in [25] the TPA itself is considered to be a threat to the security of outsourced data. Towards this end a novel technique was proposed to safeguard the interests of cloud users who outsource their data to cloud. In this paper we implement a prototype application that demonstrates the proof of concept of protecting cloud users from third party auditors.

III. PROPOSED SYSTEM

The proposed system is the implementation of the approach explored in [25] The proposed prototype application has different modules that takes care of data integrity in cloud computing. The data dynamics module takes care of insert, update, and delete operations on cloud. These operations allow the cloud user to maintain his data from time to time and ensure that the data is not stale. By supporting various operations on the outsourced data, the application ensures that the cloud users are able to perform all operation on their data besides securing the data that is being stored in clod infrastructure in a remote place.

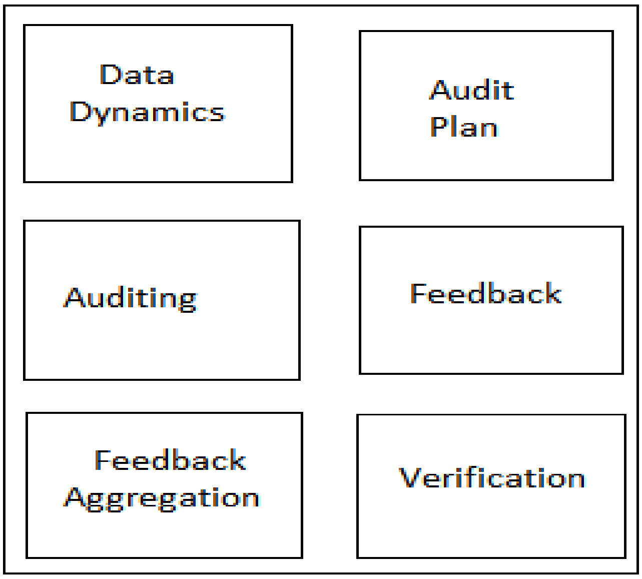

Figure 2 – Modules in the proposed system

As seen in Figure 2, it is evident that the audit plan module is responsible to have audit plan which will help the receive server to give feedback accordingly. The audit plan is given by users. The auditing module is responsible to perform third party auditing that is a kind of public auditing which will ensure that the data integrity prevails. If not, it gives appropriate messages. The feedback module is responsible to provide feedback from time to time. The feedback aggregation module is responsible to aggregate feedback to have cohesive knowledge to make well informed decisions. The verification module is responsible to verify the data integrity finally and that will ensure that the data is intact and not modified illegally. In this process, the proposed model can ensure that the TPA has no chance to perform malicious attacks as the TPA cannot forge feedback and the user is involved in receiving feedback. The data flow is between cloud data owner and cloud server indirectly.

In order to implement the scheme, the following algorithm is used.

```
1.Start
2.User generates audit plan and sends to Receive Server
3.Receive server generated encrypted challenge and sends it to TPA
4.At the same time Server is involved to register temporal events
5.The TPA gives the challenge to cloud server
```

```
6.The cloud server provides proof of integrity
7.Process proof is sent from TPA to Receive Server
8.The Receive Server generates feedback
9.Check time is performed by user
10.Aggregate feedback is given by TPA to user
11.Finally user can verify the integrity to avoid malicious behaviour from TPA
```

Listing 1 – Pseudo code of the proposed system

As can be seen in the above listing, there is sequence of communication among the parties involved. The parties involved are user, receive server, time server, third party auditor and cloud servers. The novelty in this procedure is that the third party auditor will not be able to misbehave and cannot make malicious attacks. The reason behind this is that TPA can generate feedback using process proof and returns the same to user. However, the feedback is not forgeable by TPA and thus there is no chance for him to make attacks.

IV. EXPERIMENTAL RESULTS

A prototype application is built using Java platform. The application has web interface which runs in web server. The application demonstrates the simulations pertaining to all the parties involved in the system. The simulator application demonstrates the third party auditing and the prevention of attacks from third party auditor. The proposed system is analyzed and experiments are made in terms of number of sampled blocks and TPA's computational overhead.

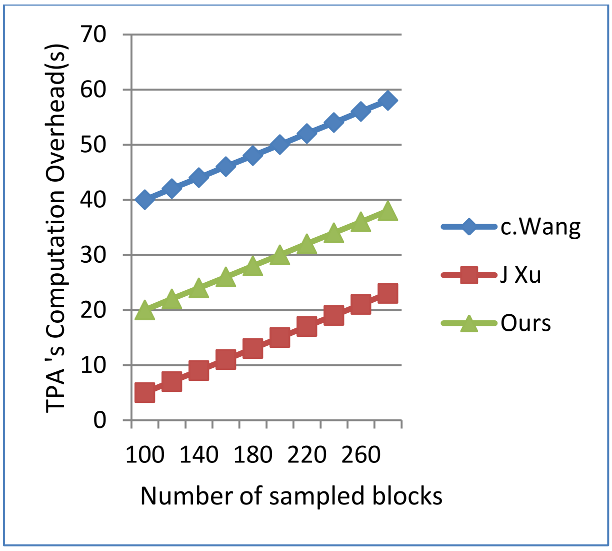

Figure 3 – Performance comparison of TPA's computational overhead

As shown in Figure 3, it is evident that there is performance comparison of the proposed solution to prior solutions in terms of number of sampled blocks and the TPA's computation overhead. The results revealed that as the number of sampled blocks is increased, the TPA's computational overhead is steadily increased. However, it is less in the proposed scheme when compared with the prior schemes.

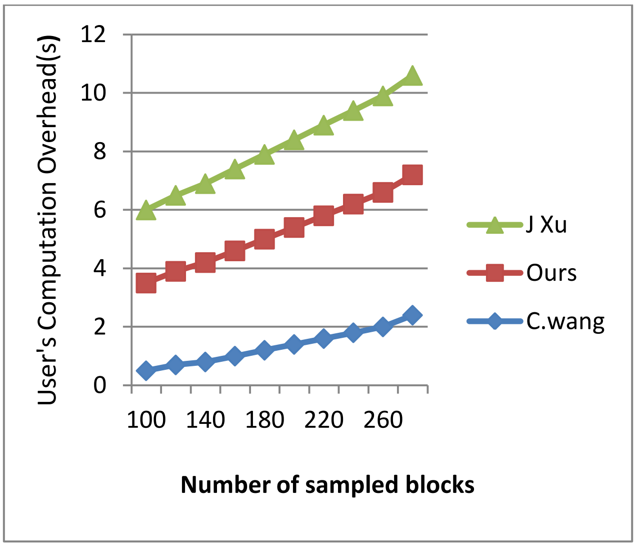

Figure 4 – Performance comparison of user's computational overhead

As shown in Figure 4, it is evident that there is performance comparison of the proposed solution to prior solutions in terms of number of sampled blocks and the user's computation overhead. The results revealed that as the number of sampled blocks is increased, the user's computational overhead is steadily increased. However, it is less in the proposed scheme when compared with one of the prior schemes.

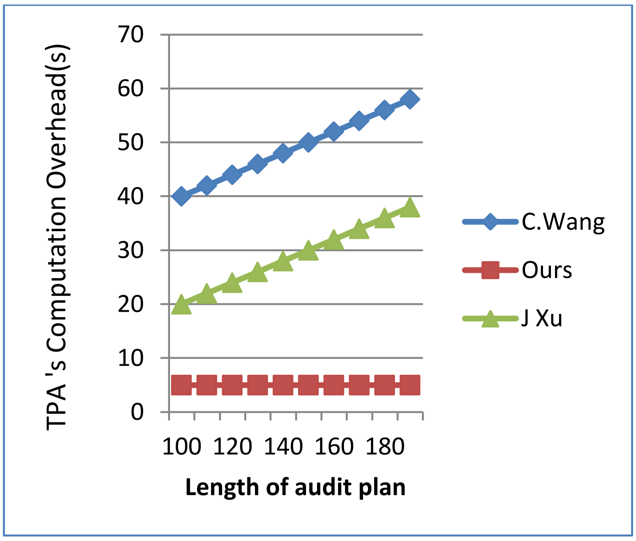

Figure 5 – Performance comparison of TPA's computational overhead

As shown in Figure 5, it is evident that there is performance comparison of the proposed solution to prior solutions in terms of length of audit plan and the TPA's computation overhead. The results revealed that as the length of the audit plan is increased, the TPA's computational overhead is steadily increased. However, it is less in the proposed scheme when compared with the prior schemes.

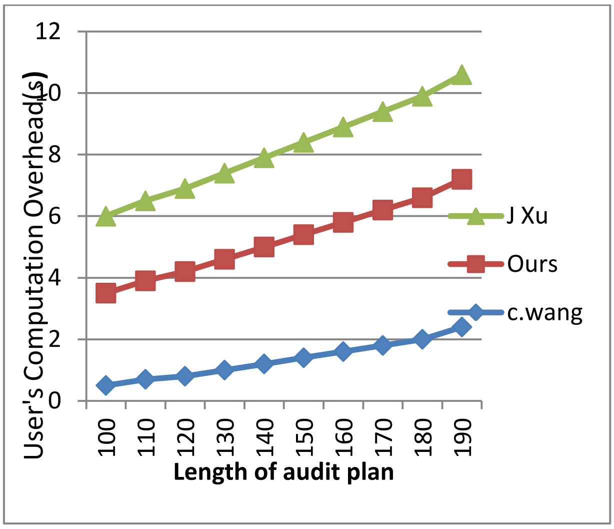

Figure 6 – Performance comparison of user's computational overhead

As shown in Figure 4, it is evident that there is performance comparison of the proposed solution to prior solutions in terms of length of audit plan and the user's computation overhead. The results revealed that as the length of the audit plan is increased, the user's computational overhead is steadily increased. However, it is less in the proposed scheme when compared with one of the prior schemes.

V. CONCLUSION AND FUTURE WORK

In this paper we studied the problem of third party auditing and the possible attacks made by third party auditors with malicious intentions. This is pertaining to cloud computing where cloud users outsource their data to cloud and they are concerned about its security or integrity. Towards this end many solutions came into existence. The most widely used solution is the third party auditing where the public users are served by a third party auditor for data integrity. However, there might be situations, may be rare, in which TPAs might have malicious intentions and make attacks. Towards this end, recently, Huang et al. [25] proposed a scheme that prevents TPA from forging the feedback given to users. The feedback –based scheme enables users to verify the integrity of data though the TPAs are involved in the process. The TPA will not be able to launch attacks since the proposed scheme does not give a chance to TPA. In this paper, this concept is practically implemented using a prototype application that demonstrates the proof of concept. The empirical results are encouraging.

REFERENCES

[1].AmazonS3Versioning2010.Availableat:http://www.doc.s3.amazonaws.com/betadesign/Versioning.html [accessed 02.11.10]

[2].Helft, M.: 'Google confirms problems with reaching its services' (The New York Times, 2009), http://www.developmentguruji.com/news/99/Googleconfirms-problems-with-reaching-its-services.html

[3].Stern, A.: 'Update from amazon regarding friday S3 downtime' (CenterNetworks, 2008), http://www.centernetworks.com/amazon-s3- downtime-update

[4]. Wingfield, N., Microsoft.: 'T-Mobile Stumble with Sidekick Glitch' (The Wall Street Journal,2009),http://www.online.wsj.com/article/SB10001424052748703790404574467431941990194.html

[5].Ateniese, G., Burns, R., Curtmola, R., et al.: 'Provable data possession at untrusted stores'. Proc. 14th ACM Conf. on Computer and Communications Security, New York, Alexandria, VA, October 2007, pp. 598–609

[6].Erway, C., Kupcu, A., Papamanthou, C., Tamassia, R.: 'Dynamic provable data possession'. Proc. 16th ACM Conf. on Computer and Communications Security, New York, Chicago, November 2009, pp. 213–222

[7].Curtmola, R., Khan, O., Burns, R., Ateniese, G.: 'MR-PDP: multiple-replica provable data possession'. Proc. ICDCS'08, 2008, pp. 411–420

[8].Curtmola, R., Khan, O., Burns, R.: 'Robust remote data checking'. Proc. Fourth ACM Int. Workshop on Storage Security and Survivability, StorageSS, 2008, pp. 63–68

[9].Ateniese, G., Pietro, R.D., Mancini, L.V., Tsudik, G.: 'Scalable and efficient provable data possession'. Proc. Securecomm, 2008, pp. 1–10

[10].Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: 'Enabling public verifiability and data dynamics for storage security in cloud computing'. Proc. 14th European Symp., Research in Computer Security (ESORICS 09), 2009, pp. 355–370

[11].Chen, B., Curtmola, R., Ateniese, G., Burns, R.: 'Remote data checking for network coding-based distributed storage systems'. Proc. 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW'10), 2010, pp. 31–42

[12]. Wang, C., Wang, Q., Ren, K., Lou, W.: 'Ensuring data storage security in cloud computing'. Proc. 17th Int. Workshop Quality of Service (IWQoS'09), July 2009, pp. 1–9

[13]. Wang, C., Wang, Q., Ren, K., Lou, W.: 'Privacy-preserving public auditing for data storage security in cloud computing'. InfoCom2010, IEEE, March 2010, pp. 525–533

[14].Wang, C., Ren, K., Lou, W., Li, J.: 'Towards publicly auditable secure cloud data storage services', IEEE Netw. Mag., 2010, 24, (4), pp. 19–24

[15].Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W.: 'Toward secure and dependable storage services in cloud computing', IEEE Trans. Serv. Comput., 2012, 5, (2), pp. 220–232

[16].Wang, C., Chow, S.S.W, Wang, Q., Ren, K., Lou, W.: m'Privacy-preserving public auditing for secure cloud storage', IEEE Trans. Comput., 2013, 62, (2), pp. 362–375

[17]. Hao, Z., Zhong, S., Yu, N.: 'A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability', IEEE Trans. Knowl. Data Eng., 2011, 23, pp. 1432–1437

[18]. Zhu, Y.,Wang, H., Hu, Z., Ahn, G.J., Hu, H., Yau, S.S.: 'Dynamic audit services for integrity verification of outsourced storages in clouds'. Proc. 2011 ACM Symp. on Applied Computing (SAC'11), 2011, pp. 1550–1557

[19].Zhu, Y., Hu, H., Ahn, G., Yu, M.: 'Cooperative provable data possession for integrity verification in multi-cloud storage', IEEE Trans. Parallel Distrib. Syst., 2012, 23, (12), pp. 2231–2244.

[20].Sebe, F., Domingo, J.F., Martinez, A.B., Deswarte, Y., Quisquater, J.: 'Efficient remote data possession checking in critical information infrastructures', IEEE Trans. Knowl. Data Eng., 2007, 20, (8), pp. 1034–1038

[21]. Yang, K., Jia, X.: 'An efficient and secure dynamic auditing protocol for data storage in cloud computing', IEEE Trans. Parallel Distrib. Syst., 2013, 24, (9), pp. 1717–1726

[22].Juels, A., Kaliski, B.S., Pors, Jr.: 'Proofs of retrievability for large files'. Proc. 14th ACM Conf. on Computer and Communications Security (CCS'07), 2007, pp. 584–597

[23].Shacham, H., Waters, B.: 'Compact proofs of retrievability'. Proc. 14th Int. Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT'08), 2008, pp. 90–107

[24].Dodis, Y., Vadhan, S., Wichs, D.: 'Proofs of retrievability via hardness amplification'. Proc. Sixth Theory of Cryptography Conf. on Theory of Cryptography (TCC'09), 2009, pp. 109–127

[25].Bowers, K.D., Juels, A., Oprea, A.: 'Hail: a high-availability and integrity layer for cloud storage'. ACM Conf. on Computer and Communications Security, 2009, pp. 187–198

[26].Bowers, K.D., Juels, A., Oprea, A.: 'Proofs of retrievability: theory and implementation'. Proc. 2009 ACM Workshop on Cloud Computing Security (CCSW'09), 2009, pp. 43–54

[27]. Zheng, Q., Xu, S.: 'Fair and dynamic proofs of retrievability'. Proc. First ACM Conf. on Data and Application Security and Privacy (CODASPY'11), 2011, pp. 237–248

[28]. Xu, J.: 'Auditing the auditor: secure delegation of auditing operation over cloud storage'. Proc. IACR Cryptology ePrint Archive, 2011, p. 304

[29] Cong Wang. (2010). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. IEEE, p1-16.

Authors:

SAIF KHALID MUSLUH
DEPARTMENT OF MS.C.IS
OSMANIA UNIVERSITY, INDIA
FOUNDATION OF TECHNICAL EDUCATION, IRAQ
saifalkhaldi@gmail.com

T. RAMDAS NAIK
Assistant professor (B.E, MCA, M.TECH, PH.D)
Department of it Nizam college
Hyderabad, Telangana, India
ramdas_teja@gmail.com