International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 8 Issue 11 Series. I || November 2019 || PP 01-04

"A Review on Third party Storage Auditing Service"

Afrin Sheikh, Monika Ranghuwanshi
(Computer Science Department, RKDF College RGPV University Bhopal, India)
Corresponding Author : Afrin Sheikh

Abstract : *To fully check the data security and save the cloud users' computation resources, it is of critical importance to permit public audit ability for cloud data storage so that the users may resort to a third party auditor (TPA), who has expertise and skill that the users do not audit the outsourced data when needed. Based on the audit result, TPA have to discharge an audit report, which would not only help users to evaluate the risk of their subscribed cloud data services, but also be profitable for the cloud service provider to improve their cloud based service platform. In a word, enabling public risk auditing protocols will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in Cloud. In this paper, survey has been done for third party audit services and problem statement has been given in the paper based on existing method.*

Keywords : *third party, auditing, cloud computing, encryption algorithms, storage security.*

Date of Submission: 26-10-2019 Date of acceptance: 11-11-2019

I. Introduction

Cloud Computing has been envisioned as the next generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. As a disruptive technology with profound implications, Cloud Computing is mold the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.[2].

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a achieve, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time [3]–[5].

II. LITERATURE SURVEY

C. Wang et. al. 2010 introduces the cloud computing is the since a long time ago imagined vision of registering as an utility, where clients can remotely store their information into the cloud in order to appreciate the on-request top notch applications and administrations from a mutual pool of configurable processing assets. By information redistributing, clients can be diminished from the weight of neighborhood information stockpiling and upkeep. Nonetheless, the way that clients never again have physical ownership of the perhaps enormous size of redistributed information makes the information respectability insurance in Cloud Computing an extremely testing and possibly considerable assignment, particularly for clients with compelled figuring assets and abilities. Therefore, empowering open auditability for cloud information stockpiling security is of basic significance with the goal that clients can turn to an outside review gathering to check the trustworthiness of re-appropriated information when required. To securely proposed an efficient third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy

Alese, B. K. et. al. 2012 has been proposed as a cryptosystem on the grounds that it fulfils both security prerequisites and proficiency with shorter key lengths. This exploration work centres around the near examination of RSA Encryption algorithm, ElGamal Elliptic Curve Encryption algorithm and Menezes-Vanstone Elliptic Curve Encryption algorithm. These elliptic curve analogues of ElGamal Encryption scheme were implemented in Java, using classes from the Flexi provider library of ECC. The RSA algorithm utilized in the correlation is the Flexi supplier execution. Execution assessment on the three calculations dependent on the time slip by for their Key age, encryption and decoding calculations, and scrambled information size was completed and analyzed. The outcomes demonstrate that our elliptic bend based usage are increasingly better than the RSA calculation on every similar parameter.

Eman M. et. al. 2012 with distributed computing, every one of our information is put away on the cloud. So cloud clients pose a few inquiries like: How secure is the cloud? Will unapproved clients access your secret information? There are three kinds of information in distributed computing. The primary information in travel (transmission information), the second information very still (stockpiling information), lastly information in handling (preparing information). Mists are hugely intricate frameworks can be decreased to straightforward natives that are imitated a huge number of times and basic useful units, These complexities make numerous issues identified with security just as all parts of Cloud figuring. So clients consistently stress over its information and ask where the information is? Furthermore, who approaches? Each cloud supplier scrambles the information by utilizing the encoding calculations they make improvement to information security model in distributed computing. They execute programming to the cloud supplier. This product is actualized with two factor verification. This product looks at between eight modem encryption calculations.

P. Mell et. al. 2009 proposed an architecture and taxonomy for cloud computing based model that lays out the central elements of cloud computing for Federal CIOs, Procurement Officials and IT Program Managers. The cloudscape is open and expanded and the going with scientific categorization gives a way to portray it in an unambiguous way. The RA is introduced in two sections: a total diagram of the entertainers and their jobs and the important design parts for overseeing and giving cloud administrations, for example, administration organization, administration arrangement, cloud administration the board, security and protection. The Taxonomy is displayed in its own segment and supplements are devoted to terms and definitions and instances of cloud administrations.

M. Armbrust et. al. 2009 Cloud computing, the since quite a while ago held fantasy about figuring as an utility, can possibly change an enormous piece of the IT business, making programming much progressively alluring as a help and molding the manner in which IT equipment is planned and acquired. Engineers with imaginative thoughts for new Internet benefits never again require the huge capital costs in equipment to convey their administration or the human cost to work it. They need not be worried about over provisioning for a help whose prominence doesn't meet their forecasts, accordingly squandering exorbitant assets, or under provisioning for one that turns out to be uncontrollably well known, in this way missing potential clients and income. Also, organizations with enormous bunch situated errands can get results as fast as their projects can scale, since utilizing 1000 servers for one hour costs close to utilizing one server for 1000 hours. This versatility of assets, without paying a premium for huge scale, is exceptional throughout its entire existence. Distributed computing alludes to both the applications conveyed as administrations over the Internet and the equipment and frameworks programming in the server farms that give those administrations. The administrations themselves have for some time been alluded to as Software as a Service (SaaS). The server farm equipment and programming is the thing that they will call a Cloud. At the point when a Cloud is caused accessible in a compensation as-you-to go way to the overall population, they consider it a Public Cloud; the administration being sold is Utility Computing. They utilize the term Private Cloud to allude to inward server farms of a business or other association, not made accessible to the overall population. Subsequently, Cloud Computing is the aggregate of SaaS and Utility Computing, however does exclude Private Clouds. Individuals can be clients or suppliers of SaaS, or clients or suppliers of Utility Computing. They center around SaaS Providers (Cloud Users) and Cloud Providers, which have gotten less consideration than SaaS Users.

III. Problem Statement

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1:

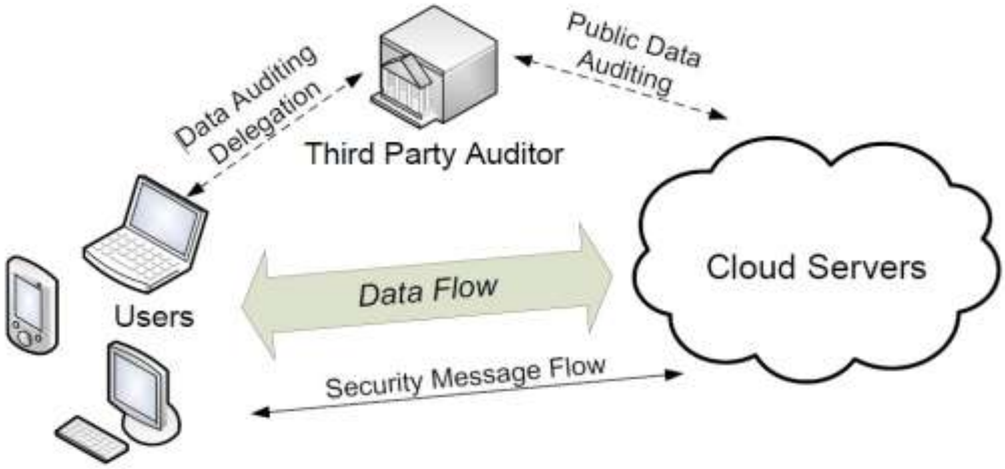

Fig. 1: The architecture of cloud data storage service

The cloud user, who has enormous measure of information records to be put away in the cloud; the cloud server, which is overseen by the cloud specialist organization to give information stockpiling administration and has critical extra room and calculation assets (we won't separate CS and CSP in the future); the outsider auditor (TPA), who has skill and capacities that cloud clients don't have and is trusted to survey the distributed storage administration unwavering quality in the interest of the client upon solicitation. User rely upon the CS for cloud data storing and support. They may likewise powerfully associate with the CS to access and refresh their put away information for different application purposes. As clients never again have their information locally, it is of basic significance for clients to guarantee that their information are by and large accurately put away and kept up. To spare the calculation asset just as the online weight possibly brought by the intermittent stockpiling rightness confirmation, cloud clients may depend on TPA for guaranteeing the capacity honesty of their redistributed information, while planning to keep their information private from TPA. We accept the information trustworthiness dangers towards clients' information can emerge out of both inside and outside assaults at CS. These may include: programming bugs, equipment disappointments, bugs in the system way, monetarily inspired programmers, noxious or inadvertent administration mistakes, and so forth. In addition, CS can act naturally intrigued. For their very own advantages, for example, to look after notoriety, CS may even choose to shroud these information defilement occurrences to clients. Utilizing outsider inspecting administration gives a financially savvy strategy to clients to pick up trust in Cloud. We accept the TPA, who is in the matter of inspecting, is dependable and autonomous. Be that as it may, it might hurt the client if the TPA could get familiar with the re-appropriated information after the review. Note that in our model, past clients' hesitance to spill information to TPA; we additionally expect that cloud servers have no motivations to uncover their facilitated information to outer gatherings. From one viewpoint, there are guidelines, for example HIPAA [16], mentioning CS to keep up clients' information security. Then again, as clients' information have a place with their business resource [10], there likewise exist money related motivations for CS to shield it from any outside gatherings. In this way, we expect that neither CS nor TPA has inspirations to intrigue with one another during the examining procedure. At the end of the day, neither one of the entities will digress from the endorsed convention execution in the accompanying introduction. To approve the CS to react to the review assigned to TPA's, the client can give a declaration on TPA's open key, and all reviews from the TPA are confirmed against such an authentication.

IV. Conclusion

Now a day‘s Cloud Computing facing security Challenges. User put their data in the cloud and data is being transferred from one Cloud to another and users are concerned about the security. We concern higher security of Data and therefore we have studied Encryption Algorithms which takes least time to encrypt the Data than others and will ensures about the faster retrieval of Data. Security related parameters such as Encryption, Authentication and Access Control, Separation of Duties for the security has been satisfied in this Algorithm in order to achieve the Security. We have find that Encryption Algorithms ECC has a better performance and more secure than other Encryption Algorithms.

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'13, Feb 2013.

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

[3]. 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 view of cloud computing," University of California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb 2009.

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

[5]. M. Arrington, "Gmail disaster: Reports of mass email deletions," 2006, http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-email-deletions/.

[6]. J. Kincaid, "MediaMax/The Linkup closes its doors," July 2008, http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/.

[7]. Amazon.com, "Amazon s3 availability event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, 2008.

[8]. 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.

[9]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, 2007, pp. 598–609.

[10]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[11]. A. Juels and J. Burton S. Kaliski, "PORs: Proofs of retrievability for large files," in Proc. of CCS'07, October 2007, pp. 584–597.

[12]. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.

[13]. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt, vol. 5350, Dec 2008, pp. 90–107.

[14]. C. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine,vol. 24, no. 4, pp. 19–24, 2010.

[15]. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07, 2007, pp. 1–6.

[16]. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[17]. R. Curtmola, O. Khan, and R. Burns, "Robust remote data checking," in Proc. of the 4th ACM international workshop on Storage security and survivability (StorageSS'08), 2008, pp. 63–68.

[18]. K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. of ACM workshop on Cloud Computing security (CCSW'09), 2009, pp. 43–54.

Afrin Sheikh"A Review on Third party Storage Auditing Service" International Journal of Engineering Science Invention (IJESI), Vol. 08, No.11, 2019, PP 01-04