Survey on Cloud Storage Security Techniques

Ajithra Jayan. J[1] Prof. Simi I[2]
[1]M.Tech Student [2]Associate Professor
[1,2]Department of Computer Science & Engineering
[1,2]Musaliar College of Engineering & Technology Pathanamthitta, APJ Abdul Kalam Technological University Kerala, India

Abstract— Cloud computing will enables ubiquitous access to shared pools of configurable system resources. It has a virtual storage that the users can access it from where ever they want. But these logical pools have some problems in storage. Need to put high security technic on cloud storage. Here we would like to prepare a survey on cloud storage security methods (or) techniques that will be help to build a better and unique new security for cloud storage. Survey is based on the existing provable data possession and public key usages. For increasing the security of cloud storage we would like to introduce new methods.

Key words: Cloud Computing, Cloud Storage, Provable Data Possession, Public Key

I. INTRODUCTION

Now a day's world act like a global village that can share all type of information and data without any distance consume. The best part of internet is cloud service that provides a large storage area. Cloud computing comprises of two components front end and back end. Front end consist client part of cloud computing system. It comprise of interfaces and applications that are required to access the cloud computing platform. While back end refers to the cloud itself, it comprises of the resources that are required for cloud computing services. It comprise of interfaces and applications that are required to access the cloud computing platform

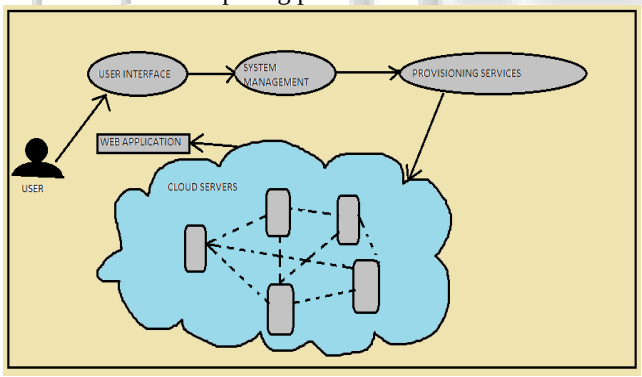

Fig. 1: Cloud system architecture

The cloud is a large group of interconnected computers; they can be public or private. It has some key properties: user centric, task centric, powerful, accessible, intelligent and programmable.

In the cloud storage it offers online storage space on demand. Managed cloud storage system presents what appears to the user to be a raw disk that the user can partition and format. The multiple copies of data stored on multiple servers and that must be on number of locations. It has the virtual storage containers that offer high performance cloud storage systems.

Storage of data on cloud is not that simple task. Apart from its convenience and flexibility, the users want to face some problems. Because of its virtual locations for data storage, there is a chance to security problems. It is a big challenge to the organizations which are used cloud services. The consumers do not have any knowledge about the exact location of storage. When it be a huge amount of storage, then it is difficult to check the particular data is safe or not. Every time consumers can't verify their data. Many cloud users report the data loss & leakage problems, for example: In 2011, Amazon's cloud EC2 was permanently destroyed some amount of data. But user's only knows when it needed. Now a day cloud is under the control of a third – party cloud services provider (CSP). Many of these challenges should be addressed through management initiatives.

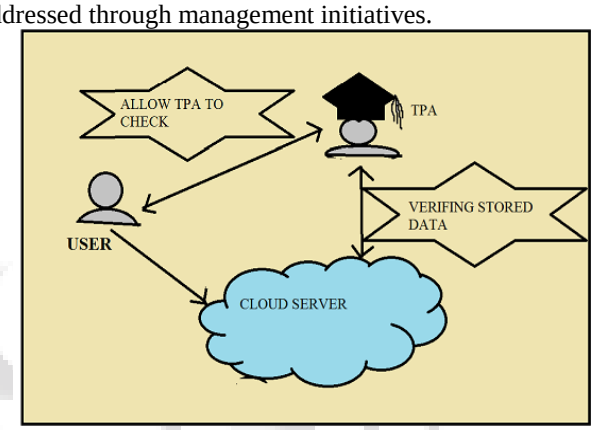

Fig. 2: System model of cloud with TPA

When organizations are trusted TPA services and they give the data details that stored in cloud. Sometimes the encrypted data for more security they are given, but still there are the chances to recover the confidential data from cloud through TPA. There are lots of researches based on these issues. So we are preparing a survey on cloud storage security technique.

II. SURVEY REPORT

The cloud is large data storage that why traditional methods cant applies directly: hash function, MAC etc. so the remote data integrity checking is used and it is a challenging research topic. According to the basics of cloud, it needs verification.

The first time a verification method for entire remote data in cloud without explicit information about the data is proposed by Blum [1]. In it a checker is provide the service for the entire structure of data stored. The various structures of data are defined as n amount of long and want to check and prove basis of these n size. It will provide alert about the environment. The methods used are not enough for large amount of remote data. Recently cloud is widely used by the online storage and distributed storage system. So it wants to meet large amount of data as unpredictable.

Khabal proposed an effective and flexible batch audit scheme with dynamic data support to reduce the computation overheads [2]. It uses a symmetric encryption for the utilization of outsourced cloud data and that will be

for the storage security of multi cloud data storage. The dynamic operations on multiple data blocks such as insertion, delete, update and replacement are secure. But the complexity is high when the cloud storage provider (CSP) handles the security message flow along with TPA. It may causes confusion in provider/client.

Provable data possession proposed by Atenies [3], [4] most effective basic way of cloud security. In the PDP method, the file data in the local storage will be formed as metadata. The metadata along with the data file will be stored in the virtual space provided by cloud server service. The cloud server wants to prove that the data stored are safe and it is in the right space by accepting the challenge given by the verifier. The verifier dynamically selects one portion and set it as the challenge and sends to cloud server. If response is matches with challenge then the data is safe in virtual space. With the use of a third party it is an effective idea for cloud security. But still want to check whether TPA is trust worthy.

Secure the knowledge of stored data from TPA, an encryption strategy is needed. Currently a public key method is used. Now a day various certified authority (CA) are available to provide public key. Boneh proposed an alternative approach to using a certificate to authenticate public key is identity based cryptography [9], in which PK is user's identity. But still have the chances to retrieve the knowledge of data stored.

The remote data integrity checking on cloud platform has huge possibilities, so the researchers are more interested in it and the resent years shows the proof [5]-[8], [7]-[10], [6]-[11], [13]-[15]. According to the research papers Ateniese's contribution is high; PDP and dynamic PDP schemes [12] are examples.

Author & paper	Concept of paper	Issues
C.Wang [15]: Privacy preserving public auditing for secure cloud storage	Zero knowledge public auditing to resist offline guessing attacks	Formal security model is not provided
C. Erway [9]: Dynamic provable data possession	PDP model extended to dynamic PDP	Limited number of queries & block insertion is not support
Q. Wang [10]: Enabling public audibility and data dynamics for storage security in cloud computing	Improve previous PDP by using MHT	MHT not enough to verify block indices
C.Wang [15]: Privacy preserving public auditing for data storage security in cloud computing	Privacy definition based scheme	Verifier can't recover whole blocks
Y. Yu [14]: Enhanced privacy of RDIC protocol for secure cloud storage	Privacy of RDIC	Work only in public key infrastructure

Table 1: Analysis Model

III. Conclusions

In this survey paper, we study the cloud security related works that for remote data integrity check and cloud platform security. Cloud is a virtual space that can be used by where ever client stands. With use of internet it makes global village for communication and data transformation. Because of virtual pool we need more conformations about our storage, which make the stream more sensible and attractive for researchers. Day by day number of users and need are increasing. So we need more user friendly and concrete cloud service with high security.

References

[1] M. Blum, W. Evans, P. Gemmell, S. Kannan, M. Naor, Checking the correctness of memories. Proc. Of the 32nd Annual Symposium on Foundations for Computers, SFCS 1991, pp.90-99, 1991.
[2] Remote data integrity checking in cloud computing – Khaba. M. V, M. Santhalakshmi . IJRITCC June 2013.
[3] G. Ateneiese, R. C. Burns, R. Curtmola, J.Herring, L.Kissner, Z. N. J. Peterson, D. X. Song, Provable data possession at untrusted stores. ACM conference on computer and communications security, 598-609, 2007.
[4] G. Ateneiese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur, 2011
[5] H. Shacham, and B. Waters, Compact proofs of retrievability. LNCS 5350,pp. 2008
[6] K. Yang, and X. Jia. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Trans. On Parallel and Distributed Systems, 2013
[7] C. Wang, Q.Wang, K. Ren, and W. Lou, Privacy preserving public auditing for data storage security in cloud computing. IEEE 2010
[8] J. Yu, K. Ren, C.Wang, V. Varadharajan, Enabling cloud storage auditing with key-exposure resistance, IEEE Trans. On Information Forensics and Security, 2015
[9] C. Erway, A.Kupcu, C.Papamanthou, R.Tamassia, Dynamic provable data possession, 2009.
[10] Q. Wang, C. Wang, K.Ren, W. Lou, and J. Li, Enabling public audibility and data dynamic for storage security in cloud computing. IEEE Trans. 2011.
[11] Y. Yu, Y. Li, J. Ni, G. Yang, Y. Mu, W. Susilo, Comments on public integrity auditing for dynamic data sharing with multiuser modification, IEEE Trans. 2016.
[12] G. Ateniese, R. D. Pietro, L. V. Mancini, G. Tsudik, Scalable and efficient provable data possession, Proc. Of SecureComm 2008.
[13] H. Wang, Identity-based distributed provable data possession in multicloud storage, IEEE Trans. 2015.
[14] Y. Yu, M H Au, Y. Mu, S. Tang, J.Ren, W. Susilo, and L. Dong, Enhanced privacy of a remote data integrity checking protocol for secure cloud storage, International journal of information security, 2015.
[15] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, Privacy preserving public auditing for secure cloud storage, IEEE Trans, 2013

