"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVI – 2013 – Issue 2
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania

THE SECURITY OF CLOUD STORAGE SYSTEMS: ASPECTS OF INFORMATION SECURITY IN THE CLOUD, DATA INTEGRITY, PROOF OF STORAGE AND PROOF OF OWNERSHIP PROTOCOLS

Ciprian RĂCUCIU[1]
Florin MEDELEANU[2]
Narcis-Florentin ANTONIE[3]
[1] Prof. PhD, eng., Titu Maiorescu University
[2] Eng. PhD candidates, Military Technical Academy
[3] Eng. PhD candidates, Military Technical Academy

Abstract: *Cloud security and subsequently their five components (confidentiality, integrity, availability, authenticity and non-repudiation) are differently comprehended by security professionals and home users. There were conducted many surveys concerning this perception, most of these among the companies, resulting that companies are warned and concerned of using information storage services available in cloud. These concerns are determined mainly by the lack of trust related to the provided level of information confidentiality. Due to the fact that the users' behavioral patterns can dramatically influence the data security, the first part of this paper analyzes users' feelings and expectations on information security in cloud, on the one hand, and the actual level of information security in cloud, on the other hand. The second part of the paper is dedicated to cloud storage systems, and specifically to cloud storage security. To overcome the problem of detecting potential tempering of the stored information, the client needs a way to check the integrity of his data and he must make sure that his data has been properly stored on the provider's network. These issues can be addressed using integrity checking, proof of storage and proof of ownership protocols.*
Key-words: *Cloud, information security, cloud storage, integrity checking, proof of ownership.*

1. INTRODUCTION

The usage of cloud computing services has been determined by the need of transforming data centers into a flexible, high-density private cloud that enables far more dynamic and automated control of systems and workloads. Public cloud services may answer to the need of users to add capacity during peak demands. The pervasive spreading of cloud computing solutions has been encouraged by the efficiency, flexibility, and financial benefits of cloud strategies on users' activity. However, in spite of evident benefits, there are yet concerns about the security and privacy of sensitive data stored or processed on shared infrastructure, especially if that infrastructure is owned and managed by a third-party cloud provider.

Security solution providers develop permanently technologies to help improve cloud security, and collaborate with leading hardware and software solution providers to enable more comprehensive and integrated solutions that can make it easier for businesses to adopt cloud computing. These technologies lay the foundation needed for:

• *Strong Data Protection*. Encryption can be implemented pervasively to protect data both at rest and in transit, without compromising performance or driving up costs.

• *Trusted Infrastructure*. Hardware can verify the integrity of key platform software to help protect against sophisticated launch time attacks and establish a control point for enhancing the security of virtualized workloads. Selected applications can be constrained to run only on these trusted pools of virtualized resources, to help protect critical assets more effectively.

• *Security and Compliance Verification*. The security environment of a cloud infrastructure can be more thoroughly monitored, assessed, and documented. With appropriate third-party applications, compliance can be verified dynamically to mitigate risk through unified, policy-based auditing, logging, and reporting.

With these capabilities integrated into the foundation of their chosen cloud solution, the users can take advantage of the benefits of cloud computing, confident that their data is safer and more secure and their business is well-protected against today's increasingly sophisticated attacks.

2. ASPECTS OF INFORMATION SECURITY IN THE CLOUD

Cloud Security Solutions

New security issues arise in cloud environments while more traditional security issues continue to evolve. In a public or virtual private cloud, data resides on servers physically controlled and managed by someone else, so traditional security models aimed at protecting the perimeter of the organization are no longer sufficient. Cloud computing shares some of these security dynamics with today's cross-business and cross-supply chain collaboration models, and it is vitally important to implement appropriate solutions for controlling access, detecting malware and intrusion, and protecting data in these environments. The growth of cloud computing has simply elevated these new security challenges, while at the same time, security issues continue to grow more and more complex. Attacks used to come primarily from individual hackers who were merely looking for personal fame or a fast profit. However, many of today's attacks are more persistent, stealthy, organized, and sophisticated. They target specific types of data and are designed to achieve and retain control of assets for financial gain. Regulatory environments are also changing. Businesses face increasing requirements for compliance, auditing, reporting, privacy, protection, and indemnification, and the risks and costs of noncompliance are large and growing.

To address these challenges, security solutions providers have introduced new technologies that help to enable comprehensive and verifiable security and compliance in cloud environments. With these technologies, they are providing a foundation to make cloud deployments suitable for increasingly sensitive and vital workloads.

Data Protection

Encryption is one of the most effective technologies available for protecting valuable information, but encrypting and decrypting data has traditionally required substantial computing power that can increase costs and slow down the performance of business applications. For this reason, microprocessors manufacturers realized special instructions to reduce the performance overhead by introducing new instructions to accelerate the compute-intensive steps of the encryption algorithms. For example, Advanced Encryption Standards New Instructions (AES-NI) which is implemented in Intel® Xeon processors. Because the Intel AES-NI, hardware instructions also significantly reduce vulnerability to side-channel attacks, subsequently encryption is not just faster, but stronger, as well, as these types of attacks use software agents to analyze how a system processes data and searches for cache and memory access patterns to help deduce elements of the cryptographic processing - and therefore make it easier to "crack".

Once encryption instruction set is built into the processor's instruction set, it eliminates the need for costly security appliances or add-on cards. Encryption can be implemented simply, cost-effectively, and pervasively to protect data.
Intel AES-NI is supported by many of today's leading software vendors to provide comprehensive data protection.
• Protection for Data in Transit. Secure banking transactions such as online bill pay, e-mail services like Gmail and Hotmail, and secure video streaming require complex processing, resulting in a stiff performance penalty and often causing security to be sacrificed to maintain responsiveness.
• Protection for Data at Rest. Encryption for data-at-rest on hard disks helps protect data from loss and theft, while facilitating decommissioning and repair.
• Protection for Data in Enterprise Applications. Oracle* and IBM* DB2* support Intel AES-NI in database tablespace encryption, and SAP* and Red Hat* JBoss* Enterprise Application Platform support Intel AES-NI in business operations. Hypervisor providers, such as Microsoft, VMware, Citrix, Oracle, and the open-source based hypervisors Xen and KVM, support AES-NI running in their guest applications.
By taking advantage of the industry-leading solutions provided by these and other vendors supporting Intel AES-NI and OpenSSL optimizations, users can protect their data more effectively and implement cloud computing with greater confidence.

End Users and Cloud Services

Several studies ranked security and privacy to be major areas of concern and impediments of cloud adoption for companies, but none have looked into end-users' attitudes and practices. Not much is known about consumers' privacy beliefs and expectations for cloud storage, such as webmail, document and photo sharing platforms, or about users' awareness of contractual terms and conditions.
While companies and governments may be able to afford to hire trained security consultants, end-users lack the necessary resources and security education to investigate the data practices of cloud storage providers. The data confidentiality, integrity, and availability risks are partly reflected by the Terms of Service (ToS) and privacy policies of consumer cloud storage companies. It is common practice for free consumer cloud storage services not to offer any service guarantees, to assume no liability for any data loss, and to reserve the right to disable accounts without reason or prior notification, as well as to change or stop providing the service at any time.
Given that users don't usually read the terms of service and privacy policies, it is unclear how many users are actually aware of these conditions. Cloud reliability questions were raised when 150,000 Gmail users and 17,000 Hotmail users found decades of personal email and documents deleted from their accounts.
Understanding users' expectation of privacy is essential in devising appropriate laws and regulations. Governments have repeatedly demanded that companies install backdoors in security solutions and build local servers to facilitate surveillance. Unlike in the case of local storage, for data stored in the cloud, users do not typically know when their data is being accessed by other parties. For example, the notice requirement for stored communications in the US is satisfied by notifying only the storage provider, not the user, of government access.
The issues of surveillance and notice requirement have only recently received media attention, when Twitter disclosed the U.S. government subpoena to turn over user data, including IP addresses, for a number of people connected with Wikileaks. Privacy activists argue that consumers expect privacy in the cloud, while law enforcement agencies in United States, to which most cloud storage providers are subject, stipulate that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties".
We will analyze users' expectations of privacy in the cloud and their awareness of the terms of service agreement with cloud storage provider. We will also investigate how practices and concerns towards cloud storage differ from those of local storage.
In [18], it is conducted a study comparing attitudes toward cloud storage in India and Switzerland, two countries with substantial cultural differences. Switzerland has an individualistic society and India a collectivist one. Indians accept that power and control in society are distributed unequally, whereas Swiss expect an equal distribution. The Swiss Federal Constitution guarantees the right to privacy, but the Constitution of India does not explicitly recognize it.
While in Switzerland, privacy is regulated through the Swiss Federal Data Protection Act, established in 1992 and amended in 2008, in India, there is no general data protection law. However, the Indian government did pass the Information Technology Act (IT Act 2000), amended in 2008. There have been efforts to introduce a data protection bill in India.
The study noted that, despite security expertise and guarantees provided by storage providers, users still consider local storage safer than the cloud, because they believe that nothing on the Internet is safe. Users would, therefore, rather rely on physically protecting devices storing their digital data. Nevertheless, a strong feeling of security in the cloud emerges from the belief that nobody would be interested in seeing their data, because "I am not important", "not famous" or "not criminal".
The results also show that users believe they have more rights and protection than the contract terms with the cloud storage provider actually grant them. The users are typically unaware of the terms and conditions, and in fact assume higher availability, integrity, ownership guarantees and privacy protection in the cloud than they actually have. Furthermore, when prompted, they agreed to pay for better privacy in their cloud storage account.
Analyzing privacy concerns and expectations in populations from two distinctive cultural backgrounds, it was noticed that their cultural differences affect their privacy concerns and expectations in the cloud. As a consequence, there is a significant attitude difference between Swiss and Indians: Swiss store less sensitive data in the cloud than Indians do and are more aware of the lack of guarantees. Furthermore, while Swiss consider government monitoring of cloud-stored data a fundamental privacy infringement, Indians regard it as a necessary step in combating terrorism.

3. DATA INTEGRITY, PROOF OF STORAGE AND PROOF OF OWNERSHIP PROTOCOLS

Cloud Storage

Cloud storage represents a service provided generally by a third party that allows clients to store their data in virtualized storage pools. Usually the CSSP has multiple large data centers which are used to virtualize storage space and provide the client with the exact amount that he needs.
Historically cloud storage is not a new idea. It is believed to have been first proposed in the 1960s by Joseph Carl Robnett Licklider, according to Wikipedia. But it wasn't put into practice until the late '90s because internet services were not very reliable and did not provide the necessary bandwidth required by the upload or download of large amounts of data. This is why cloud storage is considered to be a relatively new service, available for the masses.
The cloud storage presents many advantages over conventional types of storage. The main advantage of cloud storage resides in the fact that users pay only for what they need. But there are also other advantages characteristic with cloud storage. The fact that it's a distributed network of resources presents the advantage of high fault tolerance. Also clients do not need to concern with maintenance, redundancy and upgrading, these tasks will be taken care of by the CSSP.

The main disadvantage of cloud storage comes from the fact that the client must trust a third party. This poses the concern of whether or not the third party can be trusted, or if the travel of data between the client and the CSSP is secure enough to be able to face attacks.

Problems regarding cloud storage

The risks in adopting a cloud storage solution are not negligible. Using a cloud storage solution, with distributed storage space throughout the network, increases the risk of unauthorized access to the data by physical means. Being moved and replicated frequently the data is more vulnerable to unauthorized recovery through reuse of disk drives, disposal of old storage equipment or even by reallocation of the storage space. Also by outsourcing data storage the client does not have any control over the people handling the equipment.

Also, for the client's data to reach the provider's cloud (or vice-versa) it needs to transit a series of WANs (Wide Area Networks), usually the INTERNET. This poses significant security risks.

Sharing storage space and network with other clients increases the risk of data access by an unauthorized client, other than the owner. This may occur due to errors, faulty equipment or even by criminal intent.

Many of these risks may be avoided by using data encryption. But even with data encryption the information stored may be altered by unauthorized parties. In this scenario another problem arises, the client might not become aware that his data has been altered or deleted. So, to overcome this problem the client needs a way to check the integrity of his data. Also the client must make sure that his data has been properly stored on the provider's network. This issue can be addressed with the proof of storage methods.

Solutions to cloud storage issues: Integrity checking and proof of storage

The integrity of data stored in a cloud is very important because can severely affect the activity of the organization. Some studies, like [4], have shown that if a successful attack occurs on one server then a Trojan horse may affect security critical software and thus compromising data integrity. The consequences of such an attack may vary from the defacing of a web page to replacing the stored data with false information or even fraud.

The major problem in case of an attack is that the detection of the data tempering may occur in hours, days or even weeks after the attack. So it is very important to check frequently that critical files are not changed or deleted. One solution is to reload the server to be checked, into a safe mode of operation (usually from an external media drive like a CDROM) and verify the data integrity by computing cryptographic checksums of critical files and comparing them with checksums previously saved. This process need to be performed locally, because some viruses can trick the data analyzer to send checksums computed before tampering with the critical files. This solution is not very practical though, because it requires a lot of time and because a well trained system administrator needs to perform this task locally. Other solution for this problem could be the use of data integrity checking.

Another problem, that clients are faced with, related to cloud storage, is the certainty that the CSSP is continually and thoroughly storing the data entrusted to him. The mechanisms that give the client assurances that his data is correctly stored are called proof of storage mechanisms or POS for short. One way to have proof of storage, was proposed by Qingji Zheng and Shouhuai Xu in their paper ([8]).

Integrity checking protocols

Challenge response protocol - CRP

This is a simple generic protocol which involves a periodic request from the administrator's host, also called verifier, to the verified server. With this request, the verifier asks the server to compute a checksum of a specified file and return the result. When the verifier receives the checksum, it compares it to a reference checksum which was previously saved on the administrator's machine.

So, the response would have this form (where *H* is a one way hash function):

$$R = H(file) \quad \textbf{(1)}$$

But this simple implementation would not work if the server was manipulated in such a way that it would pre-compute all checksums before changing the files. When the verifier asks for the computation of a checksum, the manipulated server would reply with a stored checksum instead of computing a new one. This way the attacker is able to modify any file he desires without alerting the verifier. To overcome this situation the protocol should be modified so that a pre-computed checksum would not be equal with a checksum computed on demand.

One way to have such a result is to introduce a so called "challenge" (denoted *C*) into the request that the verifier sends to the remote server. This way the response checksum would be directly dependent on the challenge sent by the verifier. And when the challenge is known only by the verifier, the server would not be able to pre-compute the right response. In other words instead of computing a checksum as a result of an one-way hash function of the file, with this modification of the protocol, the server has to compute a checksum as a result of the same one-way hash function for the file and the challenge *C*. Thus the result is a totally different checksum each time.

$$R = H(C \mid file) \quad \textbf{(2)}$$

However another problem arises with this modification of the protocol. The verifier cannot compare the resulting response from the server with a saved reference checksum. Also it cannot save a reference checksum pre-compute with the challenge, because the server must not know the challenge in advance.

A solution to this problem would be to store on the verifier's machine the files used by this protocol to check integrity. But this is also not very practical, because, usually, the verifier's machine is used to maintain and verify multiple servers and devices so the storage space required on the verifier's machine would become a serious problem.

Another solution to this problem would be to have two functions *F* and *H'*, where *H'* is a one way hash function and *F* is a function that satisfies:

$$F(C, H'(file)) = H(C \mid file) = R \quad \textbf{(3)}$$

This would be a working solution only if, at least, one of the functions *F* or *H'* would be kept secret. This is because the attacker could have, if he knew both functions, a pre-computed *H'(file)* checksum stored and when the verifier sends the challenge request he would reply with the result of function *F*.

But unfortunately, this solution would not work either, because such pair of functions, *F* and *H'*, has not been found yet.

Yet another solution has been proposed by Yves Deswarte, Jean-Jacques Quisquater and Ayda Saïdane in [16].

A practical example of the challenge response protocol being implemented in a distributed, intrusion tolerant web server is given in [2] and it consists of a series of verifiers that manage and monitor a series of web servers.

Besides checking the integrity of files, directories and tables on remote servers the CRP (challenge response protocol) is used to check the aliveness of servers and other verifiers and also as a "heart beat" mechanism, due to the periodicity of the protocol (raising the alarm if the server does not respond to the challenge in time).

The CRP is intended for the integrity verification of some important system files that are not modified in the normal operation of the server such as system files (e.g. boot files) or security critical files.

Proof of storage

From the perspective of cloud data security there have been two major concepts "Proof of data possession (PDP)" and "Proof Of Retrievability (POR)". The PDP notion was first introduced by Ateniese and his colleagues in [6]. This notion allows clients to check the integrity of their data, much like the protocol presented above. The second notion, POR, was introduced by Juels and Kaliski in their work "*Pors: proofs of retrievability for large files*" [1]. Besides what PDP offered, this notion also allowed the clients to make certain that their data is actually retrievable from the cloud.

From the perspective of efficiency another notion has been proposed, that of the "Proof of ownership" or POW. This notion has been introduced by Halevi et al. in [3]. In order to prevent the server from storing the same data multiple times, thus using the cloud and network resources inefficiently, special techniques are applied to delete the duplicate data entries. POW provides the server with a mechanism to determine that a client really owns the data he claims, allowing for data deduplication.

Until recently the notions of security and efficiency have been studied separately, because they looked like two distinct or even opposite notions. The protocol analyzed in the following pages was proposed by Qingji Zheng and Shouhuai Xu in [13]. This paper proposes a scheme in which the two aspects of security and efficiency can coexist in the same framework. The scheme exploits the fact that the public verifiability of PDP and POR schemes can be used to obtain proof of ownership POW. The notion proposed was called "Proof of storage with deduplication" - POSD.

Proof of storage with deduplication scheme - POSD

Deduplication is a common technique used by many CSSPs to provide efficiency for their clouds, because much of the data stored in the cloud is duplicated. According to a 2010 survey [14] up to 75% of the data stored on clouds is not unique. Thus, using deduplication techniques, the CSSP can save lots of storage space and network resources.

The notion of deduplication was proposed by Harnik et al. in [5], but it poses a problem if applied directly, any user could claim that data. So a solution was needed to proof the ownership of the data. The first solution was the POW scheme proposed in [3], where a concrete construction was also presented.

The protocol analyzed here proposes a scheme that addresses both security and efficiency by allowing secure deduplication of data.

Notations:

l a security parameter. A function $\varepsilon(l)$ is considered negligible if it is smaller then l^{-const} for any *const* and any sufficiently large *l*;

q a *l*-bit prime number and *p* a prime number so that *q|(p-1)*.

F a data file consisting of *n* blocks. Each block is composed of *m* symbols in Z_q, i.e. $F_i=(F_{i1},\ldots,F_{im})$ where $F_i \in Z_q^m$ is the i^{th} block of the file *F*;

fid the identity that uniquely identifies the file *F*;

Tag auxiliary information that each file is associated with (i.e. cryptographic tags). There are two kinds of *Tag*: Tag_{int} and Tag_{dup}. Tag_{int} is the cryptographic information associated with data integrity checking and Tag_{dup} is the cryptographic information used for duplication checking;

[] as an identification for optional arguments of functions and algorithms (e.g. *Alg(a,b[,c])* means that *Alg* has two mandatory arguments *a* and *b* and an optional argument *c*).

Let $H_1:\{0,1\}^* \to G$ and $H_2:\{0,1\}^* \to Z_q$ be randomly chosen from the respective families of hash functions. Both H_1 and H_2 are modeled as random oracles.

Also let $PRF:\{0,1\}^l \times \{0,1\}^* \to \{0,1\}^l$ be a family of secure pseudorandom functions.

Requirements (goals) of POSD:

The requirements of the solution as proposed by the authors are:

the solutions should be built using common functions (e.g. hash functions) in order to allow cross-client data integrity auditing and data deduplication;

the solution should be more efficient than the basic solution of copying the data and perform integrity checking in order to preserve network resources (i.e. bandwidth);

the solution should not force the cloud server to retrieve any significant portion of the data files when determining if it needs to conduct deduplication. This is due to the fact that a server, when uploads large files from the storage to memory, it's consuming a lot of resources;

the solution should also require the client to make only a single pass over its data file, while using an amount of memory that is substantially smaller then the size of the respective file.

This scheme takes into consideration three models of participants, a cloud storage server (S), the cloud storage clients (C) and a third party, also known as Auditor. The auditor can be a third party that is allowed by the client to check the integrity of his data or can be another client that has the same data stored on the cloud. Another fact about this scheme is that the data is stored only in clear text in order to perform deduplication (the same can be said about POW [3]). This fact can prove to be a disadvantage for the scheme in general

The construction of POSD started from considering POSD=PDP+POW because its goal is to accomplish the functionalities of both integrity audit and deduplication.

It is proven ([13]) that POSD scheme provides a way to obtain data audit and proof of ownership within data deduplication scenarios. It is also proven ([13]) that POSD satisfies all the goals mentioned above.

3. CONCLUSIONS

Aspects of information security in the cloud

Reviewing analysis and arguments of this paper, it was showed that:

New security threats and risks arise in cloud environments, while the traditional security issues continue to evolve;

Attacks that aim at security compromising continue to grow more and more complex and try to be stealthy;

Cloud solutions for organizations incorporate reliable security solutions which allow to efficiently providing data confidentiality, integrity and availability;

The level of expertise in the security area, but also end users expectations regarding the real level of data security in cloud, is low;

Free consumer cloud storage services do not offer any service guarantees regarding provisioning of data confidentiality, integrity and availability;

The highest level of security for cloud services is offered to companies, which usually have experienced security specialists who can formulate and verify the compliance of security requirements.

Challenge response protocol - CRP

One possible way for an attacker to successfully hack a server protected by CRP is to keep copies of the files used by the protocol for integrity checking. These copies should be the original versions of the files, without any alterations made by the attacker. This way the attacker can still modify files and use them to fulfill his objectives. And he will use the original versions of the files to trick the CRP with the right responses.

Also the solution of periodically rebooting the server will not solve the original problem; even though will erase any unauthorized copy from the system. The attacker will have plenty of time between reboots to hack the servers and accomplish his goals.
The solution to prevent this security risk is to deny the attacker the possibility to make copies of the files. This can be done in many ways.
One possibility to prevent unauthorized copying of files is to size the storage space in such a way that the attacker would not have the required space available to copy another file, thus preventing him from fooling the CRP.
Another method to prevent this security threat is to instruct the CRP to check the integrity of folders too. Applying this method would allow the CRP to detect if the content of the folder has been modified. Also a host-based intrusion detection system would be able to discriminate the copying of the files from normal server operations.

Proof of storage with deduplication protocol – POSD
In computer science data deduplication is a technique used for saving data storage space by eliminating duplicate copies of repeating data [9]. Unfortunately after deduplication, a major security risk arises, anybody can claim ownership of the data stored on the server.
POSD is the first efficient scheme that aims to achieve both data ownership verification and integrity checking (data auditing).
Both parts of the scheme, data auditing and proof of ownership, are modeled as a challenge response protocol and are very similar in the implementation. The difference between them lies in the roles that the participants are playing. In data auditing the role of auditor can be played by a third party or by the client that owns the file audited. Instead, in data ownership checking the role of auditor is played by the cloud storage server.
As for the efficiency, POSD has been compared to other schemes that provide data integrity checking or proof of ownership. POSD is the only scheme that offers both data integrity checking and proof of ownership. The results of the comparison are presented in table 1.

Property \ Scheme	PDP [6]	POR [11]	POSD [13]	POW [3]
total key size	$O(m)$	$O(m)$	$O(m)$	0(no keys)
use Random Oracle?	yes	yes	yes	no
security assumption	RSA	CDH	CDH	C-RH
For integrity audit purpose				
client storage	$O(1)$	$O(1)$	$O(1)$	N/A
server storage	$O(n)$	$O(n)$	$O(n)$	N/A
audit preprocessing comp.	$O(mn)$Ex+ $O(mn)$Mu	$O(mn)$Ex+$O(mn)$Mu	$O(n)$Ex+$O(mn)$Mu	N/A
audit computation (client)	$O(c)$Ex+ $O(cm)$Mu	$O(c)$Ex+ $O(cm)$Mu	$O(c)$Ex+ $O(cm)$Mu	N/A
audit computation (server)	add	add	add	N/A
audit communication	O(mℓ)	O(mℓ)	$O((m + c)\ell)$	N/A
integrity assurance	$1 - (1 - ERR)^c$	$1 - (1 - ERR)^c$	$1 - (1 - ERR)^c$	N/A
For deduplication purpose				
dedup. preprocessing comp.	N/A	N/A	$O(n)$Ex+$O(mn)$Mu	ECC +$O(n^2)$H
dedup. computation (client)	N/A	N/A	$O(cm)$Mu	$O(n^2)$H
dedup. computation (server)	N/A	N/A	$O(c)$Ex+$O(cm)$Mu	$O(c \log(n))$H
dedup. communication	N/A	N/A	O(ℓm)	O(cmℓ log(n))

Efficiency comparison between some PDP, POR, POW and POSD schemes [13], where n is the number of blocks of a data file, m is the number of symbols of a block, c is the number of blocks that will be challenged, ERR the probability of block corruption, Ex modular exponentiation operation, Mu modular multiplication operation and N/A means Not Applicable.

In table 1 we can observe that POSD scheme requires $O(n)$ exponentiations when the client processes the file F before uploading it. This complexity is much smaller than the processing requirements of PDP and POR. But from the same table we can see that in the audit process the communication overhead of POSD is higher then that of POR and PDP. But the difference is not significant, especially when dealing with large files and if we consider today's communication possibilities.
When we compare the deduplication efficiency of POSD with POW's, we can see that POW is a bit more efficient. But POW's main drawback is that it cannot perform data audit. Also POSD uses smaller communication overhead then POW (because $O(ml)$ is usually smaller then $O(c \log(n)ml)$). We can also see that POW is secure in the standard model based on the usage of Collision-Resistant Hash functions (C-RH).
To conclude, the construction of Proof Of Storage with Deduplication scheme (POSD) was motivated by the need to perform two security operations on cloud storage systems simultaneously, integrity checking and deduplication. The scheme proved to be as efficient as other models (PDP, POR, and POW). But, unlike the other schemes POSD has the advantage of performing two security operations simultaneous.

REFERENCES
[1] - A. Juels and B. S. Kaliski, Jr. "Pors: proofs of retrievability for large files". In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 584–597, New York, NY, USA, 2007
[2] - A. Valdes, M. Almgren, S. Cheung, Y. Deswarte, B. Dutertre, J. Levy, H. Saïdi, V. Stavridou and T. Uribe, "An Adaptative Intrusion-Tolerant Server Architecture", in Proc. 10th International Workshop on Security Protocols, Cambridge (GB), 17-19 April 2002, ISBN 3-540-20830-5, 2004
[3] - B. P. A. S.-P. Shai Halevi, Danny Harnik. "Proofs of ownership in remote storage systems". Cryptology ePrint Archive, Report 2011/207, http://eprint.iacr.org/, 2011
[4] - CERT Advisory CA-2002-24, Trojan Horse OpenSSH Distribution, August 1, 2002

[5] - D. Harnik, B. Pinkas, and A. Shulman-Peleg. "Side channels in cloud services: Deduplication in cloud storage". IEEE Security and Privacy, 8:40–47, November 2010
[6] - 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, CCS '07, pages 598–609, New York, NY, USA, 2007
[7] - *http://cloudstoragestrategy.com/2009/03/defining-cloud-storage.html*
[8] - *http://en.wikipedia.org/wiki/Cloud_storage*
[9] - *http://en.wikipedia.org/wiki/Data_deduplication*
[10] - *http://searchcloudstorage.techtarget.com/definition/cloud-storage*
[11] - H. Shacham and B. Waters. "Compact proofs of retrievability". In Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '08, pages 90–107, Berlin, Heidelberg, Springer Verlag, 2008
[12] - Leslie Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, 24(11), November 1981
[13] - Qingji Zheng, Shouhuai Xu, "Secure and Efficient Proof of Storage with Deduplication", Department of Computer Science, University of Texas at San Antonio, September 2011
[14] - "The digital universe decade - are you ready?", International Data Corporation,. *http://idcdocserv.com/925*, 2010
[15] - Yan Xiangtao, Li Yifa, "A new data integrity checking scheme for cloud storage", *IACR Cryptology ePrint Archive*, Vol. 2012 (2012), January 2012
[16] - Yves Deswarte, Jean-Jacques Quisquater, Ayda Saïdane, REMOTE INTEGRITY CHECKING, How to Trust Files Stored on Untrusted Servers, ISBN 978-1-4020-7900-9, 13-14 November 2003.
[17] - Hanna, Steve. Cloud Computing: Finding the Silver Lining, Juniper Networks Inc., 2009
[18] - Ion, Iulia. Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage, http://www.vs.inf.ethz.ch/publ/papers/iion-cloud-2011.pdf
[19] - Qaisar, Sara. Cloud computing: network security threats and countermeasures, Interdisciplinary Journal of Contemporary Research in Business, Jan.2012, Vol.3, No.9
[20] - www.intel.com/go/cloud.org - *Security in the cloud.*