International Journal of Electrical, Electronics and Computer Engineering **3**(2): 144-148(2014)

ISSN No. (Online): 2277-2626

A Review of Cloud Environment and Recognition of Highly Secure Public Data Verification Architecture using Secure Public Verifier Auditor

Javed Akthar Khan* and Ritika Arora[**]

[#]*Department of Computer Science & Engineering,*
Takshshila Institute of Engineering & Technology, Jabalpur, (MP), India

(Corresponding author: Javed Akthar Khan)

(Received 05 October, 2014 Accepted 18 November, 2014)

ABSTRACT: As we all know the simple definition of Cloud computing means that the Service on Demand. The cloud computing and its work simple working concept is data stored in cloud for utilization .This data is used by cloud user at any time or in any place. In other word we can say that the cloud store the data these data is used by multiple user when they required .when data is store is in cloud server or cloud data centre due to hardware failure, human failure and human mistake cloud data integrity is occur , the major problem is cloud computing is store a big amount of data in its server so it is not possible to retrieving entire file or data from the cloud server or solve this data integrity problem with proper high level security. So in this paper we are proposed a new cloud architecture for Third party auditor authentication with minimum auditing Time.

Keywords: Cloud computing, Public Cloud, Private Cloud, Community Cloud Hybrid Cloud, Third party auditing.

I. INTRODUCTION

In the cloud storage Environment , users can remotely save their content and used software application already available in cloud server when they needed, user also able to shared his her data or information to other user cloud user use resources of cloud 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[1]. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. This is the introductory section of the paper rest of paper is organized as follows. In section II presents the cloud deployment model, Section III present the cloud service models. The section IV we discuss about public verifier and public auditing, section V represents privacy in public auditing and public verifiers. The literature survey is discussed in section VI, the problem definition and proposed solution is presented in section VII & VII. Finally section IX concludes our work.

II. CLOUD DEPLOYMENT MODEL

The clouds come in different forms: public clouds, private clouds, hybrids clouds. It depending on the type of data we are working with we will want o compare public, private and hybrid clouds in terms of the different levels of security and management required as shown in Fig. 1.

(i) Public Cloud Computing. Public Cloud computing means relying on third parties to offer efficient IT services over the Internet as needed. Public Clouds are owned by the organization(s) selling Cloud services, The National Institute of Standards and Technology defines a public Cloud as a Cloud infrastructure that is made available to the general public or a large industry group.

(ii) Private Cloud Computing. Private Cloud computing reassures the organization that their information and processes are more secure since everything is managed internally. According to the National Institute of Standards and Technology (NIST) a private Cloud is a Cloud infrastructure that is operated solely for an organization.

(iii) Community Cloud. The cloud infrastructure is use by a specific community of consumers that have shared concerns e.g., mission, security requirements, policy and compliance considerations. It may be owned, managed and operated by one or more of the organizations in the community a third party or some combination of them, and it may exist on or of premises [1].

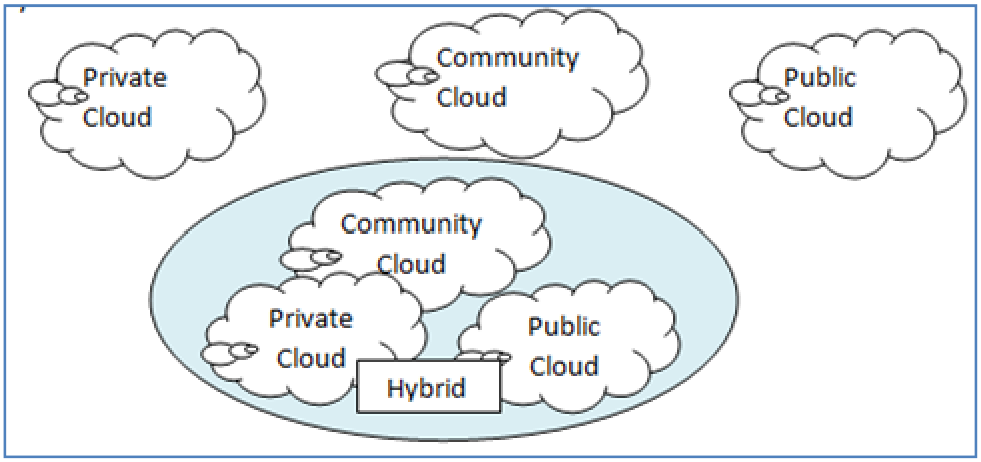

Fig. 1. Cloud Deployment Model.

(iv) Hybrid Cloud Computing. Hybrid Cloud computing is a combination of both private and public services.

III. CLOUD SERVICES MODEL

(i) Software as a Service (SaaS). This is the capability provided to consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface such as a web browser e.g., web based email, website, CRM or a program.

(ii) Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure. The consumer-created applications using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage.

(iii) Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources. Where the consumer is able to deploy and run arbitrary software which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and possibly limited control of select networking components e.g., host firewalls [1].

IV. PUBLIC VERIFIER AND PUBLIC AUDITING

Public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier. Existing system allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing[3].

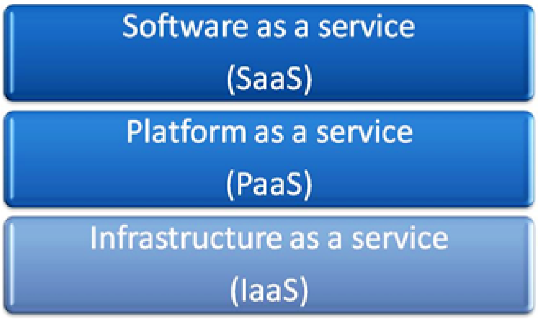

Fig. 2.

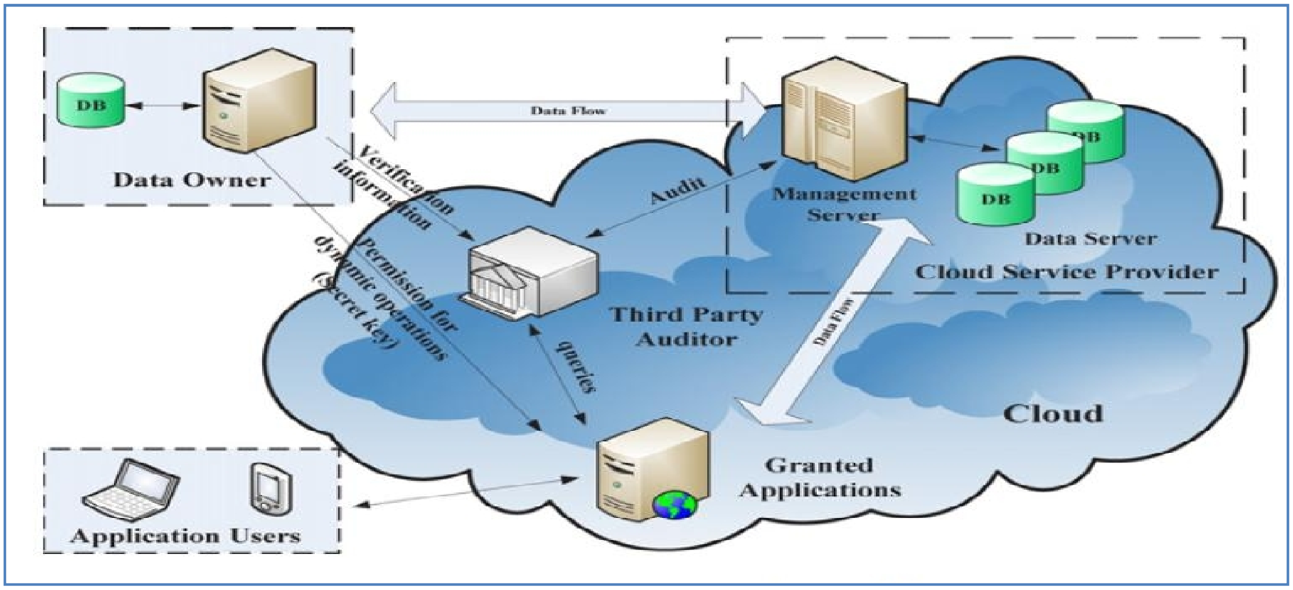

Fig. 3. Public Verifier and Public auditing**.**

Data is divided into many small blocks (as shown in above Fig. 3), where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier could be a data user who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services.

V. PRIVACY IN PUBLIC AUDITING AND PUBLIC VERIFIERS

During public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers as shown in Fig. 4. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud Sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage [5]. It is necessary to ensure the integrity of shared data in the cloud is correct. Existing public auditing mechanisms can actually be extended to verify shared data integrity.

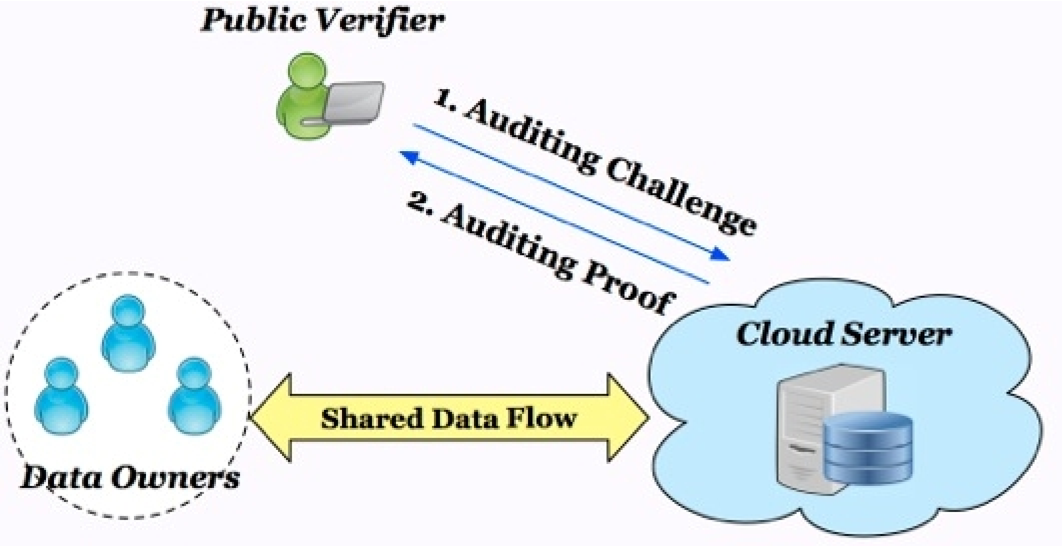

Fig. 4. Public Verifiers.

VI. LITERATURE SURVEY

A careful analysis of literature on the variants and methodologies of privacy preserving in cloud computing reveals the following: So many method are already exiting for auditing cloud content before storing cloud Environment , this will be done Third person or some time called TPA .The user might give his/her identity of proof certificate This paper includes the problems of misuse of the proof of identity (POI) certificate if fallen into unauthorized person. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers [6]. Bharathy S *et al.* decentralized key management work for providing a security to cloud data Security and privacy protection in clouds are being explored by many researchers. Wang et al. addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptographic techniques has been studied in. Many homomorphic encryption techniques have been suggested to ensure that the cloud is not able to read the data while performing computations on them. HLA homorphic liner authenticaot scheme is used by TPA to perform the auditing task in cloud , this work done in without demanding a local copy of data ,Access control in clouds is gaining attention because it is important that only authorized users have access to valid service [7,8]. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Drop box) or even personal information (as in social networking.

VII. PROBLEM DEFINITION

After study the literature review integrity of data stored in the cloud can become compromised. To protect the integrity of data in the cloud and to offer “peace of mind” to users, it is best to introduce a third party public verifier/ auditor to perform auditing tasks on behalf of users but main problem is no body can ensure that third party auditor is secure . We are just assuming third party auditor is trusted. There are so many task perform by third party public data verifier like computation/communication resources that users may not possess. Integrity of cloud data should be verified before any data utilization or share, such as search or computation over cloud data[2,3,4]. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures or hash values of the entire data. Certainly, this conventional approach is able to successfully check the correctness of cloud data. The main drawback is new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers , apart from that a conventional architecture are not provide a data privacy , and no identity. In we are show the simple working concept of Auditing task where data will be shared after completion auditing task; this task is done by public verifier / auditor. So during literature survey we read so many method describe for solving this problem . data will be audit by public verifier now here we just assume that a public verifier is doing his work honestly , solving this problem I have introduce a new cloud data public verifier architecture that supervise a working of third party public auditor .

VIII. PROPOSED SOLUTION

In my research work we have proposed a new cloud data integrity “guarding against improper information modification or destruction. “architecture that take a manage database of third party auditing record in other word we can say for providing a highly secure public data auditing we supervised a record of third party verifier in an proper manner . Privacy issue on shared data is solved by, a new highly secure privacy preserving public auditing mechanism. so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier. The main advantage of this proposed solution is to Support batch auditing, it can perform multiple auditing tasks simultaneously , Improve the efficiency of verification for multiple auditing tasks ,Preserve data privacy from public verifiers, Leverage index hash tables from a previous public auditing solution to support dynamic data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information.

IX. CONCLUSION

Data privacy is one of the biggest challenges in Cloud Computing. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. According to our scheme a user can create a file and store it securely in the cloud. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity and we show the improve result via auditing graph shown in this paper. In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

REFERENCES

[1]. Thakur Pawan & Thakur Sikma,(2014)*"Cloud Computing"*, First Edition , Satya Prakashan New Delhi.

[2]. Cloud Computing Architecture using Discretion Algorithm(2010), *Third International Conference on Emerging Trends in Engineering and Technology, IEEE,* DOI 10.1109/ICETET.2010.103.

[3]. Wang, B.; Baochun; Wang, H. L. (2012) Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, *IEEE Fifth International Conference on Cloud Computing, 2012 IEEE*, DOI 10.1109/CLOUD.

[4] Bertino, E.; Paci, F.; Ferrini, R. (2009) Privacypreserving Digital Identity Management for Cloud Computing, *IEEE Computer Society Technical Committee on Data Engineering*.

[5]. Yassin, A. A.; Jin, H.; Ibrahim, A.; Qiang, W.; Zou, D. (2012). A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing, *IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum, 2012 IEEE*, DOI 10.1109/IPDPSW.2012.148.

[6]. Syed, M. R.; and F, Mohammad; "PccP: A Model for Preserving Cloud Computing Privacy", (2012) *International Conference on Data Science & Engineering* (ICDSE, IEEE.).

[7]. W, Jian; Y, Wang; J, Shuo and Le, Jiajin; "Providing Privacy Preserving in cloud computing", (2009) *International Conference on Test and Measurement, 2009 IEEE*, ICTM.

[8]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, (2011), "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Trans. Parallel and Distributed Systems,* vol. **22**, no. 5, pp. 847-859.