ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7829-7833

Preserving Data Integrity and Public Auditing for Data Storage in Cloud Computing

M. Pavani[1], D. Jayanarayana Reddy[2], Dr. S.PremKumar[3]

[1]Student, CSE Department, GPCET(affiliated to JNTUA , Anantapur), Kurnool, India

[2] Assistant Professor, CSE Department, GPCET(affiliated to JNTUA , Anantapur), Kurnool, India

[3] Professor and Head Of the Department, GPCET(affiliated to JNTUA , Anantapur), Kurnool, India

Abstract*: In this project the utilization and combining of public key based homomorphic authenticator with random masking to achieve the preservation of privacy to the public cloud data auditing system which meets all the above requirements. If there is a situation for multi auditing tasks then we further extend the technique of bilinear aggregate signature to extend the main result to multi user setting where the third party auditor can perform the multi auditing tasks simultaneously.*

The main issue is going on, on the outsourced data. Cloud computing produces some of the new and challenging security threats to the cloud users outsourced data. Cloud service providers are the separate entities. The data outsourcing will provide an insecure performance in the user's outsourced data due to the unauthenticated performance of the strangers. In the existing scenario although the infrastructure of the cloud is good with an powerful computing devices but there were internal and external threats which leads to an issue to the data integrity. The status of the outsourced data was not clear. Although the well infrastructure cloud do not providing the exact status about the users outsourced data.

Keywords: Data storage, privacy-preserving, public audit ability, cryptographic protocols, cloud computing.

1. INTRODUCTION:

Cloud Computing has been visualised because the next-generation data technology ar-chitecture for enterprises, as a result of its long list of unprecedented advantages within the IT history: on-demand self-service, omnipresent network access, location freelance resource pooling, fast resource snap, usage-based valuation and transference of risk [1]. As a riotous technology with profound implications

Cloud Computing is remodeling the terribly nature of how businesses use data technology. One basic aspect of this paradigm shifting is that knowledge is being centralized or outsourced to the Cloud. From users' perspective, together with each people and IT enterprises, storing knowledge remotely to the cloud during a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with freelance geographical locations, and shunning of cost on hardware, software, and personnel maintenances, etc [2]. While Cloud Computing makes these benefits more appealing than ever, it conjointly brings new and difficult security threats towards users' outsourced data. Since cloud service suppliers (CSP) area unit separate administrative entities, knowledge outsourcing is really relinquishing user's final management over the fate of their data. As a result, the correctness of the information in the cloud is being place in danger thanks to the subsequent reasons. 1st of all, though the infrastructures under the cloud square measure far more powerful and reliable than personal computing devices, they're still facing the broad vary of each internal and

external threats for knowledge integrity. samples of outages and security breaches of noteworthy cloud services seem from time to time [3]–[7]. Secondly, there do exist various motivations for CSP to behave unreliably towards the cloud users concerning the standing of their outsourced knowledge. For examples, CSP would possibly reclaim storage for financial reasons by discarding knowledge that has not been or isn't accessed, or perhaps hide knowledge loss incidents thus on maintain a name [8]–[10].

In short, though outsourcing knowledge to the cloud is economically engaging for semi permanent large-scale knowledge storage, it doesn't instantly supply any guarantee on knowledge integrity and availableness. This drawback, if not properly addressed , could impede the made deployment of the cloud design. As users now not physically possess the storage of their data, ancient cryptanalytic primitives for the purpose of knowledge security protection cannot be directly adopted [11]. above all, merely downloading all the data for its integrity verification isn't a sensible solution thanks to the monetary value in I/O and transmission cost across the network. Besides, it's typically insufficient to notice the information corruption only if accessing the information, because it doesn't provide users correctness assurance for those unaccessed knowledge and may well be too late to recover the info loss or harm. Considering the large size of the outsourced information and therefore the user's constrained resource capability, the tasks of auditing the data correctness in a very cloud setting are often formidable and costly for the cloud users [10], [12]. Moreover, the overhead of mistreatment cloud storage should be decreased the maximum amount as attainable, such that user doesn't have to be compelled to perform too several operations to use the info (in extra to retrieving the data).

For example, it's fascinating that users don't have to be compelled to worry regarding the requirement to verify the integrity of the info before or when the info retrieval. Besides, there is also more than one user accesses identical cloud storage, say in associate degree enterprise setting. For easier management, it is fascinating that the cloud server solely entertains verification request from one selected party. To fully make sure the information integrity and save the cloud users' computation resources also as on-line burden, it is of essential importance to alter public auditing service for cloud information storage, so users could resort to associate degree freelance third party auditor (TPA) to audit the outsourced information once required. The TPA, who has experience and capabilities that users don't, can sporadically check the integrity of all the info stored within the cloud on behalf of the users, which provides a lot of easier and reasonable way for the users to make sure their storage correctness within the cloud. Moreover, additionally to assist users to guage the risk of their signed cloud information services, the audit result from TPA would even be beneficial for the cloud service suppliers to boost their cloud primarily based service platform, and even serve for freelance arbitration functions [9]. In a word, sanctioning public auditing services can play a very important role for this nascent cloud economy to become totally established, where users can would like ways in which to assess risk and gain trust within the cloud.

Recently, the notion of public auditability has been proposed within the context of guaranteeing remotely keep data integrity beneath totally different system and security models [8], [10], [11], [13]. Public auditability permits an external party, additionally to the user himself,

to verify the correctness of remotely keep information. However, most of those schemes [8], [10], [13] don't consider the privacy protection of users' information against external auditors. Indeed, they'll probably reveal user information info to the auditors. This severe downside greatly affects the protection of those protocols in Cloud Computing. From the attitude of protective information privacy, the users, United Nations agency own the information and admit TPA only for the storage security of their information, do not want this auditing method introducing new vulnerabilities of unauthorized info leak towards their information security [14]. Moreover, there area unit legal regulations, like the USA insurance movability and responsibleness Act (HIPAA) [15], further demanding the outsourced information to not be leaked to external parties [9]. Exploiting encryption before outsourcing [11] is a method to mitigate this privacy

concern, however it's solely complementary to the privacy preserving public auditing theme to be projected.

In this paper. while not a properly designed auditing protocol, encoding itself cannot stop information from "flowing away" towards external parties throughout the auditing method. Thus, it doesn't fully solve the problem of protective information privacy however simply reduces it to the key management. Unauthorized information leakage still remains a haul owing to the potential exposure of decoding keys. Therefore, the way to alter a privacy-preserving third-party auditing protocol, freelance to information encryption, is that the downside we have a tendency to area unit planning to tackle in this paper. Our work is among the first few ones to support privacy-preserving public auditing in Cloud Computing, with a spotlight on information storage. Besides, with the prevalence of Cloud Computing, a foreseeable increase of auditing tasks from totally different users could also be delegated to TPA. because the individual auditing of those growing tasks will be tedious and cumbersome, a natural demand is then the way to alter the TPA to efficiently perform multiple auditing tasks in a batch manner, i.e., at the same time.

To address these issues, our work utilizes the technique of public key primarily based homomorphic linear authenticator (or HLA for short) [8], [10], [13], which enables TPA to perform the auditing while not exacting the native copy of knowledge and so drastically reduces the communication and computation overhead as compared to the simple information auditing approaches. By desegregation the HLA with random masking, our protocol guarantees that the TPA might not learn any data concerning the information content stored within the cloud server throughout the efficient auditing process. The aggregation and pure mathematics properties of the critic any benefit our style for the batch auditing.

Specifically, our contribution will be summarized because the following 3 aspects:

1) we have a tendency to inspire the general public auditing system of knowledge storage security in Cloud Computing and supply a privacy-preserving auditing protocol, i.e., our theme allows associate external auditor to audit user's outsourced information within the cloud while not learning the information content.

2) To the simplest of our data, our theme is that the first to support ascendible and efficient public auditing in the Cloud Computing. Specifically, our scheme achieves batch auditing wherever multiple delegated auditing tasks from totally different users will be performed at the same time by the TPA.

3) we have a tendency to prove the protection and justify the performance of our projected schemes through concrete experiments and comparisons with the state-of-the-art.

2. PROPOSED SCHEMES:

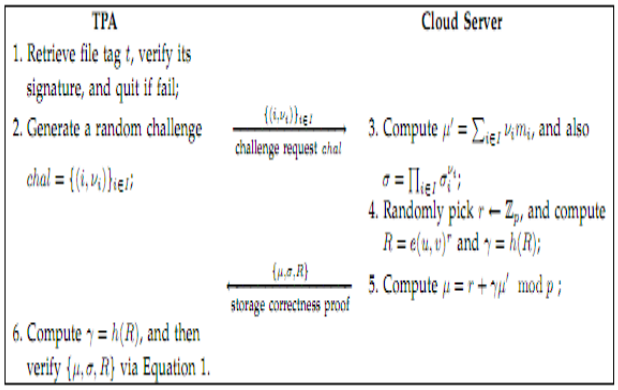
2.1 Provable data possession at un trustable stores:

The provable knowledge possession (PDP) that enables a shopper that has keep data at associate degree untrusted server to verify that the server possesses the first knowledge while not retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, that drastically reduces I/O prices. The shopper maintains a relentless quantity of information to verify the proof. The challenge/response protocol transmits atiny low, constant amount of knowledge, that minimizes network communication. Thus, the PDP model for remote data checking supports massive knowledge sets in widely-distributed storage systems. We present two provably-secure PDP schemes that ar a lot of economical than previous solutions, even in comparison with schemes that succeed weaker guarantees. specially, the overhead at the server is low (or even constant), as against linear within the size of the info.

2.2 Privacy preserving public auditing scheme:

To achieve privacy-preserving public auditing, we tend to propose to unambiguously integrate the homomorphic linear critic with random masking technique. In our protocol, the linear combination of sampled blocks within the server's response is disguised with randomness

generated the server. With random masking, the TPA now not has all the required information to create up an accurate cluster of linear equations and thus cannot derive the user's information content, regardless of what number linear combos of the same set of file blocks may be collected. On the other hand, the correctness validation of the block authenticator pairs will still be applied during a new way which is able to be shown shortly, even with the presence of the randomness. Our style makes use of a public key primarily based HLA, to equip the auditing protocol with public auditability. Specifically, we use the HLA projected in [13], that is predicated on the short signature theme projected by Boneh, Lynn and Shacham.

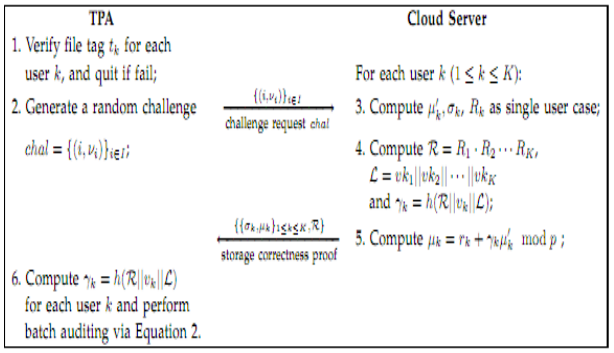


2.3 Support for batch auditing protocol:

With the institution of privacy-preserving public auditing, the TPA could at the same time handle multiple auditing upon totally different users delegation. The individual auditing of those tasks for the TPA will be tedious and extremely inefficient. Given K auditing delegations on K distinct knowledge files from K totally different users, it's a lot of advantageous for the TPA to batch these multiple tasks along and audit at just the once. Keeping this natural demand in mind, we tend to slightly modify the protocol in a very single user case, and achieves the aggregation of K verification equations (for K auditing tasks)

2. As a result, a secure batch auditing protocol for simultaneous auditing of multiple tasks is obtained.

[6] C. Wang, Q. S.M. Chow, Kui Ren and Qian Wang, "Ensuring data storage security in cloud computing," in December2011



3. CONCLUSION

In this project the privacy preserving public auditing system for data storage security in the cloud computing.TPA perform the storage auditing. The utilization of the homomorphic authenticator with random masking has been proposed in order to avoid the online burden to the user. Batch auditing is the process in which the third party auditor used to perform the multiple auditing tasks simultaneously. Enhanced security and performance analysis shows that the proposed schemes are secure and highly efficient.

4. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. of IEEE INFOCOM'10, March 2010.

[2] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009. http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html.

[3] Cloud Security Alliance, "Top threats to cloud computing,"2010,http://www.cloudsecurityalliance.org.

[4] Amazon.com, "Amazon s3 availability event: July 20,2008,"http://status.aws.amazon.com/s320080720.html, 2008.

[5] 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, 2011.

[7] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. of Eurocrypt 2003, volume 2656 of LNCS.Springer-Verlag, 2003, pp. 416–432.

[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley viewof cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.